

SOUS LA DIRECTION DE
JEAN-HERVÉ LORENZI,
BERNARD GAINNIER
ET JOËLLE DURIEUX
ET LE PARRAINAGE DE
ANTOINE PETIT, PDG, CNRS

Intelligence artificielle, blockchain et technologies quantiques au service de la finance de demain

Finance Innovation
Pôle de compétitivité mondial

RB ÉDITION

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFET
DE LA RÉGION
D'ILE-DE-FRANCE

îledeFrance

Ce Livre Blanc a été réalisé avec le soutien de
La Préfecture de Paris et d'Ile-de-France et la Région Ile-de-France.

FÉDÉRATION
BANCAIRE
FRANÇAISE

Fédération Française
de l'Assurance

afg
association française
de la gestion financière

Nous remercions chaleureusement la FÉDÉRATION BANCAIRE FRANÇAISE,
la FÉDÉRATION FRANÇAISE DE L'ASSURANCE et l'ASSOCIATION FRANÇAISE DE GESTION
pour leur contribution et leur mobilisation au sein de ce Livre blanc et des actions du Pôle FINANCE INNOVATION.

CH
&Co.

En collaboration avec Chappuis Halder & Co., acteur global du conseil en management
dédié aux services financiers d'aujourd'hui et de demain.

ISBN, impression, diffusion : en cours - Ce document est une pré-édition événementielle.

© Pôle de compétitivité mondial FINANCE INNOVATION – Palais Brongniart - 28, place de la Bourse, 75002 Paris

Pour la présente édition : REVUE BANQUE ÉDITION – 18, rue La Fayette, 75009 – www.revue-banque.fr – 2019

Diffusé par les Éditions d'Organisation – 1, rue Thénard – 75240 Paris Cedex 05

Conformément aux dispositions du Code de la propriété intellectuelle, toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du Centre français d'exploitation du droit de copie (CFC, 20, rue des Grands Augustins – 75006 Paris).

SOUS LA DIRECTION DE
JEAN-HERVÉ LORENZI,
BERNARD GAINNIER
ET JOËLLE DURIEUX
ET LE PARRAINAGE DE
ANTOINE PETIT, PDG, CNRS

Intelligence artificielle, blockchain et technologies quantiques au service de la finance de demain

Finance Innovation
Pôle de compétitivité mondial

RB
ÉDITION

Préface





Antoine PETIT

Président-directeur général, CNRS

Bernard GAINNIER

Président, Pôle FINANCE INNOVATION

En 2019, avec l'**intelligence artificielle** (IA) et les **technologies quantiques**, nous nous trouvons en présence de deux innovations de rupture. Leurs implications sur les objets connectés, les robots, les drones, les véhicules autonomes, la santé et les villes intelligentes (*smart cities*), montrent qu'au-delà d'offrir de nouvelles possibilités, elles constituent une véritable révolution.

Si on y ajoute les transformations des relations entre acteurs induites par la **blockchain**, ces innovations numériques sont en train d'envahir notre société à une vitesse qui nous surprend. Elles génèrent des espoirs et des craintes compréhensibles, car elles touchent chacun de nous dans sa vie personnelle et professionnelle.

Le Pôle FINANCE INNOVATION contribue depuis 10 ans à faire germer et grandir les innovations pour les filières banque, assurance, gestion d'actifs, immobilier, économie sociale et solidaire, métiers du chiffre et du conseil. FINANCE INNOVATION fédère les différents acteurs afin d'obtenir une ligne directrice claire et partagée du développement des innovations au sein de ces filières.

C'est aujourd'hui une réalité avec le numérique. Tant au cœur des grands groupes que dans des fintechs, le Pôle favorise l'éclosion et l'adoption de ces innovations.

L'accélération des dernières années, pour ne pas dire des derniers mois, a mis en évidence de nouvelles dimensions :

- rapidité croissante de la création et de l'acceptation de nouvelles pratiques ;
- mondialisation qui inclut maintenant des territoires tels que l'Afrique ou le Moyen-Orient ;
- interaction entre les différents secteurs d'activité où la disruption dans l'un d'entre eux se propage à l'ensemble de l'économie ;
- prise de conscience de l'intérêt pour notre pays de se positionner en leader face à ces opportunités.

Tout cela crée d'autant plus de responsa-

bilités pour le Pôle FINANCE INNOVATION.
Pour répondre aux besoins de ses membres comme de l'ensemble des acteurs et organismes concernés, le Pôle a relevé le défi de présenter dans ce livre blanc les choix à effectuer à la suite de l'émergence de ces technologies et de faire ressortir, comme il le fait habituellement, les Domaines d'Innovations Prioritaires (DIP), axes sur lesquels la communauté estime que les priorités doivent être portées : le défi n'est pas mince face à la dimension du sujet.

Pour y parvenir, une collaboration très proche entre les experts du Pôle et ceux de l'INRIA, du CNRS et des entreprises qui ont participé à ce livre blanc a permis d'identifier, au milieu de nombreux thèmes qui sous-tendent la transformation numérique de notre société, 28 tendances clés pour l'avenir,

En effet, les challenges rencontrés sont pour certains spécifiques à nos filières, pour d'autres, partagés avec différents secteurs d'activité ; certains sont particuliers à notre pays, la plupart existent au niveau européen ou mondial. Beaucoup ont une complexité engendrée par le fait qu'ils sont à la fois mondiaux et transverses tout en comportant aussi des spécificités locales ou sectorielles. C'est par exemple le cas des problématiques de sécurité, de confidentialité des données ou, pour la question de la gestion des talents et de la formation des citoyens à ces nouvelles technologies.

Pour le Pôle FINANCE INNOVATION, il est important d'accompagner la création et la croissance de fintechs françaises, mais aussi de détecter et d'intégrer les innovations des fintechs étrangères aux activités des entreprises nationales. Enfin, il est nécessaire de considérer les solutions reposant sur la blockchain pour les questions de gestion des pouvoirs et se préparer, suffisamment à l'avance, au bouleversement annoncé par les technologies quantiques.

La force de ce livre blanc provient de la très large participation, à travers plus de 200 contributeurs, des acteurs représentatifs de l'écosystème de la finance : les fintechs, insurtechs et regtechs, mais aussi les grands groupes institutionnels, assureurs, banquiers, asset managers, industriels d'autres secteurs économiques qui ont apporté une ouverture d'esprit précieuse et nécessaire, académiques, conseils et entreprises de services du numérique (ESN) qui accompagnent tous les jours l'écosystème dans sa transformation.

Sommaire

PRÉFACE 6

1. INTRODUCTION 12

1.1. Les objectifs 14

1.2. La démarche 16

1.3. La cible 17

1.4. Le comité de pilotage 18

Pilotage général 18

Les comités de pilotage des groupes de travail 18

1.5. Les enjeux de la finance 19

1.6. Bienvenue chez vous en 2030 20

2. L'INTELLIGENCE ARTIFICIELLE AU SERVICE DE L'INDUSTRIE FINANCIÈRE 24

2.1. Un peu d'histoire 27

2.2. Quelques chiffres sur le marché de l'IA 28

2.3. Des technologies au service des métiers de l'industrie financière 29

DIP 1 : développer et augmenter la capacité décisionnelle en avenir incertain 32

Focus : la gestion d'actif à l'heure de l'IA chez Bramham Gardens ... 35

DIP 2 : augmenter le conseiller face au client 38

Focus : l'IA pour augmenter l'assureur avec une Insurtech 40

DIP 3 : augmenter le collaborateur .41

DIP 4 : proposer le « self-care » ... 42

DIP 5 : solliciter le client par l'IA .. 44

Focus : le ciblage client avec mieuxplacer.com 46

DIP 6 : optimiser la distribution omni-canal 48

Focus : Chatbots : le retour d'expérience d'Orange Bank 50

DIP 7 : simplifier les processus de mise en conformité et faciliter la gestion des risques 52

Focus : l'IA au service du KYC et de la conformité dans une banque .. 54

DIP 8 : optimiser le crédit scoring.. 56

DIP 9 : lutter efficacement contre la fraude 58

DIP 10 : vers un dialogue humain-machine empathique 60

2.4. Les conditions d'un déploiement réussi : faciliter la mise à l'échelle et créer les conditions de la confiance 64

DIP 11 : accompagner la transformation des métiers 64

DIP 12 : acculturer et former à l'IA . 68

Focus : formation professionnelle en finance : de la théorie à la pratique à Singapour 70

Focus : une démarche globale pour sensibiliser les collaborateurs de BNP Paribas Securities services à l'intelligence artificielle 72

DIP 13 : mettre en œuvre les grands principes éthiques 74

DIP 14 : lutter contre la discrimination et les biais 78

DIP 15 : expliquer et auditer l'IA 81

DIP 16 : collecter, qualifier, exploiter et partager les données et les connaissances 84

Focus : l'analyse de qualité des données des prix de transactions d'actifs financiers mise en œuvre par Digitalent Consulting 88

DIP 17 : intégrer l'IA dans le SI... 90

DIP 18 : prévenir les cyberrisques en couplant IA et cybersécurité ... 92

2.5. Transposition des bonnes pratiques des autres secteurs au monde de la finance 95

Santé : l'hospitalisation à domicile. 96

Mobilité : l'optimisation du trafic. 97

Smart City : le e-gouvernement... 99
De la maintenance préventive à la maintenance prédictive et proactive..... 100
L'aide au recrutement..... 102
2.6. Points saillants juridiques 103
Propriété des données et des algorithmes..... 103
Propriété des bases de données..104
Propriété des algorithmes..... 105
La Responsabilité 108
2.7. Points saillants organisationnels et techniques..... 114
Faire savoir : communiquer, sensibiliser, former..... 114
Un Comité Numérique au sein du Conseil d'Administration 114
Les aspects organisationnels... 115
L'apprentissage automatique ... 116
Le traitement automatique de la langue..... 116
Les hybridations des technologies IA..... 117
La confiance dans la relation client ..117
Garantir dans le temps la performance, la cohérence et la robustesse de la solution à base d'IA.....118

3. LA BLOCKCHAIN AU SERVICE DE L'INDUSTRIE FINANCIÈRE..... 120
3.1. Préambule 122
3.2. Définitions de la blockchain..... 122
Plusieurs sous-ensembles de technologies distinctes..... 124
Une typologie de blockchains selon la nature, publique ou privée de leur gouvernance 125
Pourquoi utiliser une blockchain. 126
Comment ça marche : l'exemple du bitcoin 126
3.3. La crypto-économie..... 128
DIP 19 : favoriser la recherche sur la crypto-économie 134
DIP 20 : développer les ICO (Initial Coin Offering) en protégeant l'investisseur..... 138
Focus : les principes de valorisation des ICO 141
DIP 21 : sécuriser les portefeuilles numériques et adapter les fonctionnalités de conservation des crypto-actifs 143
3.4. Écosystème et plateformes de place 145
DIP 22 : identifier et décliner les bonnes pratiques de consortia pour développer des solutions de place.....145
Focus : le projet MADRE, blockchain de la Banque de France pour le registre des identifiants créanciers SEPA : les facteurs de succès 148
L'application de la blockchain à l'industrie de l'assurance 150
Recommandation sur l'interopérabilité des blockchains..... 153
3.5. Les transformations portées par les Digital Ledger Technologies (DLT).....154
L'efficacité opérationnelle 154
DIP 23 : déployer l'utilisation de la blockchain pour les mouvements internationaux 155
DIP 24 : création d'un crypto-euro propre à la zone euro pour les paiements de gros et de détail 158
DIP 25 : développer un modèle standardisé basé sur les smart contracts et appliqué aux transactions boursières 161
3.6. L'optimisation du partage de l'information entre acteurs 163
DIP 26 : utiliser la blockchain pour gérer l'identité et l'authentification 163
DIP 27 : améliorer la connaissance client (KYC) en créant une infrastructure de place..... 167

DIP 28 : la traçabilité appliquée au commerce international (trade finance) 170
Focus : retour d'expérience de grandes banques françaises dans le financement du commerce international et le crédit documentaire 172
3.7. Enjeux réglementaires..... 173
Dispositions réglementaires impactées par la technologie blockchain 173
Une réglementation adaptée à l'innovation (compétitivité) 183
L'adéquation des règles fiscales et comptables 185
3.8. Conclusion 187
Annexes..... 189
Annexe 1. Glossaire..... 189
Annexe 2. Liens pour approfondir le sujet 190
Annexe 3. Benchmark des solutions blockchain 190
Annexe 4. Benchmark de quelques solutions blockchain 191
Annexe 5. Textes « Enjeux réglementaires » 192

4. LES TECHNOLOGIES QUANTIQUES AU SERVICE DE L'INDUSTRIE FINANCIÈRE..... 194
4.1. Introduction 196
4.2. Thématique « Informatique quantique »..... 198
Les applications de l'informatique quantique 203
Les principaux algorithmes utilisés en informatique quantique et applications correspondantes en finance 206
4.3. Thématique « Sécurité des communications à l'ère de l'ordinateur quantique » 210
Cryptographie post-quantique : standardisation et développements industriels..... 211
Focus : le point de vue de Michele Mosca 213
Focus : le cas bitcoin 214
4.4. Thématique « Communications sécurisées quantiques »..... 216
La distribution quantique de clés (Quantum Key Distribution) - QKD..216
Les réseaux quantiques sécurisés..... 218
4.5. Thématique « Hardware »..... 220
Hardware de l'ordinateur quantique 220
Hardware des communications quantiques..... 225
4.6. Thématique « Ingénierie logicielle et outils de développement » 227
4.7. Thématique « Conduite du changement, nouveaux métiers, formation, éducation et enjeux réglementaires, juridiques et éthiques » 228
Annexes..... 231
Annexe 1. Pour aller plus loin ... 231
Annexe 2. Les acteurs en cryptographie 231
Annexe 3. Les grandes étapes du développement d'un internet quantique ..232
Annexe 4. Hardware..... 233

CONCLUSION 238
Synergie entre les trois technologies et perspectives 240
1. Synergie intelligence artificielle et blockchain 240
2. Synergie intelligence artificielle et technologies quantiques..... 241
3. Synergie blockchain et technologies quantiques 241
Conclusion..... 243

RÉPERTOIRE DES ENTREPRISES..... 246

REMERCIEMENTS 288





Introduction

1. introduction

1.1 LES OBJECTIFS

Ce livre blanc a identifié trois technologies permettant aux métiers de la finance d'accélérer leur transformation numérique voire de changer d'échelle : l'intelligence artificielle, la blockchain et les technologies quantiques (figure 1).

Depuis quelques années, l'IA est entrée dans une nouvelle ère grâce à la multiplication de jeux de données, à la recherche algorithmique et au décuplement des puissances de calcul. Les applications, tirant profit des masses de données désormais produites par l'économie, se multiplient et touchent à toute la chaine de valeur de la finance. Ce potentiel est abordé dans le chapitre dédié à cette première technologie.

Grâce à ses qualités de transparence et de sécurité, la blockchain va devenir un incontournable de l'industrie financière. Comme le souligne le chapitre qui lui est dédié, même si cette technologie est aujourd'hui essentiellement associée aux crypto-monnaies, elle peut aussi s'appliquer à bien d'autres domaines.

Enfin, un des atouts de l'informatique quantique est de pouvoir résoudre des questions insolubles pour les ordinateurs d'aujourd'hui. Il s'agit par exemple de problèmes de nature exponentielle dont la complexité augmente avec la dimension des données à traiter. C'est pourquoi, même si elles ne sont pas au même niveau de maturité que les deux premières,

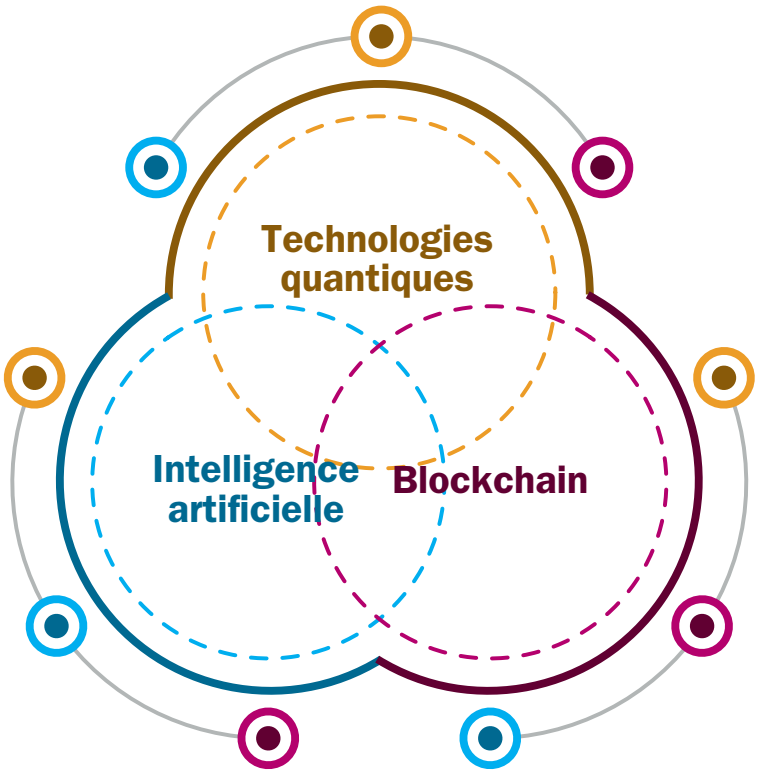


Figure 1 : les 3 technologies clés à fort impact pour l'industrie financière

ces technologies sont étudiées dans ce livre blanc.

Mais **comment maximiser leur impact sur l'industrie financière de demain ?** Pour répondre à cette question et après avoir établi un premier diagnostic des besoins et des opportunités de développement offerts par ces technologies, ce document propose des Domaines d'Innovation Prioritaires (DIP), générateurs de croissance et d'emplois (figure 2).

Mais qu'est-ce qu'un DIP ? C'est un sujet sur lequel l'innovation permettra d'améliorer d'ici cinq à dix ans la compétitivité de l'industrie française de la finance, grâce à l'émergence de réponses innovantes aux enjeux actuels et à venir. Cependant, la plupart des algorithmes quantiques d'aujourd'hui ne sont pas encore exécutables sur les ordinateurs quantiques disponibles ni même sur des simulateurs à base d'ordinateurs traditionnels.

C'est pourquoi seules les technologies d'IA et de blockchain ont donné lieu à des DIP, les technologies quantiques restant plus prospectives.

À la publication du livre blanc, le Pôle FINANCE INNOVATION mettra en place des appels à projets auprès de l'écosystème de la filière finance pour développer et mettre en œuvre ces DIP.

L'étude des limites et des opportunités de ces nouvelles technologies a été réalisée avec une attention particulière à la transformation des métiers, l'éthique et la définition des DIP induits.

Comme ces technologies concernent aussi aujourd'hui d'autres industries, une analyse des retours d'expériences a permis d'identifier de nombreuses synergies. Citons, par exemple, l'intelligence artificielle de confiance, validée, qualifiée, certifiée et éthique, condition nécessaire au déploiement de cette technologie dans le monde de la finance, mais aussi dans les domaines de la santé, des transports, de la sécurité ou de la défense.

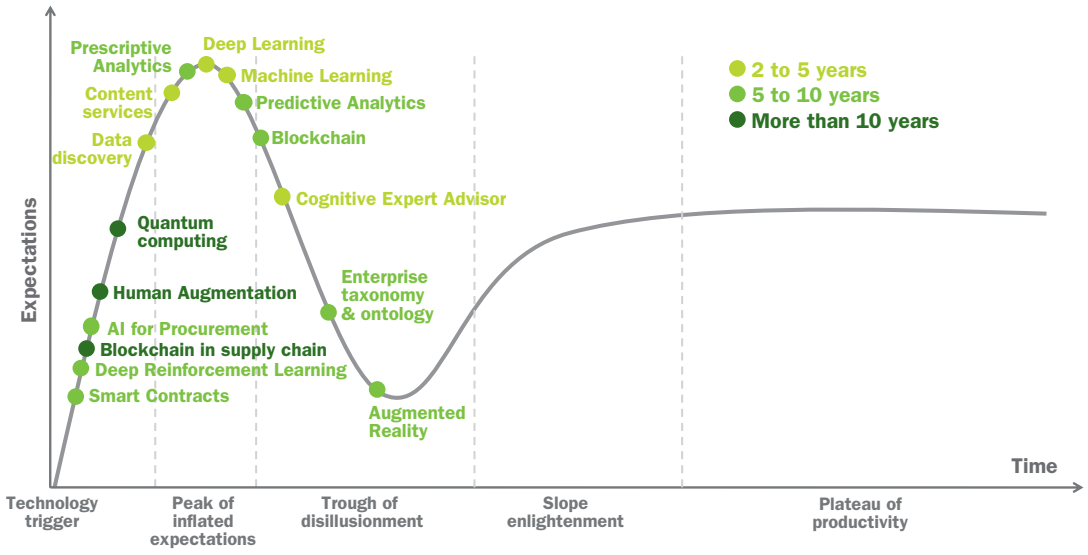


Figure 2 : le Gartner Hype Cycle 2017 des technologies émergentes, appliquées au monde de la finance

Enfin, une dernière remarque concerne le poids de la réglementation qui demeure très important dans la banque et l'assurance. Cette réglementation interdit, par exemple, que certaines décisions soient prises par des systèmes totalement automatisés, exigeant donc l'intervention humaine d'un conseiller[1]. En conséquence, il existe une certaine dichotomie entre les sujets internes à l'organisation où une assez grande liberté d'action est possible et les sujets externes en relation avec le client, où l'encadrement est plus contraint.

La démocratisation d'Internet, du mobile et des technologiques digitales a permis l'émergence de nouveaux acteurs innovants susceptibles de compléter et concurrencer l'offre des acteurs traditionnels de services financiers. La transformation digitale reste un enjeu majeur pour optimiser l'expérience client, transformer le business model et automatiser les processus métiers.

1.2. LA DÉMARCHE

Ce livre blanc est avant tout une aventure collective lancée en décembre 2017. Elle a donné la parole à des cadres issus de l'écosystème de la finance et des experts de ces technologies : fintechs et startups, chercheurs et académiques reconnus, grands groupes financiers et industriels, cabinets de conseil, éditeurs/intégrateurs de logiciels et représentants du Pôle de Compétitivité FINANCE INNOVATION.

Plus de 250 participants ont contribué aux sept sous-groupes de travail à travers 56 réunions de décembre 2017 à octobre 2018.

Mené en mode projet, se focalisant sur l'IA, la blockchain et les technologies quantiques, ce livre blanc a pour objectif d'identifier les DIP de la prochaine décennie, faisant ainsi émerger une vision prospective pour l'industrie financière, ce qui a été possible grâce à des débats riches et

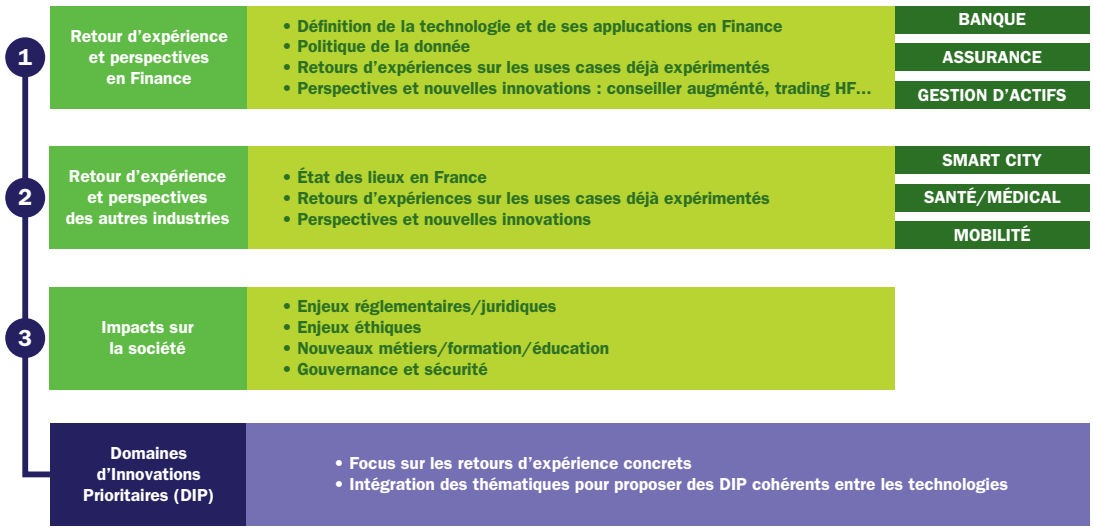


Figure 3 : démarche suivie

1. Dans la suite du document, les termes «conseiller» et «client» sont neutres : il faut comprendre «conseillère et conseiller» et «cliente et client».

des conversations animées dans un cadre libre et ouvert abordant les thématiques décrites en figure 4.

Ainsi, la réflexion et les analyses menées par les différents groupes de travail ont été largement nourries par des exemples opérationnels (cas d'usage) issus du domaine de l'industrie financière, mais aussi d'autres secteurs afin d'identifier la valeur ajoutée de leur introduction dans la finance.

1.3. LA CIBLE

Ce livre blanc a vocation à être diffusé dans l'industrie financière et les autres secteurs de l'économie pour lancer de nouveaux projets collaboratifs répondant aux DIP identifiés. Ces derniers ont une portée majeure, car ils concernent :

- les fintechs qui proposeront des solutions innovantes ;
- l'ensemble des métiers de la banque et de l'assurance ;
- les experts techniques qui souhaitent contribuer à la compétitivité de l'industrie financière.

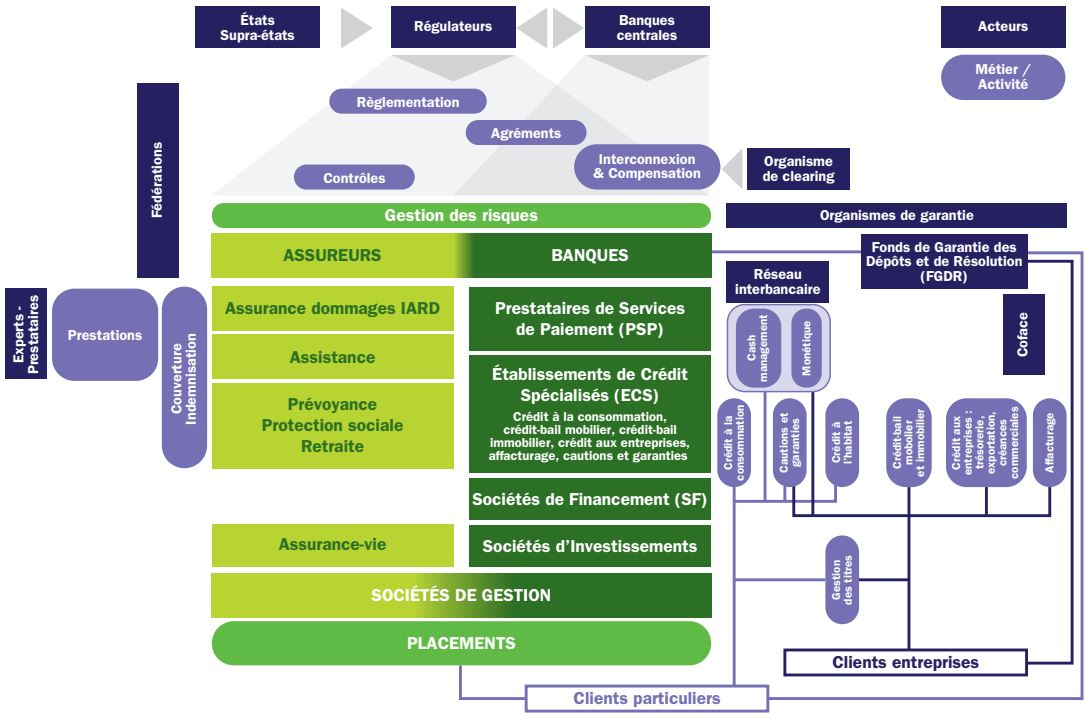


Figure 4 : cartographie des acteurs de la finance

1.4. LE COMITÉ DE PILOTAGE

Pilotage général du Livre blanc

Direction du Livre blanc

- **Bernard GAINNIER**
  Président, FINANCE INNOVATION
- **Joëlle DURIEUX**
  Directrice générale, FINANCE INNOVATION

Pilotage des groupes de travail et coordination des travaux

- **Sarah LAMOUDI**
  Responsable du pilotage du Livre blanc, experte IA/blockchain, FINANCE INNOVATION
- Avec la participation de **Patrick SEIFERT** (Senior advisor, Chappuis Hader & Co) et **Mehdi SENTISSI** (chargé de mission FINANCE INNOVATION).

Les comités de pilotage des groupes de travail

Intelligence artificielle

- **Bertrand BRAUNSCHWEIG**
  Directeur de coordination du programme national de recherche en intelligence artificielle (ex-Directeur du centre de recherche INRIA Saclay)
- **Juliette MATTIOLI**
  PhD, Expert sénior en IA, Thales
- **Hamza DIDARALY**
  Président IA pour tous.com, CEO A.I Ambassador
- **Jean-Gabriel GANASCIA**
  Professeur à Sorbonne Université
- **Gilles PAGES**
  Professeur à Sorbonne Université
- **Benoît SPOLIDOR**
  Head of Artificial intelligence, Sopra Steria

Blockchain

- **Cathie-Rosalie JOLY**
  Avocat Associé, Bird & Bird
- **Alexandre STACHTCHENKO**
  co-fondateur et directeur général Blockchain Partner – Président La Chaintech
- **Philippe DENIS**
  Head of Blockchain Lab & CDO, BNPP Securities Services
- **Marc ALAURANT**
  Marketing-Innovation, FinTechs, Blockchain, BNP Personal Finance
- **Muriel FAURE**
  Présidente Commission Recherche & Innovation, Association Française de la Gestion Financière (AFG)
- **Alain ROSET**
  La Poste, Perspective/Expert Blockchain
- **Sajida ZOUAHRI**
  Doctorant en Blockchain – Orange Labs, Blockchain architect – Consensys New York

Technologies quantiques

- **Pascale SENELLART**
  Professeur CNRS, Univ. Paris Sud, Univ. Paris Saclay, C2N
- **Maud VINET**
  Logic Technologies manager, CEA Leti
- **Eleni DIAMANTI**
  Chargée de Recherche, CNRS Université Pierre et Marie Curie
- **Adrien FACON**
  Directeur des programmes «AI for Embedded Cyber-Security» et «Cyber-Protection», SECURE-IC
- **Alexia AUFFEVES**
  Directeur de recherche CNRS
- **Philippe DULUC**
  CTO big data & security Atos
- **Georges UZBELGER**
  AI/Advanced Analytics Solution & Quantum Computing Leader, IBM France
- **Olivier SALOMON**
  Tech & Innovation, leader IT Lab - Allianz

1.5. LES ENJEUX DE LA FINANCE

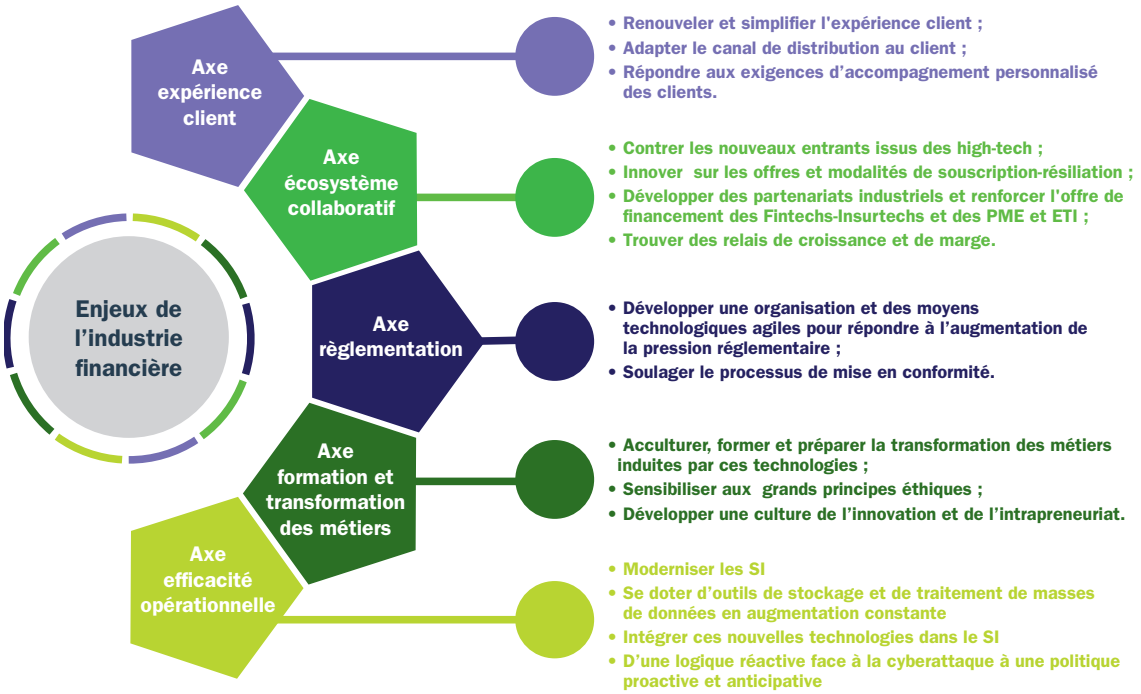
L'introduction de ces trois innovations majeures (intelligence artificielle, blockchain et technologies quantiques) représente à terme un véritable changement de paradigme pour les métiers de la finance, et ce dans tous leurs aspects qui constituent autant d'enjeux.

Tout d'abord, c'est une expérience client totalement refondue que la banque et l'assurance délivreront demain à travers des services hyper-personnalisés. Traitée et analysée par l'IA, la masse gigantesque de données disponibles leur permettra de connaître parfaitement chacun de leurs clients et de leur proposer des contrats individualisés et adaptés à leurs besoins. Aux côtés du conseiller lors de ses entretiens clients, des assistants virtuels (*chatbots*, agents conversationnels, *robo-advisors*) suggéreront en temps réel et au fil des échanges des choix d'investissement personnalisés en fonction de la situation et des projets de chacun.

En «augmentant» le conseiller ainsi débarrassé des taches à faible valeur ajoutée, l'IA lui permettra de se concentrer pleinement sur l'écoute client et l'interaction avec l'humain… Ce changement dans les tâches du collaborateur va impliquer une évolution vers de nouvelles méthodes d'organisation plus agiles, plus proches de celles en vigueur dans les startups. Cela conduira également à une nécessaire redéfinition des métiers et des emplois dans la finance, historiquement très segmentés…

Bien sûr, de nouvelles compétences techniques seront recherchées, mais ce sera aussi le cas des compétences sociales et émotionnelles (empathie, leadership, créativité…) plus difficilement automatisables. De quoi réinventer complètement les domaines de la gestion des talents et de la formation…

Ces profondes transformations internes sont à mettre en regard du bouleversement des marchés de la finance et de son business model que représente l'émergence de la blockhain.



Cette nouvelle technologie, accompagnée par les crypto-actifs et les *smarts contracts*, qui permet de transférer des actifs entre individus en toute sécurité, sans intermédiaire ni tiers de confiance, constitue pour la banque une véritable disruption. Le marché des mouvements financiers internationaux s'en verra totalement modifié, de même que surgiront de nouveaux modèles d'affaires et de nouveaux acteurs, sans parler du gisement que représentent les 1,7 milliard de personnes encore non bancarisées dans le monde…

L'efficacité opérationnelle, quant à elle, va fortement s'améliorer avec de meilleurs ciblages et scorings des clients qui sont un des atouts majeurs de l'IA, comme le contrôle optimisé du risque avec l'envoi d'alertes automatiques afin d'intervenir sur toute situation financière jugée critique. Parallèlement, la lutte contre la fraude sera plus performante avec une KYC renouvelée et des systèmes IA qui montreront, à terme, des capacités de détection supérieures.

Enfin, en matière de réglementation, les enjeux sont ceux de l'intégration de l'IA au cadre encore récent de la RGPD, de la responsabilité partagée entre humain et machine et des multiples questions éthiques qui ne manqueront pas de se poser…

1.6. BIENVENUE CHEZ VOUS EN 2030

Le réveil d'Alice sonne : il est programmé pour la réveiller lorsque son cycle de sommeil lui permet d'optimiser ses performances tout au long de sa journée. Comme tous les jours au lever, Alfred, son fidèle assistant personnel holographique, s'adresse à elle via le haut-parleur directionnel de sa chambre. Il lui présente la synthèse des informations du jour, les actualités, les flux de son réseau social sécurisé (qui préserve ses données dans un *datalake* quanticrypté personnel), son planning de la journée et l'état de ses dépenses.

En se connectant rapidement à son espace individuel e-santé, Alice vérifie qu'elle est en excellente forme (les capteurs connectés autour de son lit analysent son sommeil, ses paramètres vitaux et son état psychologique), ce qui lui permet de conserver les 30 % de réduction sur son assurance santé et d'économiser sur l'accès à la salle de sport qu'elle apprécie tant.

D'autres qu'Alice préfèrent que leur assistant personnel soit matérialisé par un robot humanoïde se déplaçant avec eux, mais Alice préfère la voix et l'affichage de la vue virtuelle d'Alfred qui la suit dans ses déplacements à travers chaque pièce de son appartement.

Auparavant, Alfred a récupéré, analysé et filtré l'ensemble de ses flux : actualités, réseaux sociaux, mais aussi mails, messages personnels, confirmation et factures de commerçants, notifications d'administrations, etc. de même que les transactions, informations et recommandations commerciales de ses banques et établissements financiers. Ayant appris des préférences et du comportement d'Alice, Alfred est en capacité de hiérarchiser et de prioriser les informations restituées et même de proposer des actions courantes. Si l'attention d'Alice est mobilisée par autre chose, comme se servir un café ou répondre à un appel, il s'interrompt automatiquement et s'adapte à son humeur comme un véritable majordome, par exemple si Alice est pressée.

Les informations envoyées par la banque d'Alice proviennent non pas de Marc, son conseiller bancaire, mais de l'assistant automatisé de Marc, Alphonse. Ce dernier a lui aussi passé en revue l'ensemble des informations du jour et a déterminé, en fonction du profil d'Alice, de l'historique de ses événements et de l'analyse de son environnement quelles informations adresser et quelles recommandations effectuer. Ainsi, Alice a dit à Marc que son fils partait aux USA pour ses études : l'information a été immédiatement prise en compte et des éléments sur les placements en zone dollar lui ont été envoyés, de même qu'une proposition de souscription d'un compte multidevises et crypto-monnaies.

Au sein de l'agence bancaire d'Alice, Alphonse, l'assistant automatisé de son conseiller est aussi capable de consolider et comparer l'ensemble des informations et propositions envoyées aux clients pour vérifier au titre de la conformité que ne se créent pas de biais ou d'inégalités dans la distribution des produits et que ceux-ci sont adaptés à leurs profils, et ce en relation avec le contrôle l'ensemble du système bancaire.

L'analyse comportementale possible grâce au logiciel d'Alfred lui permet de déceler une certaine impatience chez Alice. Alfred arrête ainsi sa présentation et écoute ses instructions : *« Je souhaiterais acheter un appartement. J'en ai regardé quelques-uns ces derniers temps ; base-toi sur ce que j'ai consulté et fais-moi des propositions. Je suis aussi intéressée par les investissements dans un fonds pour les startups de l'Edtech que tu m'as présenté dans le système éducatif aux USA, lui dit Alice. Prends rendez-vous avec Marc que l'on puisse en parler ».*

Aussitôt, son conseiller Alfred déclenche différentes actions :

- une recherche actualisée des appartements à vendre se fondant sur les similitudes des recherches précédentes effectuées par Alice en optimisant ses paramètres de vie (proximité de magasins et services, temps et moyens de transport, etc.) et sur une simulation de ses capacités financières d'acquisition et de la marge de négociation généralement applicable sur les prix affichés pour des biens équivalents,
- une fois les biens identifiés, une vérification de ceux-ci est effectuée en interrogeant les registres partagés des immeubles historisant les opérations de maintenance, la vie sociale et les données des capteurs intégrés,
- l'initialisation de la négociation pour que le prix du bien envisagé corresponde aux capacités financières d'Alice (ou aux paramètres financiers qu'elle lui a communiqués) est lancée par des échanges automatiques entre les agents respectifs du vendeur et de l'acheteur pour déterminer les zones d'accord possibles,
- Alfred va ainsi procéder à une analyse des offres et des taux disponibles sur le marché et en préparer une synthèse pour Alice avant sa négociation avec Marc,
- une demande de prise de rendez-vous avec Marc est adressée à Alice, en fonction de ses disponibilités et en en indiquant le motif.

Marc, le conseiller bancaire d'Alice, a lui aussi commencé sa journée avec une synthèse proposée par son assistant virtuel. Alphonse le décharge de toutes les tâches administratives, filtre ses mails et ses flux et optimise ses communications et son

emploi du temps. Comme chaque matin, Alphonse lui a présenté une synthèse de sa journée en classant ses activités par priorité dans son tableau de bord personnel. Il lui prépare également des mémos de présentation pour chacun de ses rendez-vous de la journée. Marc rencontre ses clients dans sa voiture autonome où un bureau lui a été spécialement installé. Alphonse lui permet d'optimiser ses déplacements qu'il calcule de façon anticipée (grâce à un algorithme dédié aux habitudes de circulation) et réajuste en temps réel en prenant en compte l'état du trafic.

Le rendez-vous sollicité en dernière minute par Alfred a modifié quelque peu l'emploi du temps de Marc. Toutefois, ce rendez-vous est optimisé par Alphonse afin que Marc ne fasse qu'un léger détour dans ses trajets pour assurer cet entretien avec Alice qui a souhaité rencontrer Marc au e-Café à côté de chez elle. Une fois le rendez-vous confirmé à Alice, Alphonse produit une synthèse de l'historique de la relation client avec Alice qu'il communique à Marc pendant le trajet ainsi que l'objet du rendez-vous et une simulation des différentes propositions de prêt que Marc pourrait lui faire.

Dès qu'Alice franchit le seuil de la porte du e-Café, sa boisson préférée se met en route, car elle a été reconnue automatiquement grâce à son identité numérique. En effet, Alice a défini son profil lors d'une visite précédente au e-Café, par le biais de listes des données collectées, de leur durée de conservation, de traitements autorisés et d'enseignes pouvant y accéder, ainsi que des modalités techniques de détection (*smartphone*, biométrie faciale ou digitale, saisie d'un code mémorisé ou de vérification unique envoyé, etc.). Elle peut notamment à tout moment modifier ces paramètres, retirer les droits d'utilisation accordés, supprimer des informations ou décider de transmettre ces données à des tiers.

Pas besoin d'utiliser sa carte de paiement, le règlement est instantanément effectué en mode « *paiement transparent* » à partir de son compte de paiement ou de son *wallet* de crypto-cash émis et conservé en ligne dans une blockchain par la Banque Centrale et référencé dans ses paramètres d'identité numérique. Alice est un peu plus tendue que d'habitude, car, même si elle se réjouit de son projet d'acquisition, cela n'en demeure pas moins une étape importante dans sa vie. L'IA du commerçant analyse le comportement d'achat de ses clients et peut demander une validation supplémentaire s'il détecte une anomalie. Dans le cas d'Alice, la première analyse du comportement a conduit à une interrogation qui amène l'IA à effectuer une deuxième analyse et demander une validation complémentaire.

Finalement, Alice voit la voiture de Marc se garer, ce qui dissipe tout doute dans son esprit concernant son projet. Le comportement d'Alice est bien normal, estime l'IA qui valide donc la transaction en crypto-cash. Depuis que la Banque Centrale distribue un kit d'accès logiciel à sa blockchain qui permet aux fournisseurs de moyens de paiement de faire preuve de la plus grande créativité dans les types et les cinématiques de paiement (collier, carte, application mobile…), le crypto-cash a totalement remplacé les espèces. La réglementation impose cependant que les caractéristiques d'anonymat et d'affichage du montant détenu soient respectées.

Le e-Café, qui souhaite accéder à l'historique de consommation d'Alice à des

fins statistiques et commerciales, lui demande préalablement son consentement pour l'utilisation de ses informations via l'application de paiement en échange de la gratuité pendant un mois de toutes les consommations qu'elle commandera dans le réseau e-Café. Alice, bien que tentée par l'offre, mais allergique à tout type de sollicitation commerciale, refuse.

Tout en dégustant son excellent cappuccino, elle monte dans le véhicule autonome salon de son conseiller. Pendant le trajet, elle a le temps de finaliser la mise en place de son achat immobilier et d'en savoir plus sur les crypto-actifs de l'EdTech. Concernant l'achat de son bien, Alice se laisse séduire par les taux très préférentiels de Marc. Elle donne son pré-accord, qui nécessitera une deuxième signature électronique après le délai légal de réflexion.

Cette acceptation déclenchera automatiquement le contrat de prêt qui sera transmis au notaire afin de régulariser l'achat de son nouvel appartement. Concernant les crypto-actifs de l'EdTech, Marc lui confirme qu'ils sont représentatifs de droits sur les revenus du panier de cours qui lui est proposé. Les crypto-actifs sont enregistrés dans une blockchain et dès qu'un étudiant s'inscrit et paye pour ses cours, un programme automatique « *smart contract* » lui reverse une quote-part déterminée de la transaction, ce qui permettra de financer les dépenses quotidiennes de son fils. Convaincue, Alice décide d'investir, donne son accord à Marc avec qui elle échange une très humaine et énergique poignée de main avant de repartir, pleinement satisfaite de son rendez-vous en cette belle journée de l'année 2030…





L'intelligence artificielle au service de l'industrie financière

2. L'intelligence artificielle au service de l'industrie financière

Le secteur de la banque, de la finance et de l'assurance va, comme les autres secteurs de l'économie, bénéficier des progrès de l'intelligence artificielle (IA). Bien qu'il ne fasse pas partie des cinq domaines identifiés dans le rapport de la mission Villani[2], il a été examiné en 2017 dans le cadre de la réflexion #FranceIA[3] et a fait l'objet de plusieurs études, comme celle de France Stratégie publiée en avril 2018[4] dont un chapitre est consacré aux impacts dans le secteur bancaire. D'autres contributions abordent l'IA dans les services financiers, comme le rapport du cabinet Roland Berger de juin 2017[5] et l'étude Athling de décembre 2017[6]. Enfin, le rapport du groupe Malakoff-Médéric de mars 2018[7] se focalise sur l'évolution des emplois et des compétences.

En complément, ce livre blanc met l'accent sur le reste à réaliser au travers de Domaines d'Innovation Prioritaires (DIP) visant à maximiser les bénéfices de l'IA pour la profession, en prenant notamment en compte ses aspects sociaux afin que les gains de l'innovation profitent à tous et à chacun.

Un point saillant de ce travail est l'universalité des applications de l'IA : tous les métiers de la banque, de la finance et de l'assurance sont concernés. Que ce soit en *front office* face au client ou en *back office* dans la préparation des contrats, dans l'établissement de notes de synthèse ou encore en automatique par le biais d'agents conversationnels dialoguant avec le client, les technologies d'IA peuvent être mises à profit pour fournir des aides à la décision, voire automatiser certaines décisions dans des contextes non critiques.

Pour modérer le propos, il faut aussi constater, au moins au niveau des entreprises françaises, que relativement peu de systèmes à base d'IA sont déjà en production. On compte beaucoup de maquettes, preuves de concepts et démonstrateurs de systèmes à base d'apprentissage dont le passage à l'échelle et le déploiement ne sont pas encore avérés. Citons cependant la technologie CEP[8] (*Complex Event Processing*) à base de règles spatio-temporelles largement déployée pour le trading.

L'offre commerciale existe, mais peu de grands groupes ont implémenté des solutions corporate. L'expérience du Crédit Mutuel, utilisant le produit Watson d'IBM pour filtrer et traiter les courriers électroniques,

2. Villani, C. et coll. (2018) « Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne », téléchargeable sur www.aiforhumanity.fr.
3. Ackerman, N. et coll. (2017) « FranceIA : Conclusions complètes des groupes de travail », www.economie.gouv.fr/files/files/PDF/2017/Conclusions_Groupes_Travail_France_IA.pdf.
4. France Stratégie (2018), « Intelligence artificielle et travail », www.strategie.gouv.fr/publications/intelligence-artificielle-travail.
5. Doucet L. (2017), « Automation in Financial Services », www.adetem.org/club-adetem-bfa-20062017.
6. Athling (2017), « L'intelligence artificielle dans la banque : emplois et compétences », www.observatoire-metiers-banque.fr.
7. Malakoff Médéric (2018) « Intelligence artificielle et capital humain : quels défis pour les entreprises ? », www.lecomptoirmm.com.
8. Le traîtement des événements complexes, ou CEP, est une méthode à base de règles (IA symbolique) permettant de suivre et d'analyser (traiter) des flux d'informations sur des événements, et d'en tirer une conclusion (une alerte). C'est l'une des technologies utilisées dans le domaine des échanges et en particulier dans le secteur des services financiers.

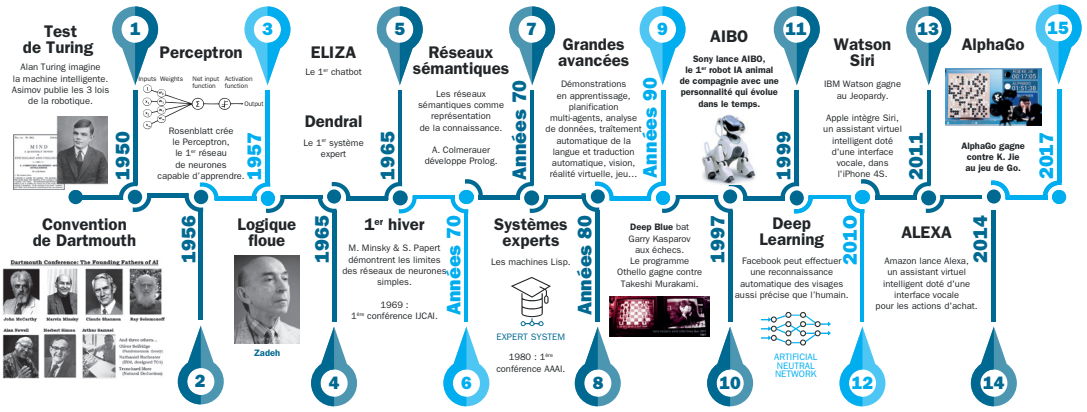


Figure 5 : un bref historique de l'intelligence artificielle (Source Thales 2017)

reste encore rare dans notre pays. Il est donc particulièrement important pour les entreprises du secteur de se saisir de ces nouvelles opportunités.

Dans ce chapitre, les 18 DIP sont d'abord organisés par technologies et appliqués aux enjeux métiers. S'ajoutent ensuite des DIP « transverses » dont la fonction principale est d'établir la confiance entre l'utilisateur et le système artificiel et de faciliter son déploiement. Ces DIP transverses traitent aussi de l'éthique, du juridique, des compétences et de la formation, capitalisant sur l'expérience d'autres secteurs industriels comme la santé, le transport et mobilité, la ville intelligente.

2.1 UN PEU D'HISTOIRE

L'intelligence artificielle est un champ extraordinairement vaste, mais difficile à définir. L'expression « intelligence artificielle » fut adoptée au Congrès de Dartmouth en 1956 pour désigner le domaine de reut adoptée au Congrès de Dartmouth en 1956 pour désigner le domaine de recherche qui s'ouvrait alors. La définition la plus simple de l'IA est celle que donne la mission Villani[9] :

« Une intelligence artificielle est un programme informatique visant à effectuer, au moins aussi bien que des humains, des tâches nécessitant un certain niveau d'intelligence. »

Grâce aux progrès considérables de la microélectronique, à la puissance de calcul et à l'accès à des quantités massives de données, l'IA vit aujourd'hui un renouveau (voir figure 5).

Cette discipline est redevenue visible ces dernières années, sous la double impulsion de résultats très médiatisés – de la victoire de Deep Blue sur Gary Kasparov aux échecs en 1997 à celle d'Alpha Go sur le grand maître Lee Seedol au jeu de Go en 2016, en passant par la victoire de Watson à Jeopardy en 2011 ou la victoire de Psibernetix en simulation de combats aériens contre les meilleurs pilotes américains en 2016 – et d'avancées

9. Villani, C. et coll. (2018) « Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne », téléchargeable sur www.aiforhumanity.fr.

significatives sur des problèmes jugés difficiles comme la reconnaissance d'image et de la parole, la traduction automatique ou l'analyse prédictive à partir de données massives.

2.2. QUELQUES CHIFFRES SUR LE MARCHÉ DE L'IA

« La technologie de l'IA (intelligence artificielle) est maintenant sur le point de transformer tous les secteurs, comme l'électricité il y a 100 ans. Entre maintenant et 2030, cela créera environ 13 billions de dollars de croissance du PIB. Bien que cela ait déjà créé une valeur considérable dans les entreprises technologiques de pointe telles que Google, Baidu, Microsoft et Facebook, une grande partie des vagues supplémentaires de création de valeur ira au-delà du secteur des logiciels. »

Andrew Ng
Professeur associé au Département de science informatique de l'Université Stanford

C'est ainsi qu'Andrew Ng, dans sa récente publication[10] estime le marché de l'IA. Pour étayer ce propos, quelques données chiffrées cernant les enjeux business de cette discipline en plein essor :

- 300 startups IA en France ;
- 278 millions d'euros[11] de levée de fonds en 2017 pour celles-ci ;
- 1,5 milliard d'euros, montant d'investissement annoncé par le gouvernement français sur la période 2018–2022 ;
- Le marché français de l'IA affiche une dynamique assez forte avec une croissance[12] trimestrielle moyenne de l'ordre de 80 % entre T2 2016 et T2 2017 ;
- 18 masters dispensant des formations IA[13] et 5300 chercheurs en IA[14] en France ;
- 90 milliards de dollars[15] pour le marché mondial de l'IA d'ici 2025 ;
- 1730 jeunes pousses consacrées à l'IA dans 70 pays[16] avec une levée de fonds moyenne de 7,5 millions de dollars par entreprise ;
- La DARPA[17] a annoncé, via son programme AI Next en 2018, l'investissement de 2 milliards de dollars sur les cinq prochaînes années.

Les attentes et les investissements les plus importants viennent aujourd'hui des secteurs de la finance, de la santé, de la défense/sécurité et du transport[18]. Dans l'industrie financière, outre l'utilisation de l'IA à des fins d'automatisation et d'amélioration de processus opérationnels (comme le contrôle de conformité des documents), les investissements d'aujourd'hui touchent majoritairement les domaines de marketing et de la connaissance client.

10. Andrew Ng, Professeur associé au département des sciences informatiques de l'Université de Stanford : AI Transformation playbook How to lead your company into the AI era, december 13, 2018.
11. fintech-mag.com/marche-de-intelligence-artificielle.
12. Tracxn.
13. Rapport France IA remis au gouvernement le 21 mars 2017.
14. Rapport France IA remis au gouvernement le 21 mars 2017.
15. www.tractica.com/research/artificial-dintelligence-market-forecasts.
16. www.slideshare.net/nathanpacer/venture-scanner-ai-report-q1-2017.
17. DARPA : Defense Advanced Research Projects Agency (Agence pour les projets de recherche avancée de défense) est une agence du département de la Défense des États-Unis chargée de la recherche et développement des nouvelles technologies destinées à un usage militaire.
18. «Pour une intelligence artificielle maitrisée, utile et démystifiée», 19/07/2017 Rapport d'information de l'OPECST.

2.3. DES TECHNOLOGIES AU SERVICE DES MÉTIERS DE L'INDUSTRIE FINANCIÈRE

Dans la suite du document, on utilisera les concepts de « donnée », « information » et « connaissance ». La **donnée** est un élément brut qui n'a pas encore été interprété et mis en contexte. C'est le résultat direct d'une mesure qui peut être collectée par un outil, par une personne ou être déjà présente dans une base de données. Il y a donc des données numériques, symboliques, textuelles, logiques... Une **information** est une donnée intelligible, qui prend un sens. Une information est donc par définition une donnée interprétée. En d'autres termes, la mise en contexte d'une donnée crée de la valeur ajoutée pour constituer une information. La **connaissance** est le résultat d'une réflexion sur les informations analysées. À la différence de l'information, la connaissance est partagée et s'appuie sur un référentiel collectif. Mais attention, des informations peuvent être communiquées sans pour autant devenir des connaissances. Il faut alors les accompagner de leur référentiel puisque celui-ci ne sera pas partagé (non implicite). Ainsi, la connaissance peut être spécifique à un métier, donc partagée seulement par les experts du métier.

L'IA peut se segmenter en sous-domaines qui ont chacun connu différents succès (figure 6) :

- L'intelligence artificielle dite symbolique[19] ou à base de modèles et de connaissances comme :
  - Le web sémantique et les ontologies ;
  - Les systèmes à base de connaissances incluant les systèmes experts

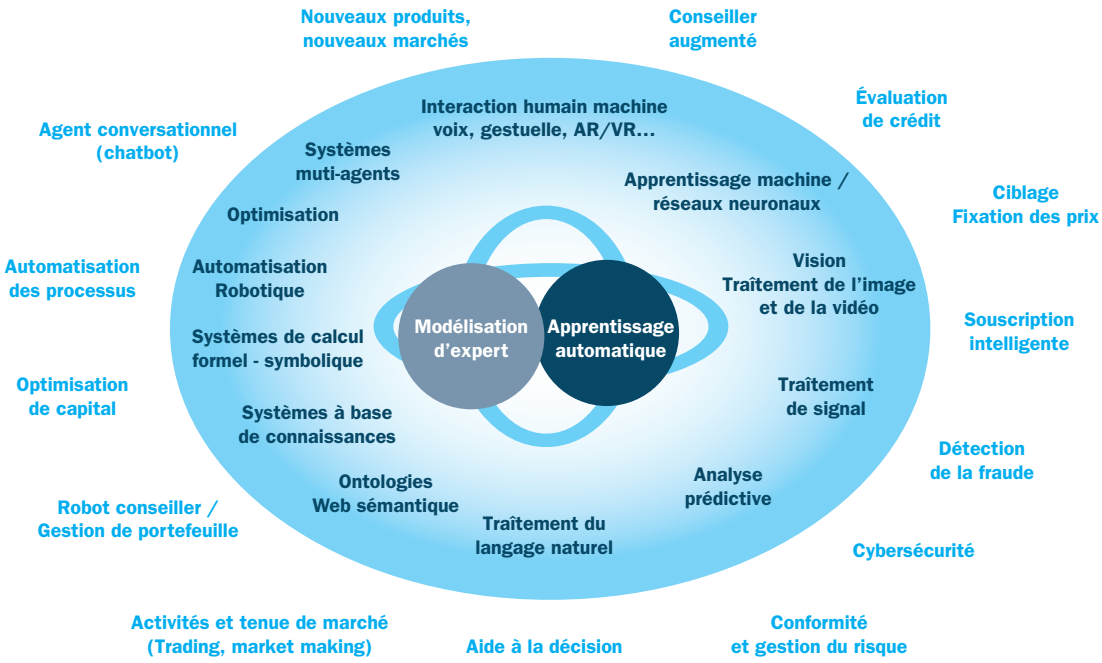


Figure 6 : différentes technologies d'IA applicables au domaine financier

19. L'IA symbolique est aussi appelée en anglais GOFAI pour « Good Old Fashion AI ».

et les systèmes à base de règles ;
- Les systèmes multi-agents ;
- La programmation par contraintes ;
- Les systèmes de calcul formel – symbolique.

- L'apprentissage automatique/réseaux neuronaux supervisé, non supervisé, par renforcement et l'apprentissage profond appliqué :
  - au traîtement du langage naturel,
  - à la vision et au traîtement d'image et de vidéo,
  - au traîtement du signal comme pour le traîtement de la parole ;
  - à la prédiction de séries temporelle…

Enfin, le dialogue et l'interaction homme-machine utilisent de manière combinée ces technologies, en particulier au travers des agents conversationnels ou de la réalité augmentée, la réalité virtuelle…

Les progrès spectaculaires des réseaux neuronaux profonds (*deep learning*), en particulier dans le domaine de la perception sont aujourd'hui mis en avant. Il ne faut cependant pas confondre l'intelligence artificielle avec *l'analytics*. Certes, l'apprentissage automatique est une discipline majeure de l'IA, mais on peut faire de *l'analytics* sans avoir recours à l'intelligence artificielle.

Dans l'industrie financière, les technologies aujourd'hui déployées de RPA (*Robotic Process Automation*) permettent de remplacer certains processus manuels répétitifs et à faible valeur ajoutée par des processus robotisés, et n'utilisent pas ou peu d'IA.

Comme l'IA ne se réduit pas aux réseaux neuronaux ou à l'apprentissage automatique, on parle alors d'IA symbolique, à base de modèles ou de connaissance.

« L'intelligence artificielle offre des techniques d'analyse et de raisonnement nécessaires pour extraire du sens, résoudre des problèmes complexes, et permettre des prises de décisions à partir de données et de connaissances, tandis que la science des données fournit les connaissances nécessaires à l'IA pour continuer à apprendre et à évoluer. »

Juliette Mattioli, AI senior expert
©Thales 2018

Dans la suite du document, quand l'« intelligence artificielle » est mentionnée, il s'agit de l'IA symbolique ou de l'apprentis-

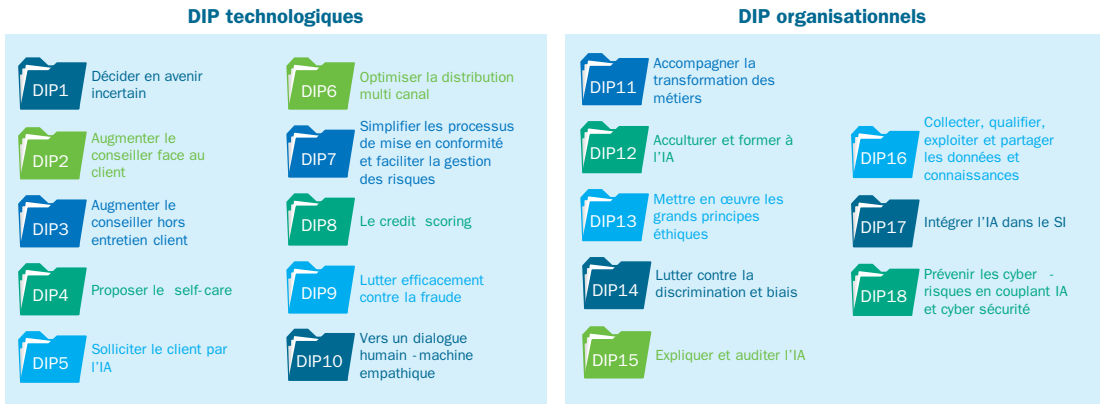


Figure 7 : Les 18 DIP de l'IA au service de l'industrie financière

sage automatique sans distinction. Sinon, les technologies sous-jacentes seront précisées.

Pour identifier les DIP, plus de 30 cas d'usages ont été étudiés et analysés orientés selon les cinq axes suivants :

- La relation client SAV, avec l'apport des agents conversationnels *(chatbots)*, la personnalisation/ultra-personnalisation des offres, le conseillé augmenté…
- L'efficacité opérationnelle incluant la gestion des contrats ou la gestion intelligente des bases documentaires sans oublier la gestion des données…
- L'investissement et le trading algorithmique, l'aide à la décision d'investissement, l'optimisation de portefeuille et la construction de dérivées.
- Les dimensions réglementaires avec un focus particulier sur la gestion du risque et la conformité ;
- La création de nouvelles offres, nouveaux produits et services. Citons par exemple, dans le domaine de l'assurance, la couverture de nouveaux types de risques induits par l'évolution de la matière assurable (comme la voiture autonome).

Les 18 DIP identifiés pour l'intelligence artificielle sont regroupés en DIP technologiques appliqués aux métiers et en DIP transverses liés à la transformation de l'organisation.

DIP 1 : développer et augmenter la capacité décisionnelle en avenir incertain

L'aide à la décision est sans doute l'un des domaines où l'émergence de l'IA apporte un bouleversement majeur, tant sur la nature de l'aide fournie que sur l'échelle temporelle où cette information est susceptible d'être disponible. Elle peut même conduire à un changement de paradigme. Cela concerne tous les métiers de la finance et de l'assurance. Mais qu'est-ce qu'une décision ? C'est le fait qu'un acteur (ou un ensemble d'acteurs) effectue un choix, si possible après réflexion, entre plusieurs solutions pour affronter une situation difficile, résoudre un problème délicat ou répondre à une question complexe. Ces différentes situations permettent de distinguer deux types de décisions : les décisions stratégiques et les décisions opérationnelles.

La décision en avenir incertain, qu'elle soit stratégique ou opérationnelle, prend tout son sens lors d'opérations de gestion d'événements rares ou exceptionnels voire en situation de crise, et cela en raison des bouleversements de l'environnement dans lequel les organisations évoluent. En effet, on ne peut prévoir ni leur forme (krach boursier…) ni le moment précis de leur déclenchement.De plus, la capacité de l'organisation à prendre des décisions justes et rapides est un facteur clé de succès vers l'issue la plus favorable. L'incertitude est alors le cadre de cette prise de décision. Il est impossible d'y échapper. Elle renvoie au fait que les conséquences d'une décision ne sont pas connues à l'avance, ce qui expose le décideur à un risque.

Cependant, le risque encouru peut être quantifiable quand la probabilité d'occurrence des différentes conséquences possibles est objectivement connue à l'avance. On calcule alors la perte encourue en multipliant le montant de la perte éventuelle par la probabilité que se réalise l'éventualité défavorable. Toutefois, l'incertitude devient intrinsèque si les risques ne sont pas objectivement mesurables à l'avance. La rentabilité du financement des investissements par le crédit bancaire et le rendement futur des titres obligataires ou des actions émises en cas de financement non bancaire sont affectés par cette incertitude. De plus, un problème de décision est souvent multicritère. Il se caractérise par la prise en compte explicite de plusieurs objectifs à optimiser simultanément dans l'analyse des préférences, la comparaison des solutions et la détermination d'une ou des solution(s) optimale(s). Les problèmes induits varient selon la question posée. On peut distinguer les problèmes de choix où l'on cherche à déterminer les meilleures solutions, les problèmes de classement où l'on veut ordonner, au moins partiellement, les solutions selon un ou plusieurs critères et les problèmes de classification où l'on cherche à affecter les solutions à des catégories prédéfinies selon leur valeur intrinsèque.

En banque de détail, banque d'investissement, gestion d'actifs et assurance, la **recommandation** est une activité essentielle, nécessitant une exploitation fine des informations historiques disponibles sur le client. Les techniques de *scoring* sont également impactées (voir le DIP 8 sur le *credit scoring*). En assurance, l'IA peut fortement

contribuer au *pricing*, à la souscription intelligente et à la gestion de fraude.

Dans les activités de marché des banques d'investissement, et surtout des *hedge funds* (fonds d'investissement spéculatifs non cotés), on est déjà souvent au-delà de l'aide à la décision *stricto sensu* puisqu'une part importante du trading se fait sous forme de **décision automatique** à une vitesse inaccessible à l'être humain, avec la recherche de micro-arbitrages à haute fréquence entre plateformes de cotations classiques et électroniques (chi-X, Turquoise, CEP…). Actuellement, ces algorithmes ultra-rapides ne sont pas ou peu augmentés, au sens où ils n'apprennent pas de leur environnement au fil des échanges. Ceci conduit à des règles de *stop-loss*[20] très basiques induisant une grande instabilité du système. Une forme d'apprentissage automatique embarquée est de nature à améliorer le trading sous réserve d'être maîtrisée (au sens compris par les utilisateurs tel que défini par le régulateur) et certifiée (voir DIP 15).

Les activités de marché, comme le *pricing* (fixation du prix d'un produit), le *hedging* (couverture du risque) et le calcul de *Value-at-Risk*[21] par agrégation de l'ensemble des desks, nécessitent à la fois une modélisation mathématique (modèles de Black-Scholes, de volatilité stochastique, etc.) et des calculs à très grande échelle, notamment pour la VaR. Elles pourraient bénéficier du **couple apprentissage automatique et IA symbolique** pour offrir une capacité d'aide en temps réel à la décision aux *traders* et aux *risks managers*.

Enjeux

L'accès aux données exploitables, en particulier pour l'apprentissage, est problématique (données brutes non nettoyées, manque de profondeur, stockage…) et/ou trop onéreux[22], même pour ceux qui les produisent (DIP 16).

La **complexité de la modélisation** est une véritable difficulté à prendre en compte. En effet, la formulation d'un problème d'aide à la décision est complexe. Il nécessite de comprendre le besoin des différents acteurs, d'identifier l'ensemble des états dans lequel le système considéré peut se trouver et d'évaluer la valeur de toutes les actions décisionnelles et leurs impacts afin de proposer une solution optimale ou un bon compromis.

Le **besoin accru de nouvelles expertises** suscite une inertie difficile à combler par le recrutement (DIP 11). Faut-il alors les développer en interne, s'appuyer sur des compétences externes (startup) ou réaliser des acquisitions ? La question est récurrente lors de chaque introduction d'une innovation dans une fonction métier.

Le principal verrou technique reste **l'explicabilité** (ou intelligibilité) de la décision proposée par le système, ne serait-ce que pour des raisons de responsabilité juridique ou de mise en conformité réglementaire (DIP 7).

La **robustesse** de ces outils en situation stressée (panique financière, risques extrêmes en assurance…) est également à prendre en compte.

20. Le stop-loss est le niveau de prix auquel l'investisseur préfère solder sa position en cas de perte.
21. Value-at-Risk (VaR) : mesure du risque de marché d'un actif financier.
22. En finance de marché par exemple, le coût d'accès aux données haute fréquence fournies par les agences de la place (Reuters, Bloomberg) se comptent en dizaines de k€mensuels par actif.

Pistes de résolution et recommandations

Les propositions suivantes contribuent à répondre aux enjeux décrits ci-dessus :

- **Qualifier et partager les données** traitées entre les acteurs pour assurer une stabilité et une robustesse du système, notamment en finance de marché (DIP 16) ;
- **Calculer le ROI**[23] de la mise en place d'un tel système pour en évaluer l'impact sur le long terme ;
- Garantir la **cohérence décisionnelle de bout en bout** (de la stratégie aux opérations) par l'hybridation de l'IA symbolique (prise en compte de la complexité de la modélisation) et l'apprentissage automatique et l'interopérabilité des systèmes ;
- **Expliquer** des décisions est incontournable pour que l'usager s'approprie le système et, dans certains cas critiques, certifier les procédures (DIP 15).

23. ROI est un acronyme qui signifie « Return On Investment » pour retour sur l'investissement.

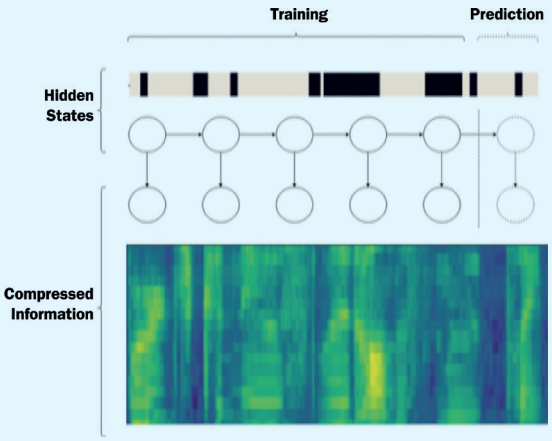
Focus
La gestion d'actif à l'heure de l'IA chez Bramham Gardens

(Précision : Il s'agit là d'une industrie B2B avec des professionnels de la gestion d'actifs qui prennent des décisions d'investissement pour créer de la performance, non de robo-advisors délivrant des conseils de gestion de patrimoine au client final).

La finance est devenue une discipline en soi il y a une soixantaine d'années grâce aux travaux du Prix Nobel Gérard Debreu sur la notion de marchés complexes. Toute la conception moderne du fonctionnement de la finance a vu le jour après-guerre : marchés et produits dérivés, pour lesquels ont été inventées des techniques de pricing. À l'origine, il ne semblait pas nécessaire d'établir une quelconque prévision pour fixer le prix d'un instrument financier. Or, s'il n'y a pas eu de révolution scientifique ces 30 dernières années, l'avènement de l'IA change aujourd'hui radicalement la donne, avec l'ambition de comprendre, grâce aux nouveaux outils dont on dispose aujourd'hui, des phénomènes jusqu'ici inexpliqués : analyser et anticiper la dynamique des prix et explorer de nouveaux domaines hier insoupçonnés (analogie de l'image des rayons X pour la finance traditionnelle et de l'IRM pour la nouvelle finance).

L'exemple ci-dessous illustre comment, en utilisant des techniques de reconnaissance de la parole couplées avec des modèles IA, on parvient à extraire de nouvelles informations sur les séries financières.

La gestion d'actif est actuellement encore une activité essentiellement de main-d'œuvre qualifiée et relativement bien rémunérée. L'avènement des technologies, notamment de l'IA, va rendre cette activité plus capitalistique, c'est-à-dire rendre les dépenses liées à l'appareil de production technique plus importantes par rapport aux coûts de personnel.



Le modèle dominant, que ce soit chez les grands groupes ou les petites structures en gestion d'actif (hors gestion passive et indices), est un modèle de nature assez artisanale : le gestionnaire de portefeuille, expert qui dispose d'un savoir-faire reconnu, est en face de son écran avec son expérience et ses données (Bloomberg, etc.) et travaille à créer de la valeur ce qui, en gestion d'actif, signifie prendre des décisions justes sur la dynamique des futurs prix. S'il investit dans un actif plutôt qu'un autre, c'est qu'il pense que cet actif va surperformer l'autre. Le système a été rationalisé pour que la prise de décision soit la plus performante possible. Beaucoup d'efforts et d'investissements (agences d'informations financières, in-

tégration de logiciels d'analyse de l'information, analystes…) ont été réalisés pour rendre l'environnement du gestionnaire le plus favorable à une prise de décision informée et qu'il puisse se concentrer sur la construction de portefeuilles aux volumes relativement importants, mais sans pour autant changer de mode opératoire.

Le prix est un agrégat des vues, avis et réflexions de nombreux individus sur de l'information permettant de comprendre sa dynamique et son évolution future. Dans ce processus de prise de décision d'achat ou de vente, la dimension de l'affect humain est extrêmement importante. L'apport de l'IA est très attendu pour permettre de s'adapter à un environnement changeant où il n'existe pas de règles précises. Dans le graphe ci-dessous, on montre par exemple que la communauté des investisseurs prend des décisions de prix en mobilisant un historique de mémoire variable.

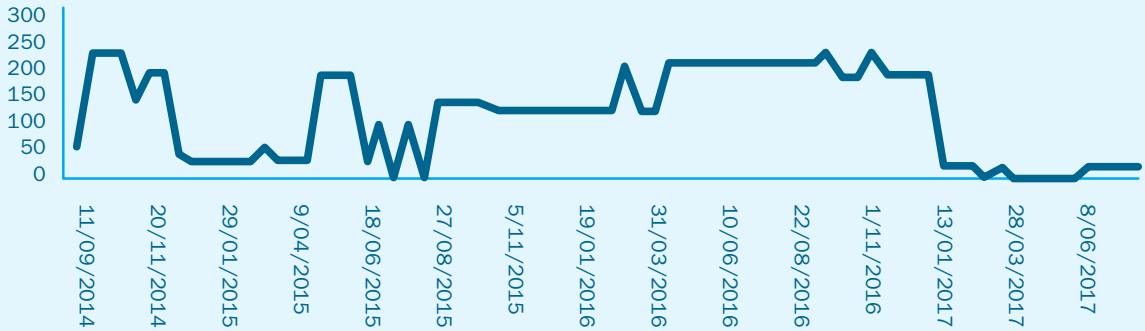
Deux approches se profilent :

- L'approche « exo-squelette », qui consiste à utiliser des outils d'aide à la décision, permet d'augmenter la productivité du gérant d'actif par le recours à des outils techniques utilisant l'IA.
- La seconde approche, à plus long terme, inclura l'industrialisation du processus d'investissement et donc de la prise de décision. C'est un changement de paradigme significatif, analogue à la révolution industrielle qui a vu la disparition de la fabrication artisanale au profit d'unités de production où les tâches rationalisées et optimisées sont effectuées par des machines contrôlées par les hommes.

Enjeux

- **Travailler sur la qualité des données** (voir DIP 16) : les données considérées comme utiles à la prise de décision sont celles sur l'entreprise, son secteur, la macro-économie et le sentiment des acteurs du marché à l'égard de l'entreprise. L'utilisation de données externes factuelles alternatives est intéressante et peut donner un avantage concurrentiel, mais elles sont sujettes à interprétation positive ou négative selon le contexte (exemple des données satellites : des stocks importants dans une entreprise peuvent vouloir dire qu'il y a une surproduction et donc des invendus [signal négatif] ou que l'entreprise a engrangé beaucoup de commandes [signal positif]. Le lien entre l'information et la décision à prendre n'est pas

Nbre de jours de mémoire utilisés par l'investisseur représentatif du secteur IT US



linéaire et l'enjeu est donc de sélectionner attentivement l'information pertinente) ;

- **Être sélectif sur les techniques IA :** l'IA étant loin de son stade de maturité, il n'existe pas de méthode unique et il faut donc trouver la meilleure combinaison. Cela implique de décomposer le processus en tâches simples et d'appliquer la technique la plus adaptée. La logique séquentielle est extrêmement importante en finance (de la même manière dans le cadre du *Natural Language Processing* [Traîtement Automatique du Langage Naturel], l'ordre des mots a une importance, contrairement à l'analyse d'images pour laquelle la date de réalisation n'a pas d'importance) ;
- **Incorporer l'humain :** la formation des prix résulte de l'agrégation de vues de milliers de personnes et donc de leur affect, le prix final étant le résultat de carnets d'ordre d'individus prêts à payer un prix donné et d'autres à vendre à ce prix, ce qui intègre des facteurs à la fois rationnels et émotionnels. L'ambition est que l'IA aide à comprendre et anticiper les mobiles de décisions basés sur des perceptions ou des sentiments. De plus, l'interaction humain–machine n'est pas encore fluide ;
- **Relancer l'innovation :** l'activité de la gestion d'actif a connu après la crise financière de 2008 une forte augmentation des coûts, liée à la réglementation et à l'émergence de la gestion du passif. Ces deux facteurs ont conduit à une contraction des marges, ce qui a entraîné la baisse de l'effort d'innovation ;
- **Une spécificité sectorielle :** la gestion d'actif est une activité marquée par la prudence et où la notion de confiance est essentielle. En effet, il faut du temps à une structure pour bâtir sa réputation auprès de ses clients/prospects afin qu'ils acceptent de lui déléguer la gestion de leur patrimoine. Cette activité requiert naturellement un cycle plus long pour l'innovation ;
- **Obtenir une taille critique :** la France dispose d'une expertise scientifique de très haut niveau en finance, très utile pour la phase de défrichage. Elle permet l'émergence d'une technologie efficace à petite échelle, mais qui reste artisanale. Il existe plus de difficultés pour passer à l'échelle supérieure, notamment dans la levée de fonds.

Pistes de résolution et recommandations

- **Permettre aux petites structures innovantes** de devenir des entreprises à taille intermédiaire (ETI) en les aidant à :
  - Lever des fonds propres en allégeant les démarches administratives et en évitant que l'entrepreneur ait à monter plusieurs dossiers de financements auprès des différentes institutions publiques ;
  - o Créer une forme de monitoring de la part des grandes sociétés de gestion en constituant un écosystème et un environnement aidant à grandir ;
  - Préserver le contrôle par l'entrepreneur en lui laissant l'autonomie pour innover.
- **Constituer des équipes d'experts multidisciplinaires** avec des experts en métiers de la finance et des techniciens de l'IA : mettre des seniors en expertise finance de juniors disposant de l'expertise technique ;
- **R&D : participer au développement des techniques IA séquentielles** avec une dimension temporelle (*Natural Language Processing*…).

DIP 2 : augmenter le conseiller face au client

Durant les deux dernières décennies, le conseiller a évolué avec son client dans un monde de plus en plus complexe. Il a dû assimiler successivement :

- Des offres de plus en plus variées avec des produits jusque-là inconnus (ex. : téléphonie mobile) où le service devient au moins aussi important que le produit lui-même ;
- La montée en puissance de l'approche omnicanal (messagerie sécurisée, mails, SMS, téléphone, chat, etc.), qui renforce le conseiller dans son rôle d'accompagnement, mais qui fragmente ses interactions avec les clients et multiplie les contacts (DIP 6) ;
- Un contexte réglementaire large et en constante évolution, vrai défi à maîtriser et à intégrer dans un entretien client ;
- Des clients eux-mêmes plus avertis ayant accès à une meilleure information ;
- De très fortes exigences de productivité commerciale malgré des compressions d'effectifs et des missions qui se rajoutent au métier de la vente (conseillers multitâches).

Que l'interaction avec le client se fasse en face à face ou par téléphone, c'est un processus complexe pour le conseiller dans lequel s'exprime toute sa valeur ajoutée. Par sa capacité à intégrer de nombreuses données dans une logique apprenante et sa capacité à raisonner, l'IA est un levier important à actionner sur les prochaînes années pour aider le conseiller. Elle doit lui permettre de comprendre plus rapidement des situations complexes (en assimilant plus de variables), d'adapter le discours et les recommandations de manière instantanée et naturelle et de concentrer son action et son attention sur l'écoute empathique et le conseil.

Enjeux

Ainsi, pour permettre au conseiller d'être augmenté de manière efficace, il est important de prendre en compte les enjeux suivants :

- **L'acceptabilité** de l'utilisation de l'IA **par le conseiller**. Ceci amène donc à revoir/redéfinir la place de la technologie ainsi que celle du conseiller (DIP 11).
- **L'interaction Humain/IA :** plus facile à distance (comme par téléphone), car le client ne voit pas les outils du conseiller, l'interaction en face à face, en agence, est plus complexe et est presque assimilable à « une vente à trois » (le client, le conseiller et l'IA). Le risque de rejet est important si l'ergonomie de ces nouvelles interactions n'est pas suffisamment travaillée et testée en amont ou que les réponses de l'IA ne sont pas en adéquation avec les requêtes du conseiller. De plus, il est aussi crucial de penser l'interaction Humain-IA comme un vrai dialogue (DIP 11).

Pistes de résolution et recommandations

L'interaction entre le client et le conseiller doit être adaptée ou repensée lorsque l'on rajoute une IA :

- Afin de prendre en compte l'acceptation du conseiller, mais aussi du client, **l'accompagnement à la conduite du changement** doit être proposé. La

co-construction de ces solutions entre conseillers et concepteurs devient plus que jamais nécessaire.

- Pour développer l'acceptation, la fiabilité des recommandations doit être **testée et qualifiée** au cas par cas, voire même être évaluée **par les conseillers et les clients** eux-mêmes (DIP 15). Pour cela, la supervision de l'apprentissage automatique par des conseillers en situation réelle est une approche possible.
- Enfin, pour fluidifier les échanges entre l'IA et le conseiller, il est nécessaire de développer des **solutions efficaces en TAL**[24] (voir point saillant sur le « Traîtement automatique de la langue »).

24. TAL est l'acronyme du « Traîtement Automatique du Langage naturel », en anglais NLP pour « Natural Language Processing ».

Focus
L'IA pour augmenter l'assureur avec Zelros

Zelros développe une technologie d'employé augmenté à destination des assureurs. Le constat de Zelros est que l'intelligence artificielle va révolutionner la façon dont les assureurs opèrent leur activité. Tous les processus de l'assureur vont être réinventés par le *machine learning* : souscription, tarification, évaluation des risques, gestion des sinistres, relation client...

La solution s'intègre naturellement dans l'environnement de travail du collaborateur sous la forme d'un « assistant virtuel » qui le conseille avec transparence et en temps réel pour l'aider à prendre les meilleures décisions. L'assistant est continuellement nourri de scores et de prédictions métier, calculés sur une plateforme de *machine learning* sécurisée.

La solution intelligente Zelros couvre aujourd'hui deux processus critiques des assureurs :

- L'aide à la vente : aider les conseillers à mieux servir leurs clients, en leur proposant des produits personnalisés dans un contexte réglementaire exigeant (Loi Hamon, amendement Bourquin, DDA) ;
- L'aide à la gestion des sinistres : faciliter la vie des gestionnaires en diminuant le temps de traîtement des dossiers des assurés.

Ces deux processus ont été adressés en priorité par la startup qui estime que vente et gestion se rapprocheront dans l'avenir. Le gestionnaire sera en mesure de réaliser des rebonds commerciaux et le conseiller de gérer des sinistres simples directement à son niveau.

La solution est déjà déployée auprès de plusieurs assureurs (Natixis Assurances, CBP, CNP Assurances, Maif...). Elle est utilisée quotidiennement par plusieurs milliers d'employés servant plusieurs millions d'assurés. Son efficacité est mesurée selon plusieurs critères : l'amélioration de la satisfaction des assurés (NPS/ *Net Promoter Score*), le taux d'adéquation entre un devis et une demande client, le délai de réponse pour un devis client ou le temps de traîtement moyen d'un sinistre.

Zelros développe son produit depuis près de trois ans. La solution a en particulier évolué pour être en conformité avec le RGPD. Par ailleurs, pour faciliter l'adoption de son produit par les employés d'assurance, Zelros intègre une approche éthique de l'utilisation de l'intelligence artificielle. En particulier, les scores et prédictions peuvent être expliqués au conseiller ou au gestionnaire afin qu'il puisse actionner les recommandations algorithmiques de la meilleure façon. Par ailleurs, tous les modèles prédictifs utilisés sont documentés dans un format standard que la startup a publié en open source, contribuant à leur transparence et auditabilité.

DIP 3 : augmenter le collaborateur

L'activité d'un collaborateur ou d'un conseiller aujourd'hui n'est pas exclusivement orientée vers le client et la relation bancaire. Il lui est de plus en plus demandé d'assurer des tâches anciennement dévolues à des middle office : contrôle de dossier de souscription, KYC (*Know Your Customer*), traîtements des mails entrants, instruction de dossier de financement, pilotage de l'octroi. Les automatismes proposés (RPA, analyse sémantique…) permettent d'alléger les tâches répétitives sans valeur ajoutée. Cependant, la mise en route d'un programme intelligent ne suffit pas pour rendre le système opérationnel : des compétences humaines sont nécessaires pour éduquer et nourrir ces logiciels dont le fonctionnement repose sur la qualité des informations récoltées.

Enjeux

La complexité grandissante des produits et services financiers et les nombreux aménagements réglementaires induisent un besoin permanent de montée en compétences. Cependant, en matière de gestion de la connaissance, le collaborateur n'a pas nécessairement le temps de la développer. Cette course à la performance nécessite un coaching actif et quasi permanent par des systèmes automatisés. Ces derniers peuvent être perçus comme intrusifs. Les assistants virtuels à base d'IA peuvent ainsi devenir de véritables « **coachs virtuels** » facilitant l'acquisition de nouvelles connaissances et compétences.

Pour l'aide à la décision, **l'adaptation en continu** aux changements réglementaires, commerciaux ou juridiques, en adéquation avec les bonnes pratiques, reste un vrai défi.

Pistes de résolution et recommandations

- Un **accompagnement personnalisé** du collaborateur facilitera l'adhésion d'une assistance passive et non intrusive en garantissant une interopérabilité active à l'initiative du conseiller, avec des systèmes simplifiant les process de la banque (DIP 11 et DIP 12).
- Pour être efficace, le **développement d'un coach virtuel** nécessite la double compétence technique et métier. Il est aussi nécessaire d'intégrer la possibilité d'une modération humaine (utilisation à la demande et selon le réel besoin).

DIP 4 : proposer le « self-care »

Un des aspects de la transformation numérique est d'externaliser vers le client un nombre croissant d'opérations à réaliser en autonomie. De plus en plus d'opérations (mise à jour des coordonnées, déclaration de sinistre, virement, souscription de crédit ou de police d'assurance, affacturage…) sont mises à la disposition des particuliers et des entreprises. Cette tendance au self-service est aujourd'hui fortement présente dans tous les secteurs. Pour autant, l'utilisation de l'IA dans ce contexte renouvèle certains enjeux du « *selfcare* » et en crée d'autres.

L'IA peut être utilisée du côté du client pour :

- Automatiser entièrement (ou en grande partie) l'accès au self-care grâce à des interfaces utilisant le langage naturel sur support écrit ou oral (« OK ma banque », « puis-je faire un virement ? »…) ;
- L'accompagner dans son parcours de self-care (« OK mon assurance », « où en est ma déclaration de sinistre de la semaine dernière ? »…) ;
- Se substituer pour interagir avec l'institution financière (« ma voiture » envoie directement à « mon assurance », la vidéo de mon accrochage avec un rapport sur les conditions météo, les conditions de trafic, le lieu et l'heure de l'accident ;
- Anticiper ses besoins et formuler des suggestions de produits ou d'opérations.

L'IA peut être aussi utilisée du côté fournisseur pour :

- Automatiser entièrement (ou en grande partie) l'arbitrage sur des actes initiés en self-care (une demande de rachat de crédit, de souscription d'assurance…) ;
- Anticiper un besoin émergent pour le client et le contacter en amont.

Enfin, le self-care peut être étendu à de nouveaux modèles d'affaires dans lesquels l'IA peut être utilisée, mais sans être l'élément décisif :

- Peer to peer et/ou places de marché (crédit par exemple) ;
- Vendor Relationship Management.

Enjeux

Toutes les opérations ne sont pas éligibles à une distribution en libre-service. En effet, la réglementation prévoit dans certains cas l'intervention de personnes qualifiées : la vente d'instruments financiers (assurance-vie et titres), l'octroi de crédit, etc.

Le rôle de l'IA en self-care pour les clients particuliers (B2C) doit donc être de :

- Préparer l'accomplissement des actes réservés aux agents humains ;
- Inciter les clients à utiliser les systèmes automatisés pour les actes pouvant être traités par la machine ;
- Savoir reconnaître et identifier un client de manière certaine (KYC) ;
- Prédire ou prévoir le plus finement possible la prochaîne action du client.

Pour les clients professionnels ou entreprises (B2B), la réglementation peut être moins contraignante.

L'acceptabilité d'une relation entièrement automatisée est à priori forte (tendance historique au self-service) mais plus la criticité des actes à réaliser est importante, plus la possibilité de débrayer à tout moment vers un interlocuteur humain est incontournable.

Enfin, il est important d'adapter les recommandations aux attentes des clients/de la société, en particulier de ne pas proposer sans cesse les mêmes produits.

Pistes de résolution et recommandations

Les innovations possibles doivent permettre de :

- Garantir la « débrayabilité » efficace des processus self-care vers des interlocuteurs humains en conservant le niveau d'information pour la personne qui reprend le dossier en cours ;
- Développer des produits de self-care B2B ;
- Développer le traîtement du langage naturel sur le canal « voix ».

Pour cela, il est nécessaire de :

- Développer le self-care « push » et des moteurs de recommandation de produits et services beaucoup plus fins et pertinents pour réaliser des ventes/actes croisés en self-care ;
- Intégrer une dimension prédictive (prochaîne action du client) et d'arbitrage (cette demande du client mérite-t-elle d'être traitée ?) dans les parcours self-care.

DIP 5 : solliciter le client par l'IA

Aujourd'hui, la sollicitation d'un client par un système se concentre sur deux aspects :

- le consentement client à la collecte et l'exploitation des données. On parle notamment de données personnelles, d'habitudes de navigation, d'historiques de consommation et de conversation. Ces données consenties, stockées au format brut, permettent, via une exploitation intelligente, l'extraction d'informations stratégiques utiles à la segmentation et au profilage des clients ;
- l'évaluation par les clients des services fournis et l'identification des points d'amélioration des réponses et des prestations produites par des robots.

Ces scores et labels recueillis permettent alors d'améliorer la prédiction automatique de la satisfaction client et de déclencher des actions correctrices ou amplificatrices.

Enjeux

En complément avec les actions d'acquisition, de nettoyage et de qualification des données (DIP 16), il est nécessaire de considérer les enjeux réglementaires (consentement explicite) : en effet, les données collectées doivent être limitées au strict besoin du traîtement avec nécessité de transparence pour les clients. On parle notamment avec la RGPD[25] *d'accountability*, de *privacy by default* et de *privacy by design*. Cette réglementation peut être perçue comme un désavantage concurrentiel, voire un ralentisseur d'innovation.

L'adoption de l'IA par le client soulève d'autres problèmes pour les entreprises, à savoir être en mesure d'évaluer et d'anticiper l'erreur induite par le système artificiel. De plus, il faut garantir que le client ne pourra en détourner l'usage.

S'ajoute à cela le cadre législatif intégrant la prise en compte des aspects éthiques dès les étapes de conception (ethics by design). Cet enjeu est détaillé dans le DIP 13.

Le troisième point consiste en une compréhension plus fine de la sémantique des phrases pour déterminer le sens des échanges écrits et oraux (DIP 11).

Pistes de résolution et recommandations

La prise en compte de la RGDP imposera des solutions fondées sur la sémantique permettant l'identification automatique des données personnelles (nom, n° sécurité sociale, adresse, maladie, etc.) ainsi que des relations (distinction des profils clients et des interactions passées).

Ces solutions permettront également d'aller plus loin dans le processus de mise en conformité en opérant les phases d'anonymisation et de pseudonymisation[26] des données personnelles, en détectant et en marquant les données sensibles à partir des contenus non structurés.

25. Le RGDP est le règlement dit Règlement Général sur la Protection des Données qui renforce et unifie la protection des données pour les individus au sein de l'Union européenne.
26. La pseudonymisation est un traîtement de données à caractère personnel de manière qu'on ne puisse pas attribuer les données à une personne physique sans avoir recours à des informations supplémentaires.

Il est recommandé de :

- Identifier et mettre en place des *process owners* pour contrôler les tâches effectuées par l'IA au niveau des entreprises ;
- Clarifier l'encadrement législatif de l'IA et des réflexions portant sur la prise en compte de l'éthique dès la conception (DIP 13) ;
- Soutenir et encourager les initiatives transverses et interdisciplinaires basées sur des approches travaillant sur des données anonymisées.

Les technologies utilisées s'articulent autour du traîtement et de la génération du langage naturel (voir le point saillant correspondant). Pour le traîtement de la voix, il est important d'encourager la mise à disposition de grandes bases de données d'audios surtout en langue française, constat similaire à celui de la vision par ordinateur.

Focus
Le ciblage client pour un meilleur conseil en gestion de patrimoine avec Mieuxplacer.com

Démocratiser le conseil en Gestion de Patrimoine (CGP), réservé aujourd'hui à une clientèle aisée, induit une industrialisation de la personnalisation en accompagnant le client dans ses choix et en lui offrant un suivi des performances et de l'évolution de ses placements. Pour ce faire, Mieuxplacer.com utilise une combinaison d'algorithmes d'IA dans le fonctionnement de ses services pour contrecarrer les deux points de blocages majeurs **du métier de CGP** :

- **Le coût :** dans la finance traditionnelle, moins le client a de ressources, plus le conseil lui revient cher. Grâce à l'IA, les temps de calcul sont réduits et la recommandation du CGP est automatisée, baissant ainsi les coûts[27] ;
- **Le choix de produits et la personnalisation :** la plupart des acteurs de l'épargne cherchent aujourd'hui à faire rentrer leurs clients dans des cases prédéfinies et n'offrent pas de personnalisation du service : c'est en effet la solution la plus couramment utilisée pour industrialiser la distribution. Grâce à l'IA et à sa gamme étendue de plus de 100 produits d'épargne, Mieuxplacer.com a créé pour ses clients des systèmes de recommandations sur-mesure adaptées à leurs objectifs, à leurs ressources financières, à leur situation patrimoniale et à leur volonté de prise de risques.

Le système, reposant sur une hybridation d'algorithmes d'apprentissage comme l'apprentissage profond et de recherche opérationnelle (ou d'IA symbolique), permet ainsi de bâtir une recommandation personnalisée. Par ailleurs, la collecte ciblée de données améliorera la pertinence de la recommandation.

Enjeux

Les institutions financières en place ont historiquement des systèmes d'information en silos. La construction de systèmes d'IA, très consommateurs de données, est alors complexifiée. Travailler au désilotage des systèmes est un prérequis à la mise en place de systèmes d'IA de grande envergure, mais doit être réalisé au départ à une petite échelle. En effet, la remise à plat de toute l'infrastructure informatique ne semble pas être la meilleure manière de procéder. Pour répondre à des usages concrets, il est donc essentiel de faire participer les experts métiers aux phases de conception et de tests afin de bénéficier de leur savoir-faire.

Il faut ensuite procéder par strates successives pour développer la solution de manière agile. L'une des erreurs les plus fréquentes est de vouloir obtenir une solution parfaite dès la première itération. Cette erreur est encore plus prononcée lorsqu'il s'agit de projets d'IA où les attentes des parties prenantes sont extrêmement fortes. Le risque est de ne jamais réussir à terminer et donc que le système

27. Le prix du conseil est impacté, car partagé avec les clients qui voient directement le bénéfice du progrès.

ne soit jamais opérationnel. Pour éviter cet écueil, il faut commencer à une échelle raisonnable, l'objectif étant d'aboutir à une première version fonctionnelle du service, puis de l'améliorer de façon incrémentale.

La gestion des attentes des parties prenantes est essentielle dans la conduite d'un projet d'IA pour éviter toute déception.

Recommandations

- **Gestion des bases de données :** désiloter les bases ou créer un système de gestion des données interconnecté ;
- **Construction en mode agile :** sécuriser les fonctionnalités primaires avant de développer les services annexes ;
- **Optimisation des algorithmes :** lever les biais éthiques potentiellement présents, améliorer l'existant au contact des experts métiers et des clients grâce au *machine learning*.

DIP 6 : optimiser la distribution omni-canal

Désencombrer le centre d'appels et réinventer le parcours client pour fournir une nouvelle expérience qui réponde aux attentes du monde actuel, tel est le défi de la distribution omnicanal qui nécessite :

- La création d'une IA conversationnelle à entraînement unique pour l'ensemble des canaux de communication ;
- La capacité de traiter des scénarios complexes allant de l'authentification à la consultation de soldes, la gestion de virement, la réinitialisation de mots de passe, l'augmentation des seuils de dépôts, les cartes bancaires défectueuses et la FAQ[28] ;
- La disponibilité des canaux du parcours client en commençant par la voix suivie par le SMS, le mail, le chat ainsi que les messageries instantanées ;
- La capacité de collaboration avec les agents de leur centre de contact ;
- …

Le client peut ainsi contacter sa banque et avoir des réponses immédiates dans la plupart des cas, sans contrainte horaire ni attente et sur **sur le canal de communication qui lui convient le mieux**. De plus, la mise à disposition de plusieurs innovations comme celles décrites ci-dessous permettrait de créer une véritable différence en termes d'expérience utilisateur :

- L'analyse en temps réel de la qualité de chaque conversation, tant sur le fond que sur la forme ;
- Le transfert de la communication d'un canal à un autre avec continuité de conversation sans perte de contexte afin de répondre à toute demande, et cela en une seule conversation (bascule d'une conversation téléphonique vers du SMS par exemple) ;
- La collaboration humain-machine en temps réel : les téléconseillers ont accès à une interface qui leur permet de superviser en temps réel les conversations entre les clients et l'IA. À tout moment, un téléconseiller peut décider de reprendre la main sur une conversation (débrayage). À l'inverse, l'IA peut, dans des cas prédéfinis, décider de transférer à un téléconseiller une conversation afin de traiter des situations nécessitant une reprise en main humaine.

Enjeux

Avoir une idée des scénarios industrialisables par l'intelligence artificielle est un prérequis pour la banque et l'assurance. Les enjeux sont alors :

- La collecte de données historiques exploitables ;
- Un système unique et sans coutures, accessible par téléphone, SMS, mail, chat et messageries instantanées ;
- Le respect des critères de protection des données personnelles (i.e. RGPD & *Privacy Shield*) ;
- L'authentification dynamique avec plusieurs niveaux de sécurité basée sur le profil de l'utilisateur et un système de vérification tiers ;
- La reconnaissance par la voix et au travers d'une IA de numéros de compte

28. Une FAQ ou « foire aux questions » vient de l'acronyme anglais pour « frequently asked questions ». C'est une liste faisant la synthèse des questions posées de manière récurrente sur un sujet donné, accompagnées des réponses correspondantes.

bancaire ou de sécurité sociale, de noms, de prénoms et d'adresses ;
- Le passage d'un compte personnel à un compte entreprise avec conservation du contexte utilisateur et scénario d'authentification différentiel…

Pistes de résolution et recommandations

Pour cela, il est important de :
- Se concentrer sur les scénarios optimisés avec 80 % des conversations pouvant être industrialisées ;
- Penser collaboration humain-machine pour capitaliser sur le meilleur de chacun d'entre eux ;
- Commencer sur un petit périmètre (identifier les tâches les plus simples à automatiser) puis faire évoluer rapidement les compétences de l'agent en s'appuyant sur les demandes des clients ;
- Concevoir un unique système sans couture interopérable avec l'ensemble des canaux visés ;
- Utiliser l'opportunité de mettre à disposition des clients un service 24 h/7 j sans file d'attente où les téléconseillers ne réalisent pas d'appels répétitifs au long d'une même journée ;
- Enclencher une conduite du changement (DIP 12) et une formation des téléconseillers qui éprouveraient le sentiment d'une compétition/rivalité avec l'IA (DIP 10) ;
- Revisiter les indicateurs de performance pour changer la donne afin de permettre aux téléconseillers de se concentrer sur la qualité de la relation client plutôt que sur la quantité d'appels traités.

Focus
Chatbots, le retour d'expérience d'Orange Bank

Lancée en novembre 2017, Orange Bank est une banque 100 % mobile reposant sur un modèle innovant en rupture par rapport aux acteurs traditionnels. Dès l'origine, la volonté a été d'intégrer dans l'offre des services disruptifs s'appuyant notamment sur l'IA. Aujourd'hui, son principal usage est le conseiller virtuel Djingo. Orange Bank a fait le choix d'en faire le canal principal de communication des clients avec la banque en complément des mails, des formulaires ou encore de la relation téléphonique : c'est le conseiller bancaire numéro un. Ses principaux atouts sont sa disponibilité 24 h/24 et 7 j/7 par chat. Il permet de répondre à une forte demande des clients de disposer de façon immédiate, quel que soit le lieu ou l'heure, des informations dont ils ont besoin.

En huit mois, Djingo a traité près de 470 000 conversations soit en moyenne 17 000 conversations par semaine (mai 2018), avec un taux de compréhension des questions posées de l'ordre de 85 %. Dans plus de la moitié des cas, le client obtient avec Djingo toutes les informations dont il a besoin en toute autonomie.

Dans les autres cas, le client est orienté vers un conseiller (humain) du Centre de Relation Client. Celui-ci visualise automatiquement l'historique de l'échange et prend le relais en apportant au client une relation plus personnalisée et un service à plus grande valeur ajoutée.

Premier cas d'usage de l'IA à Orange Bank, Djingo a pour vocation d'évoluer, dans les années à venir, vers un rôle de coach financier virtuel, anticipant les besoins des clients en proposant des services de manière proactive. Dans l'immédiat, les linguistes et *data scientists* d'Orange Bank s'attachent à l'amélioration continue de sa capacité de compréhension, via l'analyse des communications. Aux côtés de développeurs et de *business analysts*, ils constituent une équipe dédiée à l'IA au sein de la banque. En parallèle, cette équipe travaille également sur de nouveaux cas d'usage : analyse de la tonalité des commentaires laissés sur les stores et les réseaux sociaux afin de détecter et de traiter plus rapidement les clients insatisfaits ; intégration des *rich cards* dans la fenêtre de chat pour des réponses enrichies en images et vidéos ; traîtement automatique des emails et formulaires, etc.

Cette révolution du traîtement intelligent de la donnée pose évidemment des questions essentielles quant au contrôle de l'accès aux données et à l'adaptation du cadre réglementaire du secteur bancaire.

Dans un autre registre, fédérer les différentes initiatives Djingo au sein du Groupe Orange est également un enjeu majeur. Il s'agit en toile de fond d'offrir aux clients du Groupe une expérience fondée sur le concept ATAWAD – *AnyTime, AnyWhere, AnyDevice*. Pour l'heure et à plus court terme, l'un des challenges à relever sera de rendre le conseiller virtuel davantage proactif ou multimodal en intégrant notamment la voix, par exemple via l'enceinte connectée « Djingo speaker » développée par Orange.

Les ressources de l'intelligence artificielle sont ici particulièrement prometteuses : capacités de recommandation, personnalisation des offres, disponibilité de services, etc. Elles vont considérablement faire évoluer les modèles relationnels de nos sociétés et de l'expérience client. Orange a décidé d'en faire un enjeu stratégique majeur notamment à travers Orange Bank.

DIP 7 : simplifier les processus de mise en conformité et faciliter la gestion des risques

L'activité financière est par essence une activité de mesure et de gestion de risques de toute nature : crédit, marchés, liquidité, contrepartie et, de plus en plus, conformité. En effet, le monde de la finance et des assurances est confronté à une augmentation sensible du nombre d'amendes et de sanctions de la part des différents régulateurs pour cause de non-conformité à tel ou tel texte. Cette évolution illustre la volonté des gouvernants d'une meilleure surveillance et maîtrise des processus dans un contexte de complexification croissante des circuits/échanges d'informations. Par ailleurs, les clients sont de plus en plus sensibles à l'utilisation qui peut être faite de leurs données, mais souhaitent aussi pouvoir bénéficier des possibilités ouvertes par les nouvelles technologies (capacités de stockage et d'analyse des données) pour obtenir par eux-mêmes des informations et recevoir de la part des établissements financiers des conseils pertinents et adaptés à leurs besoins.

La question de la fiabilité des dispositifs existants et de leur évolution se pose au travers de nouvelles fonctionnalités comme :

- **La connaissance des clients** à l'entrée en relation et son actualisation **tout au long de la relation d'affaires** ;
- Le respect des dispositifs de sanctions internationales (embargos, etc.) ;
- La contribution à la lutte contre le blanchiment d'argent, le financement du terrorisme ou l'évasion fiscale ;
- La prévention de la fraude, tant interne qu'externe (DIP 9) ;
- La surveillance du respect de l'intégrité des marchés ;
- La délivrance du bon et juste conseil au bon moment (DIP3 et DIP5)…

La maîtrise des données (DIP 16) et la capacité à les exploiter efficacement sont au cœur de l'ensemble de ces sujets. Cela renvoie à plusieurs défis à relever, parfois contradictoires entre eux :

- **La confiance/confidentialité :** la confiance va devenir un enjeu majeur des prochaînes années. *« Si je n'ai pas confiance dans l'opérateur/entreprise/banque, je ne vais pas vouloir jouer la transparence et lui fournir les informations demandées, ce qui rendra plus difficile le travail d'analyse de données (perte de fiabilité, du caractère prédictif) »* ;
- **Le partage d'information :** la notion de tiers de confiance dans le domaine de la conformité n'est pas aujourd'hui très développée. Ainsi, plutôt que chaque banque demande à la même personne ses pièces d'identité, pourquoi ne pas disposer d'un registre central qui permettrait d'avoir une connaissance client fiabilisée disponible pour tout acteur mandaté à cet effet ? (voir DIP 27) ;
- **Le respect du cadre légal et du RGDP :** il convient certes de protéger les clients/utilisateurs finaux, mais aussi de vérifier qu'il n'y a pas de distorsion de concurrence avec des opérateurs utilisant les facilités offertes par ces nouvelles technologies pour s'affranchir de ce même cadre (exemple : la délocalisation du siège social de Facebook). Cela

soulève alors la question de la souveraineté : quel degré de confiance peut être accordé en tant qu'État à une structure ne relevant pas du droit national et dont les clients/utilisateurs sont dépossédés de leurs données ?

Par ailleurs, la vision consolidée en temps réel de l'ensemble des risques sous-jacents est un enjeu fort de l'industrie financière, encore plus en période de crise ou retournement de cycle économique pour permettre de continuer à exercer son activité et ainsi contribuer au retour à l'équilibre.

Pistes de réflexion et recommandations

Dans les domaines régaliens comme la lutte contre le blanchiment et le financement du terrorisme, on pourrait s'attendre à un partage plus important entre structures afin de disposer d'un socle commun d'outils offrant au final un meilleur gage de sécurité pour tous. Ainsi, pour faire face aux questions de souveraineté, le développement d'une capacité nationale de traîtement en masse des données pourrait être un atout dans le contexte actuel.

Par ailleurs, il conviendrait de développer des systèmes de consolidation et de pilotage de l'ensemble des risques issus d'opérations multiples (crédits, liquidités, marchés…) souvent gérées dans des systèmes d'information différents.

La fiabilité des analyses et des *reportings* sera d'autant plus forte que la qualité des données sera élevée (DIP 16). Une mutualisation de l'effort de collecte et de fiabilisation, dans un dispositif national offrant les gages de protection nécessaires, serait un accélérateur indéniable et attendu.

C'est pourquoi il est nécessaire de :

- Accompagner l'investissement dans les technologies apprenantes et la sécurisation/fiabilisation/agrégation des données ;
- Développer et renforcer, dans le cadre respectueux des règles de concurrence, les expériences existantes destinées à faciliter le partage d'informations et de connaissances entre banques et assurances ;
- Favoriser l'émergence de hubs d'experts en traîtement de données, tant structurées que non structurées, et en IA symbolique et encourager les initiatives de partenariats.

Focus
L'IA au service du KYC et de la conformité à la Société Générale

La conformité est le socle de la confiance entre la banque et ses parties prenantes. Agir en conformité consiste donc à connaître les règles émises par les régulateurs et à les respecter.

Parmi les principaux enjeux, la connaissance client, appelée « KYC » (*Know Your Customer*), correspond à l'ensemble des obligations portées par les organismes financiers autour de celle-ci. Le KYC s'articule autour de l'identification proprement dite du client, de la capture de son profil, de l'actualisation de ses informations et de la mise en œuvre d'une vigilance adaptée.

Pour répondre aux obligations réglementaires de KYC, la Société Générale a développé une plateforme permettant de télécharger, contrôler et partager les documents relatifs à une clientèle de particuliers.

Cette solution appelée « Insta-KYC » utilise des modèles algorithmiques et un apprentissage automatisé, permettant d'automatiser la lecture, l'analyse, le contrôle, la recherche et l'extraction des informations contenues dans les documents communiqués par ses clients. À ce jour, déjà plus d'une centaine de types de documents sont reconnus et plusieurs milliers de documents peuvent être traités en quelques heures.

Enjeux

Les activités relatives au KYC peuvent avoir une certaine récurrence lors des revues périodiques des bases clients. Ces opérations étaient jusqu'à présent manuelles, fastidieuses, très répétitives et présentaient donc un fort risque opérationnel nécessitant la mise en place d'un dispositif de contrôle qualité important et coûteux. Le potentiel de l'IA appliqué aux besoins précis du KYC a permis un changement de paradigme en répondant à trois enjeux majeurs :

- Gagner en efficacité opérationnelle : un document est traité en moins d'une seconde là où plusieurs minutes étaient nécessaires auparavant ;
- Gagner en qualité, car il n'y a plus d'erreurs opérationnelles de ressaisies et les contrôles élémentaires de cohérence sont embarqués nativement ;
- Améliorer la maîtrise des risques de conformité et le service client, car les analystes peuvent se concentrer sur l'analyse des dossiers clients pour détecter les situations à risque et solliciter de façon plus ciblée et plus pertinente les clients.

Les bénéfices de la solution sont suivis et permettent de confirmer l'excellent retour sur investissement.

« Aujourd'hui, nous investissons massivement dans ces sujets. Un des axes majeurs de la transformation de la Conformité passe par cette transformation digitale et le recours à ces nouvelles technologies. Les terrains d'application sont multiples et concernent toutes les fonctions de l'organisation. »

Edouard-Malo Henry, Directeur de la Conformité du Groupe Société Générale.

Recommandations

En termes de recommandations, les points saillants du retour d'expérience sont :

- Repenser de façon disruptive les besoins à couvrir et changer de paradigme dans l'approche menant à la solution ;
- Composer l'équipe projet de profils complémentaires : référents conformité, experts technologiques, analystes KYC ;
- Bénéficier d'un bon niveau de sponsorship interne.

DIP 8 : optimiser le credit scoring

L'attribution d'un crédit par un professionnel, que ce soit une banque ou un organisme de crédit non bancaire, est soumise à une analyse du risque de non-remboursement. Celle-ci concerne aussi bien l'attribution d'un crédit à un particulier qu'à une entreprise, visant à établir le nombre et le montant des mensualités, éventuellement la date de début du remboursement ainsi que l'éligibilité de la personne au prêt. Dans le cas où l'entité est éligible, notamment pour les entreprises, cette analyse permet d'établir le montant du taux d'intérêt du crédit.

Pour mesurer le risque de défaut ou de défaillance de l'emprunteur, les banques et professionnels du crédit ont recours à différents outils que l'on regroupe sous l'appellation d'outils de *scoring*. Ces outils mathématiques ou analytiques visent à estimer une probabilité ou plus généralement un score évaluant la capacité de remboursement via une note associée à l'entité qui emprunte.

Enjeux

La nécessité de transparence concernant les critères d'attribution d'un crédit a permis de définir des modèles simples de règles, ce qui a favorisé des approches de type système expert. Ces règles ont été généralement construites sur des critères initiaux de bon sens. Elles ont ensuite été affinées par des experts à partir d'apprentissage de comportements récurrents, permettant d'identifier de nouveaux critères susceptibles de valider la probabilité de l'entité emprunteuse de ne pas pouvoir rembourser. Notamment, l'article 313-12-1 du code monétaire et financier stipule que *« les établissements de crédit ou les sociétés de financement fournissent aux entreprises qui sollicitent un prêt ou bénéficient d'un prêt leur notation et une explication sur les éléments ayant conduit aux décisions de notation les concernant, lorsqu'elles en font la demande. Ces explications ou éléments ne peuvent pas être demandés par un tiers ni lui être communiqués ».*

Les quantités de données de toute nature dont disposent aujourd'hui les organismes de crédit permettent d'envisager le recours à des systèmes de scoring plus performants, en s'appuyant notamment sur l'apprentissage machine. Ces systèmes supervisés vont apprendre, sur la base d'une définition appropriée de la notion de défaut, les critères permettant de maximiser à la fois la détection des entités à fort risque, mais aussi celles qui ne le sont pas[29].

Cependant, ces approches peuvent être perçues comme des « boîtes noires » et l'enjeu de la mise au point d'algorithmes d'apprentissage machine capables d'expliciter leurs décisions est majeur. Cet enjeu est abordé dans le DIP 15.

La qualité des données et de la définition du défaut est un critère important pour obtenir des systèmes de *scoring* plus précis et robustes (voir le DIP 16).

29. L'analyse de la performance de détection se fait souvent en mesurant une valeur mathématique (généralement le score de Gini) et une matrice dite matrice de confusion qui permet de se rendre compte du nombre de faux positifs et faux négatifs pour juger de l'efficacité du modèle de *scoring*.

L'utilisation de ces données externes par les établissements financiers a pour vocation de renforcer l'efficacité de la détection et du ciblage grâce à l'enrichissement des données clients.

L'amélioration de la précision de ces systèmes et la facilité d'intégration aux outils existants sont aussi des enjeux forts pour les acteurs du crédit et les fournisseurs de telles plateformes (DIP 17).

Les enjeux du respect de la vie privée sont ici conséquents (voir DIP 7).

Pistes de résolution et recommandations

Une part importante du temps de développement de ces systèmes de scoring utilisant de l'apprentissage est consacrée aujourd'hui au nettoyage du jeu de données ainsi qu'à la définition d'un sous-ensemble de critères permettant d'assurer la stabilité des systèmes. Ainsi, pour améliorer la pertinence et l'efficacité de ces systèmes de scoring, un travail de préparation des données doit être réalisé (DIP 16). De plus, on peut penser à utiliser d'autres bases (à identifier) pour améliorer l'apprentissage (en utilisant par exemples des approches de type transfert learning).

Des fournisseurs d'outils et de technologies à base d'IA ont fait des avancées importantes, aussi un travail en étroite coopération permettrait de mettre en place rapidement des systèmes de crédit plus précis et plus robustes.

DIP 9 : lutter efficacement contre la fraude

L'objectif de la fraude dans les domaines de la banque et d'assurance est d'obtenir un avantage financier non consenti via l'utilisation de moyens visant à tromper l'une des parties. Elle est multiple : documentaire (faux papiers ou justificatifs), fiscale, fausse déclaration, usurpation d'identité, utilisation non consentie de moyens de paiement de tiers, fraude électronique… La lutte contre la fraude est une obligation réglementaire des banques et des compagnies d'assurance et fait supporter à ces établissements un coût important.

La difficulté de la lutte contre la fraude est liée à différents facteurs :

- Les fraudeurs développent sans cesse de nouvelles techniques pour contourner les protections. Ils bénéficient donc généralement d'un avantage plus ou moins temporaire que l'établissement financier doit identifier puis combattre ;
- Les déclarations des fraudeurs ne sont pas toujours vérifiées et les justificatifs demandés peuvent être facilement falsifiés ;
- Le manque de communication entre acteurs financiers fait qu'un fraudeur peut répliquer le même schéma de fraude plusieurs fois ;
- Les clients ne sont pas toujours informés des risques potentiels et ne sont pas assez vigilants ;
- La course à « de meilleures expériences utilisateur » amène les établissements à demander de moins en moins de pièces justificatives (ou d'informations), même si cela est compensé par le renforcement des obligations réglementaires en termes de blanchiment d'argent.

Les systèmes de lutte contre la fraude sont majoritairement basés aujourd'hui sur des ensembles de règles complexes pouvant être associés à l'utilisation de fichiers d'exclusions à la manière des systèmes de lutte contre le blanchiment. Ils sont généralement complétés par une intervention humaine (reconnaissance d'un document lourdement falsifié, d'une incohérence dans les informations communiquées…) qui ne peut être aujourd'hui automatisée.

Les règles mises en place dans ces systèmes sont construites sur la base d'hypothèses initiales et agrémentées plus ou moins régulièrement d'analyses pour identifier de nouvelles règles afin de contrer les mécanismes nouveaux que les fraudeurs pourraient inventer.

Les systèmes basés sur l'apprentissage devraient se développer pour venir en support de ceux existants. En effet, ces approches montrent aujourd'hui des capacités de détection supérieures aux systèmes à scénarios lorsque les algorithmes d'apprentissage sont correctement configurés avec un taux de faux positifs suffisamment faible pour que l'expérience utilisateur ne soit pas négativement impactée.

À ces systèmes experts viennent s'ajouter des systèmes de reconnaissance visuelle notamment pour lutter contre la fraude documentaire (systèmes d'OCR – *Optical Caracter Recognition*).

Les enjeux

Aujourd'hui, plusieurs freins au développement plus large de ces systèmes sont

identifiés, notamment deux principaux :

- La capacité à identifier un cas de fraude. En effet, dans beaucoup de cas, notamment en assurance, la fraude existe mais n'est pas détectée, car aucune plainte n'est déposée. Dans ce cas, le système, apprenant sur un historique faux, aura des difficultés à identifier de nouveaux fraudeurs ;
- La transparence des algorithmes (DIP 15).

Pistes de résolution et recommandations

Un travail conséquent au niveau de l'amélioration de la quantité et la qualité des données doit être réalisé afin de mieux nourrir les systèmes de *machine learning*. En accord avec les cadres réglementaires intersectoriel (RGPD, loi Informatique et Libertés) et propre au domaine bancaire et financier (secret bancaire), la mise en commun des jeux de données issus de plusieurs acteurs financiers avec des techniques d'anonymisation réconciliant un individu entre plusieurs banques permettrait de développer des systèmes beaucoup plus performants (DIP 16).

Le recours à des algorithmes apprenants plus évolués offrirait de meilleures capacités de détection.

La recherche sur la transparence des algorithmes et le développement de partenariats avec des acteurs fournissant dès aujourd'hui des approches évoluées et transparentes doivent être favorisés (DIP 15).

Les acteurs de la lutte contre la fraude documentaire mettent en avant l'importance des processus de vérification KYC. Ces derniers permettent de vérifier l'identité des clients et des prestataires d'une entreprise via la production et le contrôle de documents tels qu'un extrait de Kbis récent, une copie de RIB, les statuts de la société certifiés conformes, un justificatif d'identité du gérant de la société, etc. Différents outils existent contre ce type de fraude. Certains donnent un score de conformité au document, d'autres réalisent des contrôles de cohérence par rapport à des bases de données externes.

Le recours à des systèmes intégrant une reconnaissance de la parole et notamment des émotions pourrait permettre de détecter des fraudes lors d'appels téléphoniques.

DIP 10 : vers un dialogue humain-machine empathique

Au-delà de sa capacité de raisonnement, l'efficacité d'un système exploitant l'IA dépend aussi d'une interaction humain-machine réussie. Il est nécessaire, comme dans le cadre du conseiller ou collaborateur augmenté (DIP 2 et DIP 3), que les machines fournissent aux utilisateurs les informations leur permettant de reprendre la main au moment opportun, avec les éléments nécessaires pour continuer l'action. Les interfaces humain-machine (IHM), aujourd'hui multimodales, permettent de couvrir différents types d'interactions. Les IHM usuelles (textuelles, graphiques, vocales) peuvent être complétées par des interfaces gestuelles, tactiles ou encore AR/VR[30] déjà très présentes dans l'univers des jeux vidéo.

Ainsi, les interactions avec des agents conversationnels, personnages virtuels qui dialoguent avec des utilisateurs à travers un langage verbal et non verbal (voir Focus Retour d'expérience Orange Bank sur le déploiement d'un chatbot) ou des systèmes robotiques (robots de l'usine du futur) sont appelées à se développer.

Cependant, la communication humaine repose aussi sur une compréhension des émotions, parfois des sentiments, permettant alors une adaptation de la teneur des échanges au plan sémantique et au plan non verbal. Cette adaptation est plus ou moins efficiente en fonction de la capacité de l'agent de comprendre l'état émotionnel de son interlocuteur, voire de comprendre au mieux ses intentions au travers de ces éléments émotionnels. Une inadéquation dans cette interprétation peut conduire à une incompréhension pouvant aller jusqu'à une opposition directe, voire une rupture du dialogue.

Cette **détection et compréhension des émotions, des sentiments et des intentions** repose chez l'humain sur l'analyse des signaux émis par les interlocuteurs, sur un ensemble de capacités cognitives s'appuyant sur des circuits neuronaux (comme les neurones miroirs) et enfin sur un long apprentissage épigénétique, développemental, éducatif et social.

Dans le cas d'une interaction entre un agent virtuel et une personne, une lecture incomplète ou fausse des émotions peut conduire à une expérience utilisateur défavorable ou à une réaction contraire à l'effet voulu. L'émotion est alors véhiculée par le contenu du dialogue, l'intonation ou la variation de la fréquence de la voix et par un ensemble d'expressions faciales et corporelles. Par exemple, pour les serveurs vocaux interactifs des services clients, l'aspect de la détection des émotions, au cours d'un appel téléphonique prend tout son sens afin que les bots proposent différentes solutions au client selon qu'il est manifestement en colère, tendu ou calme. Il est alors envisageable que des composants d'analyse du contenu ou de variation vocale soient intégrés dans

30. La réalité virtuelle (VR ou RV) et la réalité augmentée (AR ou RA) sont deux technologies sœurs qui ont pour ambition de se substituer aux interfaces traditionnelles, sur écrans plats. Leur principale caractéristique est l'immersion : le fait soit de plonger l'utilisateur dans un environnement virtuel (VR), soit de faire apparaître des éléments virtuels dans l'environnement réel de l'utilisateur (AR).

les agents conversationnels de l'industrie financière.

Le contrepoint dans le dialogue humain-machine de cette capacité de compréhension et de détection par l'agent virtuel des états émotionnels du locuteur humain est la capacité à **générer** en retour **une réponse dotée d'une expression empathique adaptée et orientée**. Cette génération assure donc la fonction émettrice de la communication humain-machine et se présente ainsi comme le processus réciproque de la compréhension automatique (il s'agit là d'exprimer au lieu de comprendre).

L'attendu en sortie d'un générateur doit être du même type que les données d'entrée d'un système de compréhension. Il peut donc s'agir de productions linguistiques (synthèse vocale ou textuelle), mais aussi de signes dans le cadre d'interaction avec les malentendants. De plus, pour que l'usage des agents conversationnels soit adopté par tous (quelle que soit la classe sociale, la culture ou la génération), il est important qu'il soit aussi réaliste que possible et donc doté de capacités telles que l'empathie, l'émotion…

Enjeux

Au-delà de son aspect innovant, l'agent conversationnel est là non pas pour remplacer l'humain, mais pour apporter une valeur ajoutée à l'internaute et une qualité de service supplémentaire. Il peut, en particulier dans le support client, répondre à des questions standards de manière accessible par tous.
Cependant, il reste encore du chemin à parcourir avant de concevoir un agent virtuel capable de détecter et comprendre les émotions dans un flux audio ou vidéo… D'où l'importance des travaux qui existent aujourd'hui autour de **la détection d'émotion ou de l'analyse de sentiment**. Néanmoins, ce champ de recherche est moins avancé que celui de la compréhension du langage naturel. Pour le vocal, la palette des émotions véhiculées par les voix humaines est infinie et rendre une machine capable de les identifier à coup sûr reste un véritable défi. La détection de sentiments voire d'intentions est plus complexe, car elle nécessite une compréhension du contexte de l'interaction pour le premier point et de l'historique des réactions pour le second. Une autre limite importante correspond à la granularité des émotions de référence pour les solutions à base d'apprentissage, liée à la nature des jeux existants de données labélisées. Enfin, dans le domaine de la réaction émotionnelle, une approche personnalisée semble plus souhaitable afin de mieux caractériser des ensembles de signaux faibles permettant de détecter un point d'inflexion dans un continuum émotionnel. Une détection trop lente risque d'induire une réaction tardive de l'agent autonome, qui pourra à son tour être méjugée par l'interlocuteur humain.

Outre le fait d'essayer de comprendre l'objet d'une question, le second enjeu est de **générer des réponses élaborées, cohérentes et compréhensibles par l'humain afin de poursuivre l'interaction**. Ce qui signifie qu'un processus de génération de langage (parlé, écrit ou par signes) doit être développé, de même qu'une interface bien réfléchie et bien conçue. Il existe beaucoup de technologies matures, principalement issues des jeux vidéo, pour animer de tels avatars. Certaines reposent sur des approches statistiques ou d'apprentissage automatique. Elles permettent à

la fois d'intégrer proprement l'incertitude inhérente au traîtement des données en provenance de l'utilisateur (par exemple la parole), mais aussi de pouvoir envisager l'optimisation automatique de la politique d'interaction à partir de données grâce à l'apprentissage par renforcement. Néanmoins, le dialogue entre un humain et une machine n'est pas encore similaire au dialogue naturel entre deux humains. Hybrider plusieurs techniques permettrait de gagner en fluidité, par exemple avec le couplage de l'analyse linguistique, l'identification des actes de dialogue, la compréhension des intentions et des mécanismes de raisonnement pour produire un message doté d'empathie en retour.

Pistes de résolution et recommandations

Pour avancer, certaines approches réduisent le problème de **la détection des émotions** à celui plus simple et limité de la reconnaissance de quatre états émotionnels : la tristesse, la joie, la colère et la neutralité. Elles sont souvent basées sur un apprentissage supervisé, mais supposent de disposer de corpus annotés. On peut dans ce cas utiliser des corpus (publics) existants issus d'autres domaines comme ceux des centres d'appel.

Cependant, les solutions multimodales, couplant la détection d'émotion via des signes corporels (au travers d'analyse d'images ou de vidéo) à l'analyse de la voix (acoustique, prosodique et sémantique) posent un réel défi, à la fois du côté des outils algorithmiques de fusion et sur la création d'une véritable base de données annotées multisources. De plus, au-delà de la simple corrélation, la concordance cognitive entre les sources d'information doit être mieux comprise, car certaines personnes comme les malvoyants basent leur interprétation sur des signaux acoustiques et sont capables de détecter un mensonge à la voix mieux que les personnes à la vue non altérée.

Dans les premiers **systèmes simples de dialogue (utilisant des questions fermées)** comme ceux de certains centres d'appel, la discussion est guidée par l'agent conversationnel d'après un *workflow* prédéfini et l'interaction peut sembler rapidement limitée. L'intelligence du *workflow* et des messages d'erreurs sont donc autant de points importants à imaginer lors de la génération des réponses. **Les systèmes plus évolués (discussion ouverte)** se basent sur trois familles d'algorithmes. La première est entièrement basée sur l'apprentissage machine : le système apprend à partir d'exemples, comment exprimer telle ou telle notion dans un langage donné (que ce soit une langue ou un langage symbolique comme la langue des signes). La deuxième famille d'algorithmes, dite à base de règles, repose uniquement sur la connaissance des différentes modalités d'interactions humaines. Enfin, la troisième famille hybride ces méthodes afin de profiter du meilleur des deux mondes.

Cependant, l'écrit doit se séparer des autres modalités. En effet, l'écrit rend plus difficilement compte d'une émotion alors que l'oral peut transmettre des inflexions plus fines. À l'écrit, le discours doit absolument transmettre, dans son choix de vocabulaire (sémantique) et dans le ton général, l'émotion adaptée. Enfin, il faut ajouter à cela une capacité de génération de dialogue dans des langages spécifiques comme les expressions faciales ou le langage des signes, rarement présents dans les chatbots.

Concevoir ces agents conversationnels implique de les doter d'une certaine forme d'intelligence socio-émotionnelle. Celle-ci doit leur permettre de gérer la dimension intrinsèquement sociale et émotionnelle de l'interaction humain-machine, en adoptant un comportement émotionnel et une attitude sociale adaptés au contexte de l'interaction. De plus, ces agents devraient pouvoir être capables d'exprimer leur attitude vis-à-vis de l'utilisateur non pas seulement à travers des mots, mais aussi à travers leur comportement non verbal.

Pour répondre à cette problématique, une approche est de construire à partir de la perception de l'utilisateur un agent capable de raisonner sur le contexte de l'interaction pour déterminer quel comportement adopter dans une situation. Ces systèmes doivent aussi dépasser une détection d'émotion figée dans le temps pour intégrer une dynamique conversationnelle, par exemple en détectant qu'il s'est passé quelque chose dans l'environnement cognitif de l'interlocuteur, pour évoluer quand cela est nécessaire vers une certaine forme d'empathie. Par ailleurs, il est nécessaire de construire des bases de données d'apprentissage réalistes et de travailler sur les algorithmes de fusion que ce soit au niveau bas (des capteurs : fusion de données) et qu'au niveau sémantique (des décisions : fusion sémantique information-connaissance).

Il est aussi essentiel de prendre en compte l'ensemble de la population visée pour la conception de tels systèmes. En effet, pour la génération textuelle, le degré de littératie limite souvent la compréhension de messages écrits longs et techniques. De plus, une part importante de la population nécessite soit une adaptation des moyens usuels de communication, par exemple une parole ralentie pour des personnes âgées ou le langage des signes pour les malentendants. Proposer des règles de transitions sur la base de modèles personnalisés en fonction de l'interlocuteur et de l'historique récent ainsi que des mécanismes d'apprentissage devient alors nécessaire. Ainsi, la création d'agents capables de simuler des émotions, des sentiments voire des intentions de façon située, faisant sens de façon écologique pour l'interlocuteur humain, pourrait avoir un impact fort pour la socialisation des générations natives du numérique.

Enfin, un axe prometteur pour le dialogue homme-machine, mais peu abordé aujourd'hui, est celui de la reconnaissance d'intention, permettant ainsi de générer des réponses adéquates. Pour cela, il est nécessaire de proposer des mécanismes de raisonnement que l'on pourrait baser sur le sens commun (*common sense*).

2.4 LES CONDITIONS D'UN DÉPLOIEMENT RÉUSSI : FACILITER LA MISE À L'ÉCHELLE ET CRÉER LES CONDITIONS DE LA CONFIANCE

Trop souvent, l'insertion de l'IA dans des produits/solutions/services est abordée comme un problème technologique alors qu'elle est aussi d'ordre organisationnel, culturel et donc humain. Avant de lancer dans l'aventure de l'IA, il est essentiel de bien identifier le périmètre du premier projet. En effet, si l'on souhaite l'adhésion des équipes et du management, il est important de classer les potentiels POC par une analyse ROI/complexité, tout en réfléchissant à la pérennité du service ou du produit visé. Pour cela, il est également indispensable de prendre en compte les impacts de l'introduction de l'IA sur l'évolution et la transformation des métiers, ses aspects éthiques ainsi que la discrimination et les biais que peuvent intégrer les algorithmes. Enfin, l'un des enjeux majeurs d'un déploiement réussi de l'IA sera aussi celui de son explicabilité. Ces différents points seront abordés dans les DIP suivants.

DIP 11 : accompagner la transformation des métiers

Comme souligné par les DIP précédents, l'IA va assister et augmenter les collaborateurs et les managers dans la réalisation de nombreuses tâches, en particulier celles à faible valeur ajoutée. Contrairement à ce a pu être dit, l'IA ne va pas supprimer des emplois, mais les transformer voire même dans certains cas, en créer de nouveaux.

« 67 % des professionnels de la banque pensent que l'intelligence artificielle leur offrira de nouvelles perspectives de carrière. »

Groupe BPCE

Cependant, le marché du travail, y compris dans la finance, est encore très segmenté par métiers et va donc devoir se réorganiser. L'IA va non seulement permettre une évolution des tâches et des compétences, mais également faire émerger une nouvelle catégorie de travailleurs capables de gérer des situations auparavant dévolues aux professions intellectuelles, comme l'indique l'étude de McKinsey[31] publiée en mai 2018.

Aujourd'hui, le débat sur le volume d'emplois concernés n'est pas tranché. En 2013[32], une étude estimait à 47 % la part des emplois aux USA à risque élevé d'automatisation. L'étude de l'OCDE en 2016[33] modère ce propos, prévoyant que les emplois les moins

31. Étude McKinsey Mai 2018, Skill shift : automation and The future of the Workforce.
32. The future of employment : How susceptible are jobs to computerization?, C.B. Frey, MA Osborne, 2013.
33. The risk of Automation for jobs in OECD countries: a comparative analysis», OCDE mai 2016.

qualifiés restent les plus susceptibles d'automatisation pour 40 % des travailleurs ayant un niveau inférieur au bac contre 5 % pour les diplômés de l'enseignement universitaire.

Pour la France, le conseil d'orientation de l'emploi (COE) retient que « moins de 10 % des emplois existants présentent un cumul de vulnérabilités susceptibles de menacer leur existence dans un contexte d'automatisation et de numérisation » et qu'environ 50 % des emplois existants sont susceptibles d'évoluer de façon significative. Selon le World Economic Forum[34], il s'agit d'une *« révolution de la requalification »* à grande échelle.

Enjeux

Comme les tâches changent, les emplois auront besoin d'être redéfinis. Ainsi, pour rester compétitif, il devient nécessaire de réaliser des changements organisationnels. De plus, d'autres facteurs que techniques sont à prendre en compte, comme le niveau de formation, les nouveaux usages, les obligations réglementaires, l'éthique…

Pour les dirigeants, le premier défi à relever en termes de ressources humaines est de *« repenser l'organisation du travail, la répartition des tâches entre humains et IA »*.

« Le troisième hiver de l'IA pourrait être humain et social. »

Bertrand Braunschweig, Directeur du centre de recherche INRIA de Saclay, faisant référence aux deux précédents hivers de l'IA (1974-1980 et 1987-1993) dus aux freins technologiques.

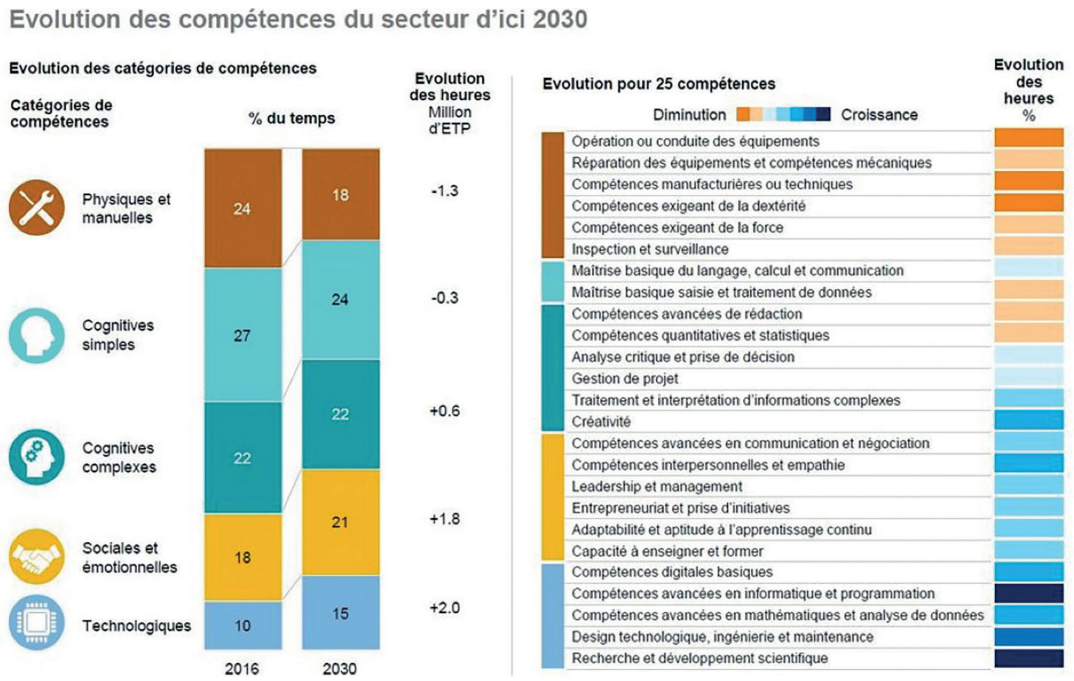


Figure 8 : évolution des compétences du secteur de la finance selon MacKinsey.

34. « Towards a reskilling Revolution, A Future of Jobs for All », janvier 2018.

Certaines entreprises l'ont déjà compris et ont mis en place des séminaires de sensibilisation pour les managers, les commerciaux, et les usagers. Elles ont aussi déployé une organisation agile où les employés sont en équipes autonomes et flexibles. Cependant, tous ne sont pas « digital addict » et il est donc important de développer les compétences correspondant aux besoins des employeurs et d'offrir des outils simples à utiliser.

Même si beaucoup parlent de « guerre des talents » (les entreprises s'arrachant aujourd'hui les étudiants formés en IA et en science des données pour répondre à leurs besoins de transformation numérique), les compétences sociales et émotionnelles comme inventer de nouveaux usages, négocier, manager, communiquer ainsi que la gestion de projets, la lecture ou l'écriture de niveau supérieur[35] vont être recherchées.

En effet, les questions de complémentarité et de partage entre l'humain et la machine vont devenir cruciales[36]. Comme le souligne le rapport Althling[37], cette évolution du profit des compétences transversales pose de nouvelles questions :

- leur définition ;
- leur identification ;
- leur reconnaissance (en interne, mais aussi sur le marché du travail dans une logique d'employabilité) ;
- leur évaluation…

Pistes de résolution et recommandations

Pour accompagner cette évolution, voire cette transformation des métiers au sein de l'industrie financière, il est important de se poser les questions suivantes :

- Comment l'IA est-elle susceptible d'affecter les postes actuels ?
- Quelles fonctions du monde de la finance l'IA remplacera-t-elle à terme ?
- À contrario, quelles fonctions ne pourront pas être remplacées ?

L'IA peut même être considérée comme un thème privilégié de dialogue social, ce que les syndicats ont bien compris.

Celui-ci gagnerait à être accompagné par une action généralisée dans l'entreprise par une acculturation (voir le DIP 10) et en favorisant le partage d'informations et de connaissances afin de permettre à l'ensemble des collaborateurs de comprendre les transformations en cours.

Cependant, l'IA devrait aussi permettre de faciliter l'apprentissage de ces nouveaux métiers dans la mesure où les compétences techniques sont bien plus faciles à automatiser que les compétences générales (empathie, leadership, créativité…). Dans ce contexte, la formation continue couplée avec une mise en pratique pourrait suffire.

Gérer les impacts de l'IA sur l'emploi nécessite donc la coordination de toutes les parties prenantes de la société. Il faut ainsi :

- Intégrer des scénarii de développement de nouvelles activités liées à l'IA dans l'entreprise ;
- Mettre en place des évaluations des impacts sur emplois et compétences et

35. Étude McKinsey Mai 2018, Skill shift: automation and the future of the Workforce.
36. Villani, C. et coll. (2018) « Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne », téléchargeable sur www.aiforhumanity.fr.
37. L'intelligence artificielle dans la banque : emploi et compétences, décembre 2017, Athling.

mesurer les transferts de tâches ;

- Anticiper la requalification et repérer les formations adaptées (DIP 10) ;
- Analyser les projets pilotes en cours de développement au travers du prisme humain et leur impact sur les métiers ;
- Travailler avec les branches métiers pour participer à une gestion collective de la transformation (fédérations métiers bancaires et d'assurances) ;
- Concevoir des outils d'aide à l'analyse de la chaîne de valeur et de l'évolution des structures de l'entreprise en fonction du degré de pénétration de l'IA dans chacun de ses processus ;
- Concevoir des parcours de progression-promotion et de formation qui anticipent et optimisent les besoins de l'entreprise en fonction de son évolution stratégique, du niveau de pénétration de l'IA dans les fonctions-métier et des aspirations des collaborateurs ;
- Favoriser les partenariats avec des startups et des spécialistes en IA et data sciences en particulier, pour pallier aux pénuries des talents (linguistique, gestion de la connaissance, raisonnement, dialogue…).

DIP 12 : acculturer et former à l'IA

Comme tout outil, il est indispensable de comprendre le rôle, les usages, le fonctionnement, les potentialités et les limites de l'IA. Conçue par et pour l'humain, nous allons tous progressivement l'utiliser, la concevoir ou la promouvoir. Pour cela, il est nécessaire d'éduquer et de former à l'IA.

- **Éducation :** il est indispensable d'éduquer dès le jeune âge sur le sujet de l'IA afin d'en préciser les rôles, d'en mesurer ses effets, d'en déterminer les usages et de changer ses modes de pensées ;
- **Formation initiale :** elle doit permettre de former les prochains utilisateurs, promoteurs, juristes, et experts ingénieurs/scientifiques en IA. En effet, une nouvelle industrie et de nouveaux usages vont apparaître, entraînant des formations initiales auprès des futurs ingénieurs, chercheurs, commerciaux, acheteurs de solutions et utilisateurs ;
- De nombreuses formations existent déjà en France autour des data sciences et de l'intelligence artificielle dirigée par les données (ex. apprentissage), mais celles-ci doivent être complétées par des formations en IA symbolique (peu enseignée aujourd'hui) nécessaire au développement et à l'appropriation des outils d'aide à la décision ou permettant de réaliser des tâches complexes. Il importe également de les élargir pour développer les aspects éthiques, de conduite du changement et des modèles économiques associés. Cela permettra aussi de favoriser l'émergence de nouvelles compétences de chercheurs et d'ingénieurs afin de traiter des problèmes scientifiques non encore résolus et concevoir des solutions plus pertinentes et plus performantes. Enfin, il est important que les futurs ingénieurs/chercheurs comprennent les biais et les imperfections de ces outils pour appréhender de manière rigoureuse les questions de validation, de vérification, de qualification, de certification et d'auditabilité des IA (DIP 15) ;
- **Formation continue :** les entreprises doivent dès maintenant développer de nouveaux programmes de formation continue pour accompagner les salariés éligibles à l'usage (utilisation), à la promotion (marketing, commercialisation…) ou au développement/recherche de nouveaux algorithmes. La formation continue doit concerner tous les niveaux de compétences de l'entreprise à des degrés divers de technicité : formation au numérique et à l'innovation, à la science des données, aux techniques d'apprentissage automatique, à l'ingénierie des connaissances, à l'IA symbolique, au cycle de vie des systèmes à base d'IA allant de la conception à l'industrialisation en passant par la maintenance sans oublier la cybersécurité et la robustesse.

Enfin, en entreprise ou en organisation, chacun doit contribuer à reporter et diffuser ses connaissances sur des intranets afin de partager celles acquises au travers de MOOC[38] ou de liens documentaires…

Enjeux

Le véritable défi reste de franchir le pas entre la simple prise de conscience et la

38. Un MOOC (*Massive Open Online Course*) est un type de formation en ligne, ouvert à tous et à distance capable d'accueillir un grand nombre de participants.

phase de formation.

- Très peu de professionnels parviennent à comprendre l'impact de l'IA sur les fonctions de la finance ;
- Les cours en ligne apparaissent comme une solution, mais là encore, le format ne répond pas forcément aux attentes des étudiants. Les instituts de formation s'accordent à dire qu'environ 90 % des inscrits abandonnent leur formation à mi-chemin faute de temps, de motivation ou d'enseignement de qualité[39].

Recommandations

Employés et cadres dirigeants doivent être sensibilisés et/ou formés. Les dirigeants auront pour tâche de définir la stratégie et le positionnement de l'entreprise et les employés vont devoir utiliser ou mettre en place des solutions à base d'IA.

- Acculturer le public en tenant compte de ses différentes composantes :
  - Le vertical métier, avec focus sur les spécificités de chacun ;
  - Le vertical secteur : fédérations, syndicats, groupements… ;
  - Sensibilisations tous publics à l'IA et travailler sur l'avenir collectif en favorisant l'échange : *think tanks* intégrant la diversité[40], groupes thématiques… ;
  - Adaptation aux changements permanents ;
- Former les spécialistes et praticiens de l'IA et assurer le recrutement de nouveaux profils (développeur IA, ingénieur data, data scientist, data miner, chief data officer) ;
- Développer les compétences moins aisément gérées par l'IA (*soft skills*) : l'intelligence émotionnelle, la créativité, la pensée critique, l'empathie, le jugement éthique ;
- Définir l'approche pédagogique spécifique à l'IA ;
- Présenter les valeurs ajoutées de l'IA sur les métiers et chaînes de valeur ;
- Adopter une démarche d'expérimentation « *Test & Learn* » :
  - Le *Test & Learn* pour démystifier l'IA : associer les collaborateurs à la démarche d'expérimentation participative (co-création) permet de diminuer rapidement les appréhensions et les craintes en développant des pilotes et de se rendre compte des gains potentiels de la technologie ;
- Mettre en place avec les institutions de formation, universités et centres de recherche un réseau de partenariat avec cycles de conférences pour évangéliser sur les réalisations à effectuer sur les métiers des entreprises ;
- Former les formateurs et les référents : auditeurs, inspecteurs…

Ce n'est que par le biais d'une formation continue tout au long de sa carrière qu'un professionnel de la finance sera en mesure de maîtriser l'application de l'IA au quotidien. L'apprentissage de l'IA ne représente donc pas une fin en soi, mais un parcours.

39. www.formaguide.com/s-informer/mooc-un-grand-chantier-pour-l-enseignement-superieur.
40. *« Les femmes doivent comprendre que le code, l'IA et l'ensemble des métiers du numérique sont pour elles une formidable opportunité d'émancipation et d'action. »* - Aurélie Jean, scientifique numéricienne et entrepreneuse.

Focus
Formation professionnelle en finance : de la théorie à la pratique à Singapour

Avec l'arrivée de nouvelles technologies comme l'IA, les gouvernements, les institutions bancaires et les employés eux-mêmes évoquent tous l'importance d'une formation continue tout au long de leur carrière afin de mieux appréhender les nouveaux défis et enjeux du secteur. Cependant, la prise de conscience s'arrête là. En pratique, la plupart des institutions financières ne parviennent pas encore à mettre en place les mécanismes nécessaires à la formation et à l'éducation de leurs employés.

Le vrai défi à l'heure actuelle reste donc de franchir le pas entre la prise de conscience et la phase éducative.

Pourtant, l'exemple de Singapour est là pour nous rappeler que de tels investissements sont possibles. OCBC Bank et United Overseas Bank (UOB), par exemple, ont annoncé en début d'année leur intention de former leurs employés par le biais du cours « AI in Finance ».

Bien plus qu'un simple effet d'annonce, l'initiative prise par ces deux banques illustre la volonté de l'État de former ses citoyens à l'intelligence artificielle. Ainsi, lors d'un discours prononcé au FinTech Festival en novembre 2016, Ravi Menon, directeur du Monetary Authority of Singapore (MAS), exprimait déjà son souhait de former de nouveaux talents aux compétences du numérique.

Dès lors, un véritable écosystème est apparu. Tous les acteurs, que ce soit l'État, le régulateur, les banques, mais aussi les instituts de formation, se sont réunis pour déployer massivement l'enseignement de l'intelligence artificielle.

Pour cela, deux nouvelles initiatives ont vu le jour. Tout d'abord, l'Institut de la Banque et de la Finance (IBF) a lancé le « Future Enabled Skills » afin de former les professionnels du secteur aux nouvelles technologies et à leurs implications.

Dans un deuxième temps, le gouvernement singapourien a mis en place le « Skillsfuture Singapore » (SSG) qui relève du Ministère de l'Éducation et qui permet aux Singapouriens de suivre des heures de formation en vue d'évoluer dans leur carrière.

Tous les sujets sont abordés. Au total, les citoyens de plus de 25 ans ont accès à plus de 18 000 cours. Le programme « AI in Finance » en fait partie.

Dès le départ, SSG s'est d'ailleurs engagé à subventionner la formation à hauteur de 70 % pour une majorité de Singapouriens. Les plus de 40 ans voient quant à eux leur formation financée à hauteur de 90 %.

À l'instar de nombreux autres États, Singapour a très vite compris que la formation des professionnels de la finance aux technologies nouvelles comme l'IA était essentielle. La seule différence réside probablement dans le fait que, contrairement à d'autres, Singapour a implémenté une stratégie de financement.

Certes, adopter une telle approche dans des pays à la culture et aux processus différents paraît difficile. En revanche, de nombreuses banques à travers le monde ont maintenant la maturité suffisante pour réaliser l'urgence à se transformer. Que ce soit du fait de l'arrivée des fintechs ou parce que les profils s'orientent vers les entreprises de technologie, il est à présent temps pour elles d'évoluer. Et cela passe bien évidemment par la formation de leurs employés.

Le Centre for Finance, Technology and Entrepreneurship (CFTE) a développé le cours « AI in Finance » en partenariat avec l'Institut Polytechnique de Singapour, Ngee Ann. Le cours est entièrement dispensé en ligne et réunit les experts du monde entier. Il s'adresse aussi bien aux employés d'institutions financières qu'aux professeurs d'université qui sont aujourd'hui nombreux à suivre cette formation afin de mettre à jour leurs connaissances.

Focus
Une démarche globale pour sensibiliser les collaborateurs de BNP Paribas Securities Services à l'intelligence artificielle

La transformation digitale de BNP Paribas Securities Services est l'une des principales priorités de la banque. Pour embarquer dans cette transformation ses 10 000 collaborateurs répartis dans 28 pays, Securities Services a choisi d'investir sur le sujet de la formation et de l'acculturation au digital, avec une démarche globale pour répondre aux besoins des différentes cibles et métiers de l'entreprise.

Des sessions d'acculturation en présentiel pour toucher un maximum de collaborateurs

Entre juin 2017 et juin 2018, des sessions de deux heures ont été organisées dans l'ensemble des géographies, animées par des champions digitaux et l'équipe IA, mobilisée pour aller à la rencontre des collaborateurs et répondre à leurs questions.

Le COOC, un format idéal pour diffuser le savoir dans tous les pays

Lancé mi-janvier 2018 sur une durée de deux mois, le COOC sur l'intelligence artificielle a été élu meilleur Dispositif Digital de Formation Corporate par Cegos, lors des Digital Learning Excellence Awards 2018. Conçu pour préparer les équipes à l'arrivée de l'intelligence artificielle, il a été suivi par près de 1 300 collaborateurs volontaires, avec un temps moyen consacré de huit heures et un taux de complétion du parcours de 30%. Il permet de démystifier ce qu'est l'IA dans la réalité et de fournir des clés pour comprendre les impacts et enjeux et de préparer au changement induit par la transformation digitale.

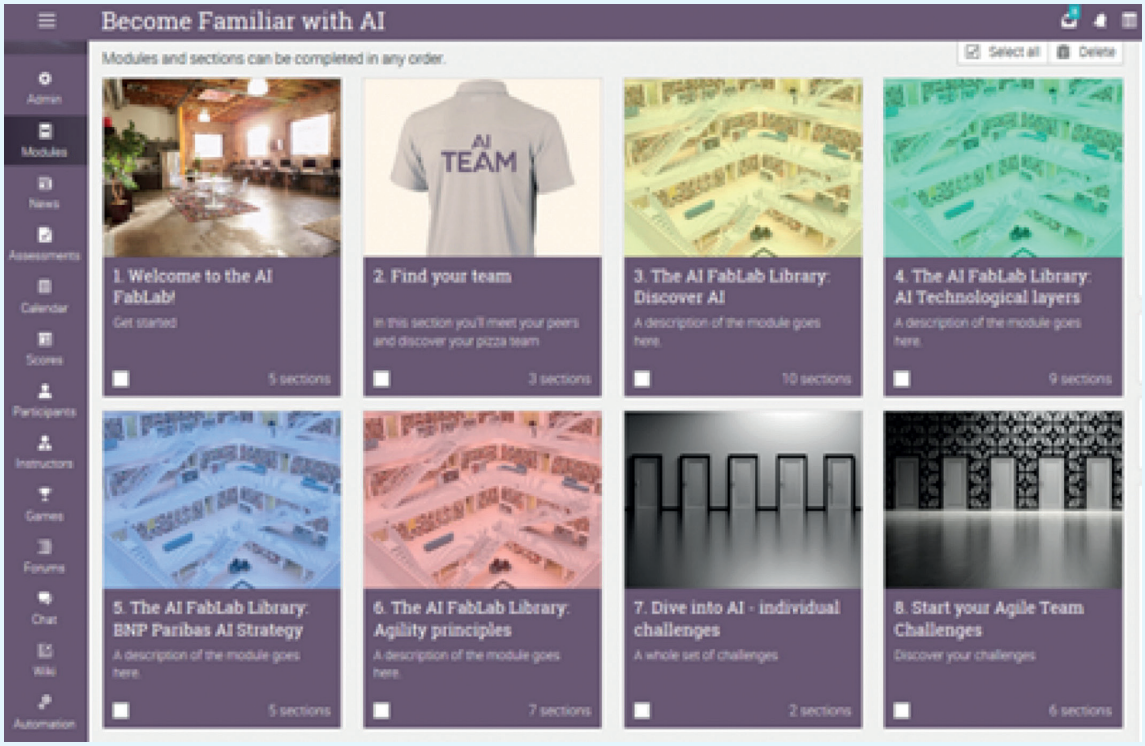


Disponible en français et en anglais, ce programme de sensibilisation comprend un mélange de contenus pédagogiques théoriques et pratiques, répartis dans neuf modules : interviews d'experts, vidéos, infographies, questionnaires, exercices individuels et travaux de groupe, avec la réalisation d'un prototype, et bien sûr des sessions en direct. Le travail collaboratif permet de contribuer à la création de communautés et favorise le partage des meilleures pratiques et de l'expertise liées à l'intelligence artificielle.

Un séminaire dédié pour créer une communauté de 250 personnes autour de l'intelligence artificielle

Les experts de l'intelligence artificielle se sont retrouvés lors d'une Summer School de deux jours en août 2018 pour partager des retours d'expérience et échanger avec des intervenants prestigieux, issus de la recherche (INRIA – Prairie) et d'autres secteurs.


BNP PARIBAS
La banque d'un monde qui change
Meilleur dispositif de formation
« CORPORATE »
ANGLAIS
Evaluation
Attestation de réussite
COOC
10.000 personnes
28 pays
Quiz
Abonnez Vous


Become Familiar with AI
Modules and sections can be completed in any order.
Select all
Delete
Admin
Modules
News
Assessments
Calendar
Scores
Participants
Instructors
Games
Forums
Chat
Wiki
Automation
1. Welcome to the AI FabLab!
Get started
5 sections
2. Find your team
In this section you'll meet your peers and discover your pizza team
3 sections
3. The AI FabLab Library: Discover AI
A description of the module goes here.
10 sections
4. The AI FabLab Library: AI Technological layers
A description of the module goes here.
9 sections
5. The AI FabLab Library: BNP Paribas AI Strategy
A description of the module goes here.
5 sections
6. The AI FabLab Library: Agility principles
A description of the module goes here.
7 sections
7. Dive into AI - individual challenges
A whole set of challenges
2 sections
8. Start your Agile Team Challenges
Discover your challenges
6 sections

DIP 13 : mettre en œuvre les grands principes éthiques

L'IA a cette caractéristique d'être présente dans tous les secteurs, sur tous les sujets et dans tous les esprits et bouscule (ou va bousculer) nos conventions, philosophies et modes de gouvernances. Le corollaire de cette omniprésence est la question centrale de son universalité : l'universalité de compréhension qui génèrera l'universalité de son adoption. L'une des clés d'entrée pour établir la confiance reste la bonne définition de l'éthique. Mais quand on parle d'éthique, de quoi parlons-nous exactement ? Suffit-elle à établir la confiance dans l'adoption de l'IA pour tous ? Peut-elle revêtir un caractère universel ?

Pour bien poser le sujet, il est nécessaire de reprendre la définition de l'Éthique :

« Le mot éthique provient du grec** ethos **qui désigne les mœurs, c'est-à-dire les habitudes de comportement relativement au bien et au mal. En cela, il se rapproche du mot "morale" (qui vient de** mores, **mœurs en latin). Il existe certes des distinctions entre éthique et morale. Celles-ci tiennent sans doute aux différences entre la Grèce et Rome : d'un côté, une culture philosophique éprise de ratiocination ; de l'autre, une civilisation juridique, soucieuse de règles et de lois. Ainsi, la morale énonce les règles de conduite tandis que l'éthique cherche à établir le fondement de ces règles. Aujourd'hui, personne ne doute que l'éthique apporte un "supplément d'âme" aux techniciens, tout en suscitant de nouveaux développements, par exemple, les architectures de logiciels qui préservent la vie privée. »

Jean-Gabriel Ganascia,
Professeur à l'Université de la Sorbonne

Avec le progrès et la complexité de l'IA, l'évaluation des conséquences des choix devient de plus en plus difficile. Les connaissances requises pour parvenir à une décision éclairée demandent des connaissances dont un homme seul ne peut disposer. Et si l'une des pistes était l'universalisme moral ?

« L'universalisme moral est la position méta-éthique qu'un système d'éthique ou une éthique universelle s'applique universellement, c'est-à-dire pour "tous les individus dans la même situation[41]", indépendamment de la culture, de la race, du sexe, de la religion, de la nationalité, de l'orientation sexuelle ou tout autre élément distinctif. »

Wikipedia[42]

Enjeux

- **La définition des valeurs éthiques et morales** à préciser :
  - L'évolution du droit n'est pas celle de la morale ; l'éthique et la morale restent des exercices théoriques qui sont sujets à interprétation selon les

41. Garth Kemerling, « A Dictionary of Philosophical Terms and Names » 12 novembre 2011.
42. https://fr.wikipedia.org/wiki/Universalisme_moral.

cultures et les croyances ;
  - Neutralité : est-il possible de créer une IA neutre (non influencée, non influençable, protégée des lobbies, etc.) ?
- **Rapidité, accélération, non-maitrise :**
  - Une technologie en perpétuelle mutation qui évolue plus vite que nos valeurs et qui peut influencer nos conceptions éthiques ;
  - Les craintes sur la capacité de « garder la main ».

Pistes de résolution

La Déclaration universelle des droits de l'homme des Nations Unies peut être lue comme supposant une sorte d'universalisme moral. Le comité de rédaction de la Déclaration universelle a supposé, ou du moins aspiré, à une approche « universelle » d'articulation des droits humains internationaux. Bien que la Déclaration ne reflète pas adéquatement certaines visions du monde, elle en est indéniablement venue à être acceptée comme une pierre angulaire du système international pour la protection des droits de l'homme et donc pour instaurer une confiance universelle.

L'objectif n'est pas, on le voit, d'atteindre la perfection dans la rédaction d'une éthique universelle de l'IA, mais bien de commencer à établir un consensus mondial sur des critères fondamentaux, sur la base de ceux déjà énoncés et communément admis.

Ce thème est le plus discuté du moment, surtout depuis le début du deuxième semestre 2018. En effet, après de nombreux articles dans de nombreux domaines, aussi bien philosophiques, que sociaux, moraux et juridiques, de nombreux acteurs dans le monde entier ont souhaité lancer des initiatives.

Le point de départ a été, selon nous, le rapport de la CNIL en décembre 2017, qui a fait suite à un débat riche et intéressant.

> ***« Comment permettre à l'Homme de garder la main ? »***
>
> **Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle, CNIL**[43]

Pour l'heure, la plupart des initiatives se sont cantonnées à des serments ou déclarations[44] incitant les professionnels à se conformer à une attitude, à une pensée, à des concepts, c.-à-d. à un code déontologique rendant plus tangible ce désir émis par la communauté mondiale.
Le Serment Holberton-Turing reste le plus remarqué et remarquable par sa hauteur

43. www.cnil.fr/fr/comment-permettre-lhomme-de-garder-la-main-rapport-sur-les-enjeux-ethiques-des-algorithmes-et-de.
44. Voici donc les liens et un résumé de chacune de ces initiatives :
16 mai 2018 : The Toronto Declaration - Protecting the rights to equality and non-discrimination in machine learning systems : www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems;
12 juin 2018 : Google souhaite encadrer le développement de l'IA par sept grands principes – Triple objectif pour ce texte : rassurer le grand public qui découvre de nouvelles technologies et de nouveaux usages, donner un cadre à une industrie en pleine expansion, mais aussi montrer aux employés de l'entreprise que la direction prend au sérieux une polémique récente. : www.siecledigital.fr/2018/06/08/google-encadre-le-developpement-de-lia-par-7-grands-principes ;
Juin 2018 : Data for Good propose un Serment d'Hippocrate pour Data Scientist – cinq principes auxquels les professionnels de la donnée s'engagent à respecter : www.hippocrate.tech ;
Juin 2018 : Confederation of Laboratories for Artificial Intelligence Research in Europe – (C.L.A.I.R.E) - www.claire-ai.org;
15 juin 2018 : Le serment Holberton-Turing pour l'intelligence artificielle au service de l'humain : sur le modèle du serment d'Hippocrate des médecins, Aurélie Jean et Grégory Renard, deux experts de l'intelligence artificielle (IA), proposent un code éthique afin d'encadrer son utilisation par les professionnels de l'IA : www.service-sens.com/le-serment-holberton-turing-pour-lintelligence-artificielle.

de vue. Listant des comportements, mais non des cas d'usages, il a été initié dans l'objectif de fédérer au niveau mondial l'utilisation des compétences des professionnels de l'IA autour de valeurs morales et éthiques communes. Le serment s'articule autour de trois grands principes :

- le respect de la vie et des sciences ;
- l'inclusion ;
- la transmission des connaissances.

Il a été construit à l'image d'un code en logiciel libre, destiné à évoluer dans le temps en fonction des contributions de chaque acteur de l'échiquier technologique et social. Enfin, le serment a été conçu pour être compris par tous les pairs de la discipline, mais aussi par les citoyens qui trouveront dans ce texte une base de réflexion à élargir et à approfondir dans les débats publics.

Recommandations

Mettre la place de l'éthique au centre de nos préoccupations et à tous les stades :

- Éducation initiale et continue : enseignement de l'éthique dans les écoles, universités, entreprises et l'illustrer par des cas d'usages pour la rendre simple d'accès ;
- Former les actuels développeurs en IA pour s'assurer qu'ils génèrent des algorithmes avec des principes éthiques (auto-contrôle), d'où le focus sur le serment d'Holberton-Turing ;
- Former les utilisateurs d'IA à user des applications avec éthique et responsabilité, mais aussi à signaler les problèmes (prendre en compte la législation et l'adapter pour les lanceurs d'alertes) ;
- Former des contrôleurs pour tester et observer les usages de l'IA avant leur diffusion et pendant leur utilisation dans la vie réelle ;
- Soutenir les initiatives citoyennes, les associations de consommateurs, les think tanks… afin qu'ils s'approprient le sujet de l'éthique ;
- Rendre la connaissance de l'IA dynamique, en partageant largement et en favorisant le dialogue et les débats, en créant des chaires de recherche connectées avec la société civile et les entrepreneurs ;
- Tester l'IA avec une autre IA « neutre » sur les scénarios possibles d'interprétations et faire des recommandations d'amélioration ou de précision ;
- Instaurer une Haute Autorité chargée de vérifier le respect des droits fondamentaux, dont les critères d'inclusion et de solidarité dans les applications IA.

Il est à noter que ces préoccupations ont pris très récemment une dimension internationale avec, à l'occasion de la 40e Conférence internationale des commissaires à la protection des données et de la vie privée, l'adoption le 23 octobre 2018 d'une déclaration sur l'éthique et la protection des données dans l'intelligence artificielle. Rédigé par la CNIL et le contrôleur européen de la protection des données de l'Union européenne (CEPD), le texte est désormais ouvert à consultation publique et à contribution jusqu'au 25 janvier 2019[45].

Il semble que ces principes rejoignent nos recommandations fondées sur quelques principes clés :

- Les technologies d'intelligence artificielle et d'apprentissage automatique doivent être conçues, développées et utilisées dans le respect des droits fondamentaux de l'homme et conformé-

45. www.actuia.com/actualite/consultation-publique-ethique-et-protection-des-donnees-dans-lintelligence-artificielle-jusquau-25-janvier-2019.

ment au principe de loyauté ;
- Il est nécessaire de continuer à faire preuve d'attention et de vigilance ;
- Il convient d'améliorer la transparence et l'intelligibilité des systèmes d'IA, l'objectif étant de permettre leur mise en œuvre efficace ;
- Dans le cadre d'une approche globale basée sur l'« Ethics by design » (éthique dès la conception), les systèmes d'IA doivent être conçus et développés de manière responsable ;
- Il convient de donner davantage de pouvoirs à chaque personne et d'encourager l'exercice des droits individuels, tout en créant des opportunités de participation publique,

€ Il convient de réduire et d'atténuer les préjugés ou les discriminations illicites.

Par ailleurs, pour participer à la création d'une gouvernance commune future au niveau international et mieux définir l'orientation qui accompagnera ces principes d'éthique et de protection des données en matière d'IA, la 40e Conférence internationale des commissaires à la protection des données et de la vie privée a établi un groupe de travail permanent dont la mission sera de relever les défis associés au développement de l'intelligence artificielle.

Ce groupe de travail sera chargé de favoriser la compréhension et le respect des principes de la résolution par toutes les parties concernées impliquées dans le développement des systèmes d'intelligence artificielle, y compris les gouvernements et les autorités publiques, les organismes de normalisation, les concepteurs de systèmes d'intelligence artificielle, les prestataires et les chercheurs, les entreprises, les citoyens et les utilisateurs finaux de ces systèmes.

DIP 14 : lutter contre la discrimination et les biais

L'IA s'intègre de plus en plus dans les processus de décision ayant un impact fort sur la vie des individus, de l'attribution d'un prêt bancaire à l'orientation de leur cursus universitaire. Cette nouvelle chaîne de valeur qui raisonne de façon systémique, pour ne pas dire écosystémique, est amenée à avoir un impact majeur sur la société.

Si, du fait de son caractère technique, l'IA peut être perçue comme neutre, elle n'est en réalité pas exempte de biais. En effet, un certain nombre de techniques d'IA sont basées sur l'exploitation de données, en particulier celles fondées sur des algorithmes d'apprentissage. Or, les données ne sont pas objectives, en ce sens qu'elles sont toujours le fruit d'une sélection, d'un échantillonnage du réel et fournies dans une représentation qui a une grande incidence sur les traîtements ultérieurs. Cela peut être source de discriminations.

Ainsi les systèmes d'IA fondés sur l'apprentissage retranscrivent des situations observées dans les données historiques du monde réel et extraient des règles de conduite qui les généralisent. De ce fait, s'il l'on n'y prend pas garde, ces systèmes reproduisent et perpétuent les injustices, voire les discriminations existantes.

Les données et leur exploitation permettent de programmer automatiquement des systèmes informatiques qui reconduisent les décisions anciennes. Ils tiennent compte de l'usage, mais ne comportent aucune autre source prescriptive, nécessaire si l'on veut corriger les inégalités existantes.

Enjeux

Concernant les **données** :

- Comment définir la source des données : peut-on utiliser toutes les données pour n'importe quelle finalité ?
- Notion de responsabilité : définir le propriétaire de la donnée. Pour une donnée précise, qui a le droit de la manipuler ? Et à qui les résultats peuvent-ils être communiqués ?
- Comment s'assure-t-on que les critères retenus ne sont pas discriminants ?
- Comment s'assure-t-on que les jeux de données ne sont pas eux aussi discriminants (ex. : jeux de données servant à l'apprentissage de la reconnaissance faciale et qui peuvent être biaisés sur le genre ou l'origine ethnique) ?
- Le développeur va malgré lui injecter ses propres biais de perception du monde dans l'algorithme qu'il construit. Comment s'en prémunir ?
- Le choix du critère à optimiser dans l'algorithme génère des biais (ex. : systèmes de recommandation de YouTube qui proposent aux internautes les vidéos les plus extrêmes et qui « buzzent »).

La chaîne de valeur d'un **algorithme** se partage entre différents acteurs :

- les concepteurs qui ont la responsabilité morale de réfléchir à l'usage de la technologie qu'ils conçoivent ;
- les vendeurs qui doivent s'assurer que la solution qu'ils proposent est bien adaptée aux besoins de leurs clients ;
- les utilisateurs des solutions, qui sont de plus ceux qui vont manipuler les données et en tirer des actions, sont

concernés comme le maillon agissant de la chaîne.

Les solutions d'IA sont des boîtes noires pour les utilisateurs : dès lors, comment les entreprises les utilisant peuvent-elles contrôler la bonne exécution des algorithmes ?

Les bulles ou le risque de surpersonnalisation doivent être pris en compte :

- Comment se prémunir du risque d'accumulation de stratégies identiques, du manque de créativité et du conformisme qui peuvent résulter de l'utilisation de l'IA ?
- Comment protège-t-on la liberté d'accès à toutes les informations et l'égalité de traîtement des clients d'un service ?

L'assurance a par définition un fonctionnement mutualiste : le tarif d'une police dépend de quelques critères permettant de caractériser l'appartenance d'un client à un groupe de taille statistiquement significative (ex. : clients masculins entre 30 et 40 ans, vivant en région parisienne). L'accès potentiel à de nombreuses sources de données combinées avec des techniques d'IA permettant de caractériser individuellement chaque client ne risque-t-il pas d'amener vers une tarification complètement individualisée, effaçant ce caractère mutualiste ?

Pistes de résolution

Les algorithmes d'IA étant complexes et résultant de nombreuses interactions entre plusieurs d'entre eux, l'analyse du contenu de ces « boîtes noires » s'avère extrêmement complexe. Cependant, pour s'assurer de l'absence de discrimination et de biais, il est nécessaire de s'assurer de l'explicabilité des résultats. Cette piste a été initiée par des chercheurs (*Equality of Opportunity in Supervised Learning*, Moritz Hardt, Eric Price, Nathan Srebro, 07/10/2016), des groupements d'entreprises privées (Partnership on AI) ainsi que par les autorités publiques (RGPD).

Par ailleurs, il est également nécessaire de s'assurer que les données utilisées pour calibrer les algorithmes ne présentent pas de biais, aussi bien dans les champs retenus que dans le choix des individus constituant la base d'apprentissage. Comme le savent les concepteurs de solution d'apprentissage « *garbage in, garbage out* », un algorithme n'est jamais de meilleure qualité que celle des données utilisées pour le calibrer. L'analyse préalable des données en entrée est donc d'une importance majeure dans la construction de dispositifs d'IA. Ce travail a l'avantage de s'appuyer sur des outils disponibles et répandus au sein de la communauté.

Recommandations

- Mettre en œuvre une association de place afin de surveiller dans la durée les nouveaux usages de l'IA et l'utilisation de nouvelles sources de données dans le secteur financier ;
- Disposer d'outils de contrôles et de gouvernance au sein des entreprises afin de s'assurer à la fois de la fidélité (la bonne transmission des connaissances quant au fonctionnement de l'algorithme) et de l'homogénéité (l'algorithme fait bien ce pour quoi il est programmé) des algorithmes ;
- Avoir des protocoles de test des algorithmes afin de détecter les potentiels biais avant qu'ils ne soient mis en production ;
- Mettre en place un outil de suivi des risques qui permet :

  - une analyse en amont au cas par cas de « type risque » ;
  - d'identifier à la sortie de la solution qu'elle se prémunit bien des biais trouvés dans l'analyse ;
  - à surveillance continue des résultats produits (approche statistique/sociale), en particulier sur les populations à risque ;
- S'assurer de la diversité et de l'interdisciplinarité des profils des concepteurs, développeurs d'algorithmes pour éviter des biais cognitifs.

DIP 15 : expliquer et auditer l'IA

De plus en plus de systèmes à base d'IA peuvent avoir un impact sur nos vies. Ils embarquent des algorithmes pour qualifier les demandes de prêt, gérer les patrimoines, analyser de manière automatique les CV, aider aux diagnostics médicaux, surveiller des sites critiques... Les décisions publiques sont aussi concernées : lutte contre la fraude fiscale, attribution d'un logement social, affectation des élèves dans un établissement scolaire ou des étudiants à une formation...

Qu'ils reposent sur des techniques d'apprentissage ou sur des approches plus symboliques, la conception de ces algorithmes n'est pas neutre, leurs résultats produits ne sont pas forcément corrects et leurs performances évoluent au cours du temps, soit par leur capacité intrinsèque d'apprentissage, soit par l'évolution de leur environnement. De plus, l'impact des données utilisées pour l'apprentissage s'avère critique pour leur fonctionnement.

En effet, ces algorithmes (qu'ils soient à base d'apprentissage ou d'IA symboliques) mettent en œuvre, le plus souvent de manière opaque et parfois non maîtrisée, des critères de priorité, de préférence et de classement qui ne sont généralement pas connus des personnes concernées. Cette opacité peut aussi masquer toutes sortes de dérives : discriminations, traîtements déloyaux, manipulation, etc.

Du point de vue de l'usager, le véritable besoin est d'avoir une explication intelligible (explicabilité) plus que la traçabilité du raisonnement. En effet, le fonctionnement de l'algorithme sous-jacent n'a que peu d'intérêt pour eux : il s'agit surtout d'obtenir une explication utile pour en comprendre voire interpréter les résultats. Cependant, fournir ces explications n'est pas simple, surtout quand les algorithmes reposent sur des techniques d'apprentissage. Même leurs concepteurs ne sont aujourd'hui pas en mesure d'analyser par quel raisonnement ces méthodes parviennent à leurs résultats. C'est l'effet « boîte noire ».

Du point de vue des entreprises, des organisations, des pouvoirs publics et des usagers, comprendre ces boîtes noires et garantir leur comportement vont devenir un enjeu majeur. En particulier si l'on veut favoriser l'insertion de composants d'IA pour l'industrie financière ou dans des applications critiques, que ce soit pour la mobilité, la médecine, l'aéronautique, la défense et la sécurité.

Enjeux

Pendant de nombreuses années, la performance a été privilégiée par rapport à **l'explicabilité** et **l'interprétabilité**, ces deux néologismes provenant de l'anglais, qui font référence à l'intelligibilité des algorithmes. Par exemple, avec les techniques d'apprentissage automatique, d'un point de vue mathématique, la recherche d'un bon modèle met l'accent sur la minimisation d'une fonction de coût ou la maximisation d'une fonction de vraisemblance. Ainsi, la performance du modèle est mesurée presque exclusivement sur les résultats par rapport à des métriques correctement choisies. Cette tendance a conduit à des algorithmes de plus en plus sophistiqués et complexes, au détriment de leur explicabilité et de leur auditabilité.

- **L'effet boîte noire** des algorithmes :

> ***« Le phénomène des boîtes noires appelle un effort de recherche fondamentale pour accroître leur transparence (…) Le défi à relever est donc celui de l'explicabilité ».***
>
> **Rapport d'information[46] de l'OPECST, (Office parlementaire d'évaluation des choix scientifiques et technologiques).**

- La sûreté des systèmes critiques à base d'IA nécessite de **démontrer que les algorithmes sont corrects**, c'est-à-dire qu'ils font ce qu'on attend d'eux. Plus précisément, l'algorithme reproduit directement la spécification étant donné les hypothèses sur ces données. Celui-ci devra être transparent, neutre, loyal, ou équitable, notions qui sont développées dans le DIP 13. Il devient donc indispensable de vérifier la conformité entre ses spécifications et son comportement, autrement dit mesurer l'écart entre ce qu'il est supposé faire et ce qu'il fait.
- Au-delà des systèmes critiques ou des environnements réglementés (DIP 7) qui imposent l'explicabilité, l'adoption commerciale de solutions sur des environnements non critiques (marketing, retargeting, chatbot par exemple) va également imposer des justifications de retour sur investissement et d'engagement des fournisseurs qui conduiront le marché à proposer des solutions et services auditables.
- La répartition des responsabilités sur le fonctionnement des systèmes à base d'IA est plus large que sur les systèmes dits classiques et imposera en cas de dysfonctionnement une capacité de mesure des rôles de chacun dans la solution : fournisseurs de données, concepteurs, fournisseurs de la solution, utilisateurs.

Pistes de résolution et recommandations

Il est nécessaire de proposer de nouvelles approches d'ingénierie de l'algorithme pour le développement des nouvelles générations d'algorithmes d'IA. En effet, il faudra prouver que, par construction même, ces algorithmes sont :

- **Transparents**, contribuant à leur explicabilité et à la traçabilité de leur raisonnement. En effet, la tendance étant que l'explicabilité d'un modèle est une métrique primordiale au même titre que la performance et la robustesse, un bon compromis entre explicabilité et précision est de plus en plus nécessaire. Cela pourrait être la clé pour rendre les algorithmes aussi transparents que possible pour les utilisateurs finaux.
- **Responsables**, garantissant leur conformité aux lois, normes, réglementations et/ou à certaines valeurs de notre société.
- **Contrôlables**, intégrant dans le processus de fonctionnement une traçabilité des actions, des restitutions, des feedbacks des utilisateurs et des systèmes ainsi qu'un processus d'alerte en cas de dérive et de maintenance systématique pour anticiper les divergences potentielles du système ou de son environnement de fonctionnement.

Ces algorithmes doivent constituer **une chaîne du traîtement de la donnée maitrisée** (DIP 16) de la collecte à l'exploitation. Enfin, sans collaboration multidisciplinaire, d'experts des métiers, de data-scientists,

46. « Pour une intelligence artificielle maitrisée, utile et démystifiée », Rapport d'information de l'OPECST (Office parlementaire d'évaluation des choix scientifiques et technologiques), 19/07/2017.

d'ingénieurs en IA et d'utilisateurs, il sera très difficile de s'assurer de la qualité de ces systèmes, voire même d'en définir les critères d'acceptabilité. Celle-ci s'avère nécessaire en raison de l'imbrication des expertises métiers et technologiques nécessaires tant à l'élaboration qu'au contrôle de ces solutions.

La définition, la publication et l'adoption par le marché de labels internationaux, européens ou nationaux, couvrant l'ensemble des périmètres de conformités éthiques ou réglementaires attendu des solutions à base d'algorithmes d'intelligence artificielle, permettra progressivement d'améliorer la qualité et la conformité de ces solutions.

DIP 16 : collecter, qualifier, exploiter et partager les données et les connaissances

Dans un monde de plus en plus collaboratif, la collecte, la production et le partage d'informations et de connaissances de qualité entre différents acteurs constituent un enjeu stratégique des professions de la finance et de l'assurance.

On peut citer par exemple les mouvements anormaux de marché sur les actifs financiers (actions, obligations, etc.), la détection d'événements inhabituels touchant la vie des entreprises (dirigeants, opérations financières inhabituelles), de sinistres dans l'assurance ou encore celle d'attitudes ou de messages clients comme signaux d'attrition.

Les technologies à base d'apprentissage ont besoin de données d'entraînement de qualité. On pense en particulier à des corpus annotés en français pour le traitement de la langue, mais plus généralement à des jeux de données labélisées dans le domaine bancaire et assurantiel, notamment pour les besoins des agents conversationnels (DIP2 et DIP3). Les besoins peuvent dépasser le secteur financier, aussi des données complémentaires venant d'autres secteurs, jouant par exemple un rôle particulier dans des estimations économiques, sont utiles. Les questions d'anonymisation doivent aussi être traitées.

L'impact de non-qualité des données, qu'elles soient collectées ou produites, peut alors engendrer un manque à gagner ou avoir d'importantes conséquences dans le pilotage d'une institution financière ou assurantielle.

Au-delà des jeux de données brutes annotées, on peut également signaler le besoin de disposer ou de développer des ontologies du domaine pour faciliter les divers traitements sémantiques.

La transformation de contenus, en particulier la traduction, demeure incontournable. Les institutions financières doivent être capables de communiquer en de multiples langues pour faire preuve de transparence et de proximité vis-à-vis de leurs clients particuliers et institutionnels. On pense à la communication urgente ou de crise, la réponse à des appels d'offres, la communication de résultats financiers et la traduction de rapports ou de documents sensibles de toutes natures.

La synthèse de contenus est réalisée à partir de données permettant de rédiger un texte avec le même niveau de qualité que s'il avait été écrit par un humain : rapports financiers, risque crédit, analyse de fonds financiers, documents de préparation et comptes rendus d'entretien, recommandations d'investissement personnalisées, etc.

Enfin, du fait de la multiplicité des supports et des terminologies et du manque de standards, il est difficile de partager de manière accessible toutes ces ressources informationnelles (données, informations, connaissances, modèles).

En réponse à ces mutations, l'IA intervient comme un complément aux méthodes habituelles de détection des anomalies.

Enjeux

Disposer de « bonnes » données est essentiel pour tirer une valeur ajoutée des traitements reposant sur des méthodes d'intelligence artificielle à base de données comme l'apprentissage.

En pratique, la gestion des données est exercée par des Data Scientists lorsque l'on applique des algorithmes d'apprentissage automatique, des Data Analysts ou Data Engineers lorsque l'on est en environnement Big Data et, bien entendu, la Data Gouvernance pour définir les processus et garantir leur mise en œuvre. Il devient donc nécessaire de fédérer et d'outiller les différents acteurs dans l'entreprise pour aborder sereinement cette maîtrise de la qualité des données.

Il est nécessaire de progresser sur la détermination **de la confiance envers les données d'entrée** (fake news), sur la qualité et l'exploitabilité des résultats, sur la mise en place de solutions verticales pour de grands domaines d'application et sur la réduction de l'effort de paramétrage des solutions de traitement du langage naturel mises en œuvre…

Préserver les connaissances et le savoir-faire est toujours un véritable enjeu pour la pérennité d'une entreprise. Par exemple, la valorisation d'une entreprise (ex. : sa cotation en bourse) repose de plus en plus sur des actifs immatériels, dont son patrimoine de connaissances. Étant souvent diversifiées, délocalisées et difficilement contrôlables, ces informations et connaissances stratégiques sont aujourd'hui traitées et gérées **par le biais d'outils de gestion de la connaissance (*Knowledge Management* - KM)**. Ce défi que les institutions financières ont parfois abordé dans le passé reste porteur de gains en productivité et en qualité dans toute la chaîne de valeur. Cette gestion des connaissances s'appuie souvent sur des contenus analysés pouvant ainsi être synthétisés dans des modèles, des représentations sémantiques (ontologie, graphe sémantique) ou graphiques, des règles métier, etc.

De plus, les problèmes sont le passage à l'échelle, la cohérence des bases, leur maintenance et évolution dans la durée – y compris la gestion de l'oubli, mais aussi leur intégration avec des systèmes apprenant à partir de données, ce qui reste un défi technologique non résolu à l'heure actuelle. De plus, le cycle de vie de la gestion des connaissances dans son sens de savoir-faire tacite – subjectif, informel, contextualisé, sous-jacentes à l'expérience pratique – est difficile à identifier, à capter, à traiter, à formaliser, à modéliser et à transmettre et donc à capitaliser dans un système informatique.

La difficulté n'est pas seulement dans la collecte des données, mais aussi dans **la validation des informations produites**, tant pour l'accomplissement d'une tâche que pour la prise de décision, et cela au moment adéquat. Par exemple, en matière de traduction de contenus, il reste des progrès à faire sur la qualité des traductions qui demandent la plupart du temps une relecture pour atteindre un niveau autorisant leur publication.

En parallèle, dans un cadre collaboratif multidisciplinaire, il est aussi nécessaire d'harmoniser ces ressources informationnelles et décisionnelles afin de permettre à des acteurs de profils variés de pouvoir interroger et de **partager des sources documentaires**,

à l'aide de leurs propres mots-clefs ou de leurs propres concepts.

Enfin, **de nombreuses réglementations et directives régissent la gouvernance des données financières**. Certaines sont d'ordre général, telle que l'entrée en vigueur du RGPD en mai 2018, d'autres plus spécialisées dans les domaines financiers, telles que BSBC 239 qui cible en particulier les données bancaires et MiFiD 2 qui amplifie le volume des données à sauvegarder ou encore FRTB qui amplifie la quantité des données de mesures risques.

L'IA est alors une réponse aux limites des outils classiques de gestion de la qualité des données. En effet, les méthodes conventionnelles consistent à définir des règles de contrôle par des humains et les programmer ensuite sous forme d'algorithmes. Ces règles sont statiques. Elles ne permettent pas l'apprentissage à l'exception de nouvelles conditions rajoutées manuellement. Dès lors, ces systèmes ne permettent de détecter que ce dont on a connaissance et ne trouvent que ce que l'on cherche. L'IA vise alors à rompre cette logique de protocoles de contrôle définis a priori par des règles de métiers et par l'expérience des dysfonctionnements connus.

Pistes de résolution et recommandations

Les solutions de gestion de la qualité des données (*Data Quality Management*) ne doivent pas être exclusivement basées sur la gestion informatique de la donnée, car elles doivent améliorer les processus décisionnels visés. Avant toute mesure de mise en œuvre, il est important de définir les objectifs et usages des données à traiter en fonction des enjeux selon le principe du « *fitness for use* » : dans certains cas, une tolérance à l'erreur est acceptable (comme des systèmes de recommandation d'achat en B2C) alors que dans d'autres (comme les systèmes critiques ayant un impact juridique, médical, financier…), l'ensemble du système d'information devra être traité avec la plus grande rigueur. Il s'agit donc d'une problématique liée au domaine métier et à l'usage :

- en amont, il faut que les producteurs de données deviennent des sources qualifiées, voire certifiées. On parle alors de cotation des sources ;
- en aval, il s'agit de fournir aux utilisateurs tous les éléments utiles afin qu'ils puissent en faire un usage pertinent et durable.

Ensuite, il est nécessaire de distinguer de manière automatique les données pertinentes du bruit, d'identifier la crédibilité et la légitimité du producteur de la donnée et de garantir son actualisation et sa mise à jour.

Si les humains n'éprouvent pas de réelles difficultés à résoudre les ambiguïtés de langage, il n'en est pas de même pour les systèmes numériques qui ont besoin de contextes sémantiquement explicites. Étant une représentation formelle des connaissances d'un domaine, les ontologies ou les graphes conceptuels permettent la définition d'un langage commun entre l'usager et un expert métier. Cependant, la représentation choisie a besoin d'être constamment adaptée pour notamment être réutilisée et répondre à de nouveaux usages tout en garantissant la préservation de la consistance lors de toute modification. Pour répondre aux enjeux décrits ci-dessus, **les outils mis en œuvre sont les technologies de traîtement de langage naturel, les technologies du web sémantique et de l'OBDM (*ontology-based data management*)**, la

traduction par approche statistique ou avec apprentissage (neural machine translation) et plus généralement les technologies de gestion des connaissances.

Pour la traduction automatique, il est important de favoriser la mise à disposition de grandes bases de contenus annotés et traduits, facteur essentiel pour la performance de ces systèmes. En particulier, **il faut soutenir les avancées dans les technologies de traîtement du langage naturel**, notamment en produisant des corpus partagés pour les métiers de la finance, de l'assurance et de l'asset management.

Enfin, mener des expériences mêlant approche sémantique pour la gestion des connaissances et apprentissage sur des contenus textuels, structurés ou non, peut permettre de réduire les ambiguïtés conceptuelles terminologiques au travers de mécanismes de raisonnement.

On s'attend à voir émerger des produits verticaux sur certains domaines métier : par exemple sur la performance des fonds financiers, la production automatique de contrats, la préparation d'entretien, l'analyse de performance d'un réseau, etc. Pour cela, **casser les silos** permettra de fluidifier les échanges par un partage efficace des données et des connaissances, ce qui favorisera l'agilité.

Pour **favoriser la collaboration et le partage entre acteurs de disciplines différentes**, la mise à jour des bases de données hétérogènes, des outils de capitalisation des connaissances et des algorithmes de corrélation et de fusion sémantique sont alors incontournables.

Enfin, **la représentation et la visualisation des données et des connaissances doivent être intelligibles pour un acteur non expert en IA**. Les résultats produits doivent ainsi faire l'objet de traitements spécifiques, appelés post-traitements, dont le but est d'expliquer (voir DIP 15), d'interpréter et de traduire ces résultats sous forme de synthèses, graphiques, rapports…

Focus
L'IA appliquée a l'analyse de la qualité des données financières mise en œuvre par Digitalent Consulting

Afin de parvenir à détecter des anomalies avant leur propagation dans le système d'information, Digitalent Consulting a développé et mis en place auprès de grands groupes du secteur bancaire trois axes de la qualité des données. Le premier par le biais de prédictions de la valeur attendue, un deuxième par la création de nouvelles règles par le *machine learning* et le dernier par la détection des déviations par rapport à l'ensemble des données, c.-à-d. les *outliers*.

- **Prédiction de la valeur attendue :** prendre un pas d'avance sur ce que devrait être la donnée. Autrement dit, prédire la valeur que devrait avoir la donnée compte tenu de facteurs externes la déterminant.
  Prenons l'exemple d'une variation du prix d'une transaction. Cette variation peut avoir plusieurs raisons : une forte volatilité sur le marché, un effet d'annonce spécifique à cet actif ou encore une erreur humaine.
  En modélisant la variation des cours boursiers par des modèles multi-facteurs, la détermination d'un intervalle tolérable d'évolution du prix de la transaction est possible.
  Une comparaison de la valeur prédite à la valeur observée permet de déclencher une alerte au-delà d'un certain seuil de tolérance qui peut être lui-même modélisé de façon dynamique.

- **Définition de nouvelles règles par l'IA :** la seconde approche est d'utiliser l'IA pour permettre de définir des règles non connues par les experts métiers. Dans ce cas, l'IA intervient comme un outil d'aide à la décision permettant d'établir de nouvelles règles.
  L'utilisation d'arbres de décision ou des méthodes de sous-espaces aléatoires et de *bagging* permet de mettre en exergue des règles qui ne sont pas encore mises en évidence.
  Dans le cas des caractéristiques d'un ordre de bourse, la typologie de l'ordre est conditionnée par d'autres métadonnées telles que le délai d'expiration ou les seuils de déclenchement.
  Les algorithmes d'arbre de décision nous ont permis de définir selon quelles conditions un champ prendrait une valeur en fonction de la valeur des autres champs. C'est là tout l'apport de l'IA qui permet d'apprendre à partir des données historiques, supposées propres, afin de mettre en avant des règles sur des champs peu explorés, soit par leur complexité ou par l'incapacité de définir des règles sur l'ensemble des champs caractérisant un ordre.
  Évidemment, la mesure est de rigueur dans l'IA. Il convient de pratiquer cette démarche en deux temps. Un premier en pur *machine learning* sur l'ensemble des variables afin de libérer tout le potentiel de l'IA. Et ensuite en calibrant, sélectionnant ou remplaçant les déterminants qui ont du sens pour le métier. D'où l'importance d'avoir une équipe Data Science qui maîtrise la technicité de l'IA et du métier des données sur lesquelles elle est appliquée.

- **Détection des outliers :** en parallèle à ces deux approches pour prédire la valeur attendue et définir de nouvelles règles par l'IA, d'autres méthodes non supervisées permettent de ressortir des observations inhabituelles.
  Des algorithmes basés sur l'analyse des distributions existent, tels que les algorithmes d'*Isolation Forest*[47], *SVM adapté à la détection d'anomalies*[48], le *Local Outlier Factor* (LOF) qui utilise lui-même l'algorithme *k-nearest neighbors* (KNN) ou encore certains algorithmes de minimisation de la covariance[49] ou d'estimation par noyau (*Kernel Density Estimation*, méthode de Parzen-Rosenblatt).
  Par la mise en pratique de toutes ces règles, nous avons conclu que seule une combinaison permettant le calcul d'un score d'anomalie permet de donner un résultat probant. En effet, chacune des méthodes porte ses limites et, par nature, n'est sensible qu'à certains signaux : déviation par rapport à la valeur prédite, écart par rapport à la distribution de la série, observation inhabituelle…
  La combinaison de tous les aspects peut confirmer une alerte ou du moins faire apparaitre de nouveaux comportements par l'analyse prédictive de la donnée.

Les limites d'une qualité de données intelligente et une transition vers l'IA qui se révèle complexe.

Il ne fait aucun doute que l'IA peut apporter une valeur ajoutée considérable à l'analyse de la qualité de données. Toutefois, une transformation profonde de l'entreprise est nécessaire pour s'approprier les outils, les maintenir et en interpréter les résultats.

- Par ailleurs, il convient de détecter une anomalie dès son arrivée dans le système d'information plutôt que de la constater a posteriori une fois stockée et probablement déjà utilisée dans les chaînes métiers. Cela implique l'implémentation de la data science dans toutes les étapes de vie de la donnée. Comme toute technologie, elle rencontre de nombreux obstacles. Certains sont d'ordre technique, comme l'accessibilité qui reste limitée à l'IA. D'autres existent pour des raisons plus structurelles, notamment là où les habitudes de travail prédominent sur l'innovation. La mise en place de l'IA pour l'analyse de la qualité de données implique une nouvelle conception, une nouvelle approche de mode de gestion de la donnée et un maintien à jour des modèles.

47. Fei Tony Liu, Kai Ming Ting, and Zhi-Hua Zhou. 2012. Isolation-Based Anomaly Detection. ACM Trans. Knowl. Discov. Data 6, 1, Article 3 (March 2012), 39 pages.
48. Estimating the support of a high-dimensional distribution Schölkopf, Bernhard, et al. Neural computation 13.7 (2001): 1443-1471.
49. Rousseeuw, P.J., Van Driessen, K. «A fast algorithm for the minimum covariance determinant estimator» Technometrics 41 (3), 212 (1999).

DIP 17 : intégrer l'IA dans le SI

L'intégration de l'intelligence artificielle de façon industrielle dans un système d'information n'est pas chose facile et représente une difficulté majeure pour une entreprise qui souhaite passer du stade de POC[50] ou MVP[51] à une organisation en pleine transformation numérique.

Cette transformation requiert la mise en place d'un **Système d'Information (SI) Cognitif**, c'est-à-dire un SI capable d'intégrer de façon centralisée à la fois la donnée, structurée ou non, et la connaissance métier pour proposer des services intelligents exploitables par l'ensemble des collaborateurs de l'entreprise, au travers de moteurs de recherche sémantique et de recommandation apprenant de «*next best action*», d'outils intelligents d'analyse de la donnée, d'assistants virtuels, etc.

En effet, dans le domaine de la finance et des assurances, le volume des données tant structurées que non structurées est gigantesque. Dès lors, la capacité de traitement est un facteur clé dans la réactivité et l'adaptation aux changements. Or, les investissements nécessaires ne sont pas à la portée de la majorité des acteurs, induisant une dépendance de l'industrie financière aux gros pourvoyeurs de plateformes et infrastructures dont beaucoup sont étrangers.Ce SI cognitif devra aussi pouvoir dépasser les frontières de l'entreprise et se connecter à des fournisseurs externes de données, d'API cognitives ou d'algorithmes. Ces fournisseurs pourront être des éditeurs, prestataires, clients, fournisseurs, partenaires, voire des concurrents. Ce SI se place au centre d'un écosystème riche, se transformant ainsi en véritable cerveau évolutif de l'entreprise.La force de ce dernier sera donc d'industrialiser l'ensemble de la connaissance de l'organisation et de s'interfacer à des collaborateurs internes ou partenaires externes pour continuer à apprendre et fournir des services de plus en plus riches, contextualisés, personnalisés et performants.

Cependant, il est important ne pas négliger la dimension d'interprétabilité. En effet, l'absence d'explicabilité a des conséquences fâcheuses. La première est la composabilité permettant d'ajuster les éléments pour le bon fonctionnement d'un système. Si on ne sait pas ce qui influe sur le résultat, on ne sait pas quelles données sont utiles ou pas. La seconde est l'adaptabilité, c'est-à-dire la capacité à appliquer avec souplesse les connaissances acquises dans un contexte à un autre. Par exemple, un réseau entraîné à analyser le langage humain depuis Wikipedia peut complètement échouer à s'adapter à un autre contexte, comme Twitter.

Enjeux

Les points critiques à la mise en place d'un SI cognitif sont nombreux, mais nous relèverons les suivants :

- La collaboration est parfois difficile entre les métiers et la DSI[52] : l'intelligence artificielle est le terme à la mode de la dé-

50. POC est l'acronyme pour « Proof Of Concept » (Preuve de concept).
51. Le terme MVP vient de l'anglais « Minimum Viable Product », soit Produit Minimum Viable en français. Ce concept repose sur l'objectif de sortir d'abord un produit avec uniquement la fonction la plus attendue (la « Killer Feature » ou la fonction qui tue) par un public cible, et de proposer le plus rapidement le MVP afin de le confronter au marché. Une fois confronté au marché, on peut l'améliorer et l'enrichir via les méthodes de développement agile.
52. DSI : Direction des systèmes d'information.

cennie et les promesses des éditeurs et des prestataires de service ont convaincu les métiers à avancer souvent seuls dans leurs expérimentations. Les axes stratégiques business pour l'IA ne sont souvent pas clairement définis, la gouvernance des projets d'IA n'est pas clairement établie et des méthodologies de priorisation des projets restent à définir.

- Les flux de données, la gestion des connaissances, les technologies et les modèles sont généralement silotés et devenus souvent incompatibles entre métiers. Le shadow IT cognitif a fait son apparition, au détriment d'approches collégiales permettant d'aboutir à des architectures centralisées et optimales. En particulier, les données non structurées distribuées un peu partout dans l'organisation représentent environ 90 % des données de l'entreprise et restent inexploitées.
- Une urbanisation et un delivery spécifiques : des systèmes basés sur des technologies d'apprentissage machine ne peuvent pas être industrialisés ou mis en production comme des systèmes classiques ; ceux-ci doivent être supervisés en continu pour s'assurer que les réponses qu'ils apportent restent optimales. Par ailleurs, de nombreux éditeurs proposent des solutions dans le cloud qui deviendront incontournables au moins pour l'entraînement des algorithmes par de la GPU rare et chère ; on parle alors de SI cognitif à la demande.

Piste de résolution et recommandations

Pour répondre aux difficultés précédemment soulevées, les recommandations suivantes peuvent être mises en place :

- Pour ce qui est de la collaboration entre les métiers et la DSI, il est nécessaire que la DSI se positionne dans une approche partenariale forte avec les métiers qu'elle doit accompagner de façon très pédagogique, l'objectif étant de démontrer qu'un SI cognitif centralisé est incontournable. Nous pourrons par exemple noter comme services offerts par la DSI aux métiers : des formations d'acculturation à la Data Science, à l'IA, aux solutions du marché, des benchmarks, des ateliers de codesign, des rencontres avec d'autres entreprises d'autres secteurs, etc. ;
- En suivant l'exemple du groupe Schneider Electric, il est nécessaire pour les grands groupes ou industries de créer un Comité Numérique au sein de leur Conseil d'Administration.
- Pour ce qui est des données et connaissances, il est nécessaire pour l'entreprise de continuer à briser les silos afin de fournir des données uniques, riches et pertinentes aux métiers. Au-delà de la donnée structurée, il sera nécessaire de se focaliser sur les données non-structurées (textes, documents, images, etc.) par la création de bases graphs centralisées exploitables par des moteurs de recherche sémantique ou des assistants virtuels intelligents.
- Finalement, pour ce qui est de l'urbanisation et du *delivery* spécifiques, la DSI pourra identifier une urbanisation multicouche : couche applicative interne (Outlook, CRM, etc.), couche IA *on-premise* avec orchestration et couche IA externe (avec anonymisation éventuelle) se connectant aux solutions cloud du marché ou autres partenaires via API. Ce type de modèle pourra garantir la sécurité des données et répondre aux exigences réglementaires du marché.
- Pour la maintenance des solutions d'IA, le SI pourra inclure des systèmes de supervision garants de la robustesse des algorithmes apprenants.

DIP 18 : prévenir les cyber-risques en couplant IA et cyber-sécurité

Si l'impact de l'intelligence artificielle (IA) sur l'industrie bancaire (banques de détails, de financement et d'investissement) est aujourd'hui autant perçu comme une véritable opportunité que comme une source d'inquiétude (DIP 12), les liens qu'entretiennent IA et cybersécurité sont tout aussi ambivalents. Jetant un nouveau regard sur la traditionnelle dialectique de l'armure et de l'épée, l'IA semble offrir tout à la fois de nouvelles stratégies de cyber-protection que représenter de nouvelles menaces.

Les murs tombent…

La sécurisation des systèmes informatiques embarquant des IA doit s'adapter à cette évolution. En effet, contrairement aux approches traditionnelles qui défendent les systèmes informatiques face à des attaques ciblées et connues, un logiciel à base d'IA peut apprendre en continu. Cependant, si les progrès de l'IA ouvrent des pistes de défense contre les logiciels malveillants, c'est aussi de l'IA que proviendront les prochaînes menaces. Dans le cadre d'un schéma de certification strict comme les *Critères Communs*[53], la mise en œuvre d'une telle défense en profondeur repose sur des hypothèses fortes concernant l'environnement opérationnel de la cible qui se doit d'être «**de confiance**». Cette disjonction du «dedans» et du «dehors» et la gestion indépendante de ces deux périmètres convenaient pour des systèmes peu connectés, présentant des API minimalistes et préservés de potentielles mises à jour après la conception ou le déploiement. Or, pour de nombreux systèmes, la définition même d'une telle frontière s'avère aujourd'hui complexe et appauvrit du même geste l'analyse de sécurité.

Il n'est donc plus possible de garantir la sécurité par la limitation des interactions possibles avec l'utilisateur (toujours vu comme un attaquant potentiel). C'est en effet de cette utilisation personnalisée et adaptée aux besoins de chacun que les nouveaux objets connectés et les nouveaux usages tirent leur valeur. Il faut ainsi considérer que l'attaquant est inextricablement lié à l'environnement proche du système et qu'il dispose de multiples degrés de liberté pour éprouver les défenses protégeant les secrets et informations sensibles que le système renferme.

Enjeux

Apprendre l'environnement : le normal et le pathologique.

Depuis quelques années, l'IA, et plus particulièrement les techniques d'apprentissage, est utilisée par des entreprises pour identifier les vulnérabilités de leur système informatique et détecter ou anticiper des cyberattaques. La détection d'incidents ou d'événements anormaux devient donc une fonction requise. De multiples sondes ou capteurs sont aujourd'hui déployé(e)s tant sur ces systèmes embarqués (comme les puces) que sur les systèmes IT avec

53. Ensemble de normes (ISO 15408) internationalement reconnu dont l'objectif est d'évaluer de façon impartiale la sécurité des systèmes et des logiciels informatiques. Également dénommés Common Criteria, ce référentiel est né d'un partenariat entre le Canada, les États-Unis et l'Europe (Wikipédia).

comme première intention d'acquérir des données de *reporting* fonctionnel ou encore en vue d'adapter le fonctionnement du système à l'environnement (nombre de transactions, etc.). Cependant, ils peuvent aussi agir en complément de sondes dédiées à la sécurité en fournissant dans certains cas des indices de compromission (conditions d'utilisation anormales, activités suspectes). L'agrégation et la valorisation de ces multiples signaux de natures hétérogènes représentent un enjeu technologique majeur.

Cependant, si l'IA fournit des outils à la fois pour la défense, une attaque basée sur de l'IA peut adapter son comportement et prendre des décisions en fonction de la cible et de la réponse de cette dernière à l'attaque. Par ailleurs, une IA est capable de paralléliser plusieurs scénarios d'attaque et sur différents fronts afin de compromettre le système ciblé. Citons par exemple l'utilisation des faiblesses des approches de *machine learning* (les données) par les cybersattaquants qui peuvent ainsi développer des modèles *d'adversarial machine learning* pour tromper les systèmes de protection reposant sur du *machine learning* dont l'objectif est de détecter les menaces.

Pistes de résolution et recommandations

Les méthodes d'apprentissage automatique ainsi que les techniques de fusion sémantique permettant la corrélation de données et de connaissances apparaissent ici comme le candidat de choix permettant de rendre intelligible des événements de sécurité complexes, dont l'interprétation n'est permise que par la « digestion » de grandes quantités de données émanant de ces multiples capteurs. Cette analyse permet à la fois d'intégrer des indices de compromission faibles jusqu'ici ignorés et de créer une cohérence dans la multitude des signaux analysés permettant d'améliorer l'efficacité de détection. Outre une confiance accrue dans la détection (réduction des faux positifs/négatifs), l'IA permet aussi d'enrichir le diagnostic – et non plus seulement de lever des alarmes – par une analyse prédictive afin d'offrir de plus larges marges de manœuvre quant à l'action à entreprendre face à l'événement détecté.

Dans le contexte embarqué, comme pour celui des puces, l'accélération matérielle d'opérations de classification par rapport à un modèle d'apprentissage permet une détection en temps réel d'événements anormaux telle une attaque cyberphysique. Cette détection d'attaque à faible latence peut s'avérer cruciale lorsque l'intégrité d'informations boursières est mise à mal. La détection et la réaction doivent être effectives en quelques nanosecondes, ce qui est l'apanage des accélérateurs matériels. L'intelligence artificielle embarquée se doit d'être tout à la fois légère et de confiance.

En complément de l'établissement de nécessaires capacités de résilience et de l'analyse de flux renforcée par les méthodes d'apprentissage automatique au niveau des couches réseaux et des couches supérieures, il devient nécessaire de développer des méthodes de détection en temps réel au niveau des couches les plus profondes des systèmes d'information (couches matérielles). L'objectif est alors de circonscrire la menace en son cœur avant que les effets néfastes ne se fassent sentir et de prendre l'avantage sur l'attaquant en adaptant dynamiquement

les politiques de sécurité (défensive, analytique, déception, offensive…) en fonction de l'anatomie de l'attaque.

Dans le contexte IT, même si l'usage de l'IA au service de la cybersécurité est aujourd'hui centré sur l'identification des vulnérabilités d'un système et la détection de comportement anormal pour détecter des attaques, cela reste encore une démarche réactive. Il est nécessaire d'aller vers une **cybersécurité proactive** offrant des mécanismes automatiques d'anticipation, voire vers une **cybersécurité prescriptive** permettant l'automatisation de confinement d'une attaque ou des solutions de résilience prenant en compte l'impact de l'attaque et le coup de la remise en l'état.

Enfin, il convient de travailler sur la cybersécurité des composants/systèmes qui embarquent de l'IA et sur d'éventuelles cyberattaques pouvant elles-mêmes être basées sur des techniques d'IA. Cela pose en particulier pour les IA à base de *machine learning* les questions de la qualité de la base d'apprentissage (DIP 16) et de la robustesse vis-à-vis d'approches telles l'*adversarial machine learning*.

2.5 TRANSPOSITION DES BONNES PRATIQUES DES AUTRES SECTEURS AU MONDE DE LA FINANCE

Les avancées de ces dernières années en intelligence artificielle (IA), permettant de prédire, d'anticiper et d'optimiser comportements et processus métiers et dotant la machine de capacités d'apprentissage, de raisonnement et de décision, ont permis la mise en œuvre de systèmes aux résultats prometteurs dans des domaines comme la santé, la mobilité, la ville, la sécurité, l'industrie et l'entreprise.

De nombreuses applications sont aujourd'hui opérationnelles. Citons le ciblage publicitaire, la détection de comportements suspects dans des lieux publics grâce à la vidéosurveillance, la lecture automatique de comptes rendus médicaux complétée par la recommandation de prescription ou encore le support à la résolution de problèmes complexes comme la gestion du trafic urbain tenant compte d'incidents et de contraintes écologiques…

Ainsi, dans le domaine de la santé, l'IA permet de libérer médecins et personnels médicaux de tâches sans valeur ajoutée pour leur permettre de consacrer plus de temps aux patients. Les radiologues utilisent déjà depuis des années des « CAD » (systèmes d'aide au diagnostic) pour aider à détecter ou caractériser des lésions.

Le domaine de la mobilité connaît une profonde mutation grâce à l'utilisation massive de l'IA. Par exemple, que ce soit dans les transports terrestres, aériens ou maritimes, l'amélioration de la qualité de l'information fournie à l'utilisateur (voyageur, exploitant, autorité) permet d'améliorer la qualité des opérations : qu'il s'agisse de la régulation du trafic, de la logistique pour l'opérateur de contrôle ou de supervision, de la billettique, de l'information des voyageurs ou encore de la sécurité pour les usagers. CityMapper (à Londres, Berlin, Tokyo, Paris, New York) ou Moovit (dans 100 villes à travers le monde) sont des exemples d'applications au service de la mobilité qui permettent le calcul en temps réel du meilleur itinéraire, selon différents modes de transport.

La ville devient aussi le terrain de jeu de l'IA en proposant des services plus en plus individualisés. Les administrations peuvent anticiper les besoins en services administratifs des ménages pour proposer des activités adaptées à chacun. Par exemple, au nord de Londres, Amélia est un agent conversationnel qui accompagne les habitants dans leurs démarches auprès des services municipaux. En Norvège, les habitants de Kongsvinger peuvent utiliser un chatbot pour connaître le nombre de places en crèche ou les spécialités des hôpitaux de la ville.

En étudiant ainsi différents retours d'expérience de mise en œuvre de technologies à base d'IA dans la santé, la mobilité, la ville intelligente, l'industrie et l'entreprise, l'objectif de ce chapitre est de mettre en exergue des innovations et de bonnes pratiques transposables aux métiers de la banque. De plus, une ouverture vers d'autres domaines facilitera la levée de certains verrous décrits dans les sections précédentes et d'accélérer le déploiement le l'IA dans le monde de la finance.

Santé : l'hospitalisation à domicile

La HAD (Hospitalisation À Domicile) est une alternative à l'hospitalisation classique qui existe depuis une cinquantaine d'années, mais qui reste mal connue. Un département sur cinq ne dispose d'aucune structure d'accueil de ce type. Pourtant, cette solution permettant le maintien à domicile est plus économique qu'un séjour à l'hôpital.

Il s'agit d'assurer des soins chez le patient. Les actes médicaux sont équivalents à ceux réalisés à l'hôpital et, à l'exception de la psychiatrie, toutes les spécialités peuvent être concernées, même les plus lourdes comme la cancérologie ou les soins palliatifs. Les soins nécessités par les grossesses à risques peuvent également avoir lieu dans le cadre de la HAD. Les soins sont donc conséquents, ce qui différencie la HAD des simples soins à domicile dispensés par les infirmières libérales. En 2007, on comptait 200 structures d'hospitalisation à domicile en France, ce qui représente l'équivalent de 7 000 lits ou encore de 70 000 patients. Ces structures sont publiques ou privées, mais répondent toutes à des normes très strictes.

Retour d'expérience

Un objectif seuil de taux de recours à atteindre pour 2018 est fixé à 30-35 patients pris en charge par jour pour 100 000 habitants (ce seuil était de 18,5 patients par jour en 2014), ce qui correspond au doublement de l'activité globale constatée en 2011, sachant que les efforts à produire sont inégaux selon les régions. Ces objectifs impliquent une évolution de l'ensemble de l'offre sanitaire. Aujourd'hui, le ratio est de 18 patients pour 100 000 habitants, insuffisant selon la présidente de la Fédération Nationale des Établissements d'Hospitalisation à Domicile (FNEHAD).

- Côté médical : l'analyse de cette situation a conduit les professionnels à réfléchir sur les points suivants :
  - prévoir une check-list des informations données lors des transmissions entre équipes ;
  - revoir les modalités de formation sur les nouveaux matériels et notamment sur la vérification des éléments nécessaires pour leur utilisation sécurisée ;
  - revoir les modalités du double contrôle ;
  - diffuser ce retour d'expérience à l'ensemble de la communauté hospitalière pour sensibiliser chaque acteur à cette problématique ;
  - inciter les professionnels à changer de matériel lorsque leur maitrise n'est pas optimale.
- Côté patient : être dans son cadre personnel aide à guérir et favorise un rétablissement rapide.

Perspectives et futures innovations

La mise en place de telles fonctions permettrait d'apporter plus de services et de confort aux personnes âgées et isolées tout en revitalisant certaines zones et en créant des emplois.

Transposition au monde de la finance

- L'individualisation de l'offre de produit ou service.

Mobilité : l'optimisation du trafic

Optimiser la coordination des feux de signalisation est un problème complexe en milieu urbain : le réseau routier est dense et maillé, avec de faibles inter-distances entre les carrefours, surtout lorsque l'on cherche à concilier sécurité routière, libre écoulement du trafic et réduction des pollutions sonores et atmosphériques. Pour cela, de nombreuses villes ont développé des solutions d'IA par apprentissage sur des données vidéo afin d'analyser le trafic. À partir de cette connaissance en temps réel, des algorithmes d'optimisation combinatoire multicritère permettent d'optimiser le contrôle les feux.

Enfin, avec une meilleure gestion de la circulation et de la connaissance des places de stationnement, il devient possible de décongestionner les « zones d'affluence » vers lesquelles convergent les automobilistes à la recherche d'un emplacement de parking.

Retour d'expérience

De nombreux systèmes existent. Citons le système GERFAUT (Gestion et Exploitation des Régulations des Feux AUTomatisés) déployé en Seine–Saint-Denis, qui prend en charge la régulation de plus de 600 carrefours à feux, limitant les nuisances des congestions routières. La priorité est donnée au développement de l'intermodalité – tous les transports collectifs (tramways et bus) sont prioritaires aux traversées de carrefours – et à la gestion efficace des pics de trafic autour des sites du Salon du Bourget et du Stade de France. Des panneaux d'information dynamique sont déployés au profit des usagers. De même, à Bordeaux, le système Gertrude détermine de manière dynamique les différentes phases d'évolution des feux.

Avec un réseau de capteurs de trafic, de vidéotrafic et de stations météorologiques, il devient donc possible d'assurer une connaissance permanente du contexte. En effet, les techniques d'analyse vidéo permettent de calculer en temps réel des indicateurs sur le trafic comme le volume, la vitesse d'un véhicule, la densité, le temps inter-véhiculaire, la vitesse du flux, mais aussi de détecter des événements anormaux qui ont un impact sur la fluidité (et la sécurité) comme les véhicules à l'arrêt, les conducteurs à contresens, les accidents... La logique floue peut être utilisée pour déterminer le temps d'un feu en fonction du nombre de véhicules présents sur les voies : à un nombre de véhicules correspond un intervalle définissant une durée de feu. L'apprentissage permet de définir des modèles de prédiction et d'estimer l'évolution d'une situation observée. Les algorithmes d'optimisation combinatoires basés sur les observations comme les algorithmes évolutionnaires sont adaptés pour monitorer en temps réel les paramètres des plans de feux. On peut penser aussi à des approches de type optimisation black-box comme CMAES. Enfin, le couplage avec des simulations de trafic (ex. SUMO – Simulation of Urban Mobility) offre la possibilité de faire des analyses de type « *what if* ».

Perspectives et futures innovations

L'innovation est incrémentale et les premières études couplant IA et recherche opérationnelle datent des années 80. Au-

jourd'hui, l'innovation vient du couplage avec l'apprentissage pour rendre dynamique le calcul des plans de feux qui étaient jusqu'à peu statiques.

Cependant, avec l'arrivée des voitures connectées, on peut imaginer des innovations de rupture, permettant des plans de feux adaptatifs. Avec le co-voiturage et le développement de nouveaux modes de circulations (tramway, vélo, trottinette, voitures autonomes), la route intègrera de nouvelles formes de mobilité et de nouveaux modes de transport. Elle devient multimodale. Face à cette évolution, l'AI devra rendre la route plus fluide. Elle doit aussi être accessible à tous et à toutes les formes de mobilité.

De plus, dans ce nouveau paysage routier et urbain, les équipements de la route ont un rôle évident à jouer pour garantir la sécurité, la fluidité et l'accessibilité des déplacements de tous les usagers, sur la route et en agglomération. De façon plus générale, avec l'application de l'IA à la vidéosurveillance de la ville, il devient possible d'analyser et exploiter en temps réel ces flux de données pour alerter les forces de l'ordre connectées et faire ainsi de la « Smart City » une « Safe City ».

Transposition au monde de la finance

- Optimisation et aide à la décision multicritère temps réel, prenant en compte le contexte.

Smart City : le e-gouvernement

L'UNESCO a défini l'e-gouvernement comme *«l'utilisation par le secteur public des TIC dans le but d'améliorer l'information et la prestation de services, en encourageant la participation des citoyens dans le processus de prise de décision et amener le gouvernement à rendre des comptes, à être plus transparent et plus efficace»*. L'usage de chatbots pour faciliter les échanges entre les services de l'État et les citoyens se concrétise, contribuant à l'amélioration de la relation avec le citoyen en répondant aux demandes d'accès à l'information ou en élaborant des politiques. De plus, l'usage d'outils d'aide individualisée doit permettre une dématérialisation des procédures administratives avec pour but la simplification des échanges, la transparence et la réduction des litiges entre l'administration et les citoyens, quel que soit le canal utilisé (portail web, courrier, mail, guichet unique, e-formulaires, services mobiles…). La dématérialisation de la commande publique permet de concilier le développement de l'administration électronique et la lutte contre la corruption. Pour cela, des outils d'aide à la décision multicritère peuvent comparer plusieurs alternatives (offres d'un marché public, choix d'aménagement du territoire, tracés routiers, etc.) tout en prenant en compte les incertitudes et la maîtrise des risques en exploitant la connaissance et le retour d'expérience.

Retour d'expérience

Au Danemark, 80 % des transactions entre l'administration et le citoyen sont depuis 2015 effectuées en ligne. De nombreux exemples de chatbots existent. Marseille a expérimenté «Marius VDM» pour répondre instantanément aux questions récurrentes de ses habitants, complétant les services citoyens en répondant à des demandes simples et administratives comme les horaires d'ouverture, la localisation des bureaux de vote, les documents à apporter, etc. L'agglomération de Lyon a mis aussi en place un service d'assistance numérique afin d'améliorer l'accès aux services existants et d'intégrer les acteurs privés d'intérêt général. Tommy est le chatbot européen au service du citoyen, chargé de collecter les idées et doléances des citoyens. Enfin, certains organismes publics utilisent déjà des processus outillés de Réponse à Appel d'Offres.

Perspectives et futures innovations

L'interaction Homme-Système devra être de plus en plus individualisée et s'adapter au profil de l'usager afin de réduire la fracture numérique (ex. IHM adaptée aux seniors). Le domaine de l'e-démocratie et de l'e-gouvernance est un champ d'application de l'IA, car il couvre la prise de décision démocratique, notamment les canaux électroniques de consultation publique à propos des décisions et des actions du gouvernement. L'IA pourrait ainsi être utilisée pour analyser et compiler les propositions citoyennes.

Transposition au monde de la finance

- La fidélisation, la transparence et la proximité des clients ;
- La participation des clients à la gouvernance de leur banque/assurance ;
- Chatbots et coachs virtuels.

De la maintenance préventive à la maintenance prédictive et proactive

Quel que soit le domaine d'activité, la mise en place d'une stratégie de maintenance prédictive et proactive basée sur le pronostic de risques de défaillance dans un avenir proche, la planification d'interventions avant l'arrivée de la panne et l'optimisation de la gestion des stocks de pièces de rechange contribuent à réduire les coûts de maintenance en ne mobilisant pas inutilement des équipements.

La maintenance prédictive nécessite quatre étapes essentielles :

- Collecter les données à l'aide de capteurs et les centraliser pour pouvoir les analyser ;
- Modéliser des schémas de panne, en mettant au point des algorithmes qui reconnaissent les signes avant-coureurs ou les anomalies en se basant à la fois sur un historique des pannes et les connaissances métier, puis qui calculent une estimation du temps de vie résiduel (RUL – *Remaining Useful Life*) ;
- Concevoir des algorithmes qui apprennent à reconnaître les nouveaux événements et défaillances lorsqu'ils surviennent. Cette étape permet de ne pas se limiter aux seuls schémas de défaillances connus, mais d'en ajouter de nouveaux aux systèmes de diagnostic, au fur et à mesure de la collecte d'informations ;
- Optimiser la production et la gestion des stocks de pièces de rechange, mais aussi la planification des services de maintenance.

Retour d'expérience

La maintenance prédictive est une « *killer application* » de l'IA. Cependant, pour l'optimisation, la production et la gestion des stocks de pièces de rechange, la planification des services de maintenance, il s'agit surtout d'innovation incrémentale. Pour l'aide au diagnostic et l'estimation du RUL, il s'agit d'une innovation de rupture, car on observe un changement de paradigme passant de la maintenance préventive (planifiée à intervalle régulier) à la maintenance prédictive. Enfin, peu d'approches de maintenance prédictive prennent aujourd'hui en compte la cybersécurité qui devient incontournable lorsqu'il s'agit de maintenir un système critique. De plus, la disponibilité et la propriété des données sont aussi des points de blocage, car l'opérateur de maintenance n'a pas toujours accès à l'ensemble des historiques.

Citons trois exemples de déploiement de solutions de maintenance à base d'IA :

- Air France – KLM : en exploitant les historiques de vol des A-380 et des atterrissages à Paris, il est aujourd'hui possible de détecter une panne possible en moins d'une heure et d'établir son diagnostic en cinq minutes au lieu de six heures ;
- Avec un moteur d'analyse prédictive des données de ses rames connectées du Transilien, la SNCF cherche non seulement à télé-diagnostiquer les pannes, mais aussi les prédire dans les 30 minutes ;
- La maintenance prédictive des ascenseurs ThyssenKrupp repose sur une analyse en temps réel des données,

comme celles du fonctionnement des portes et de la température du moteur, qui sont injectées dans des modèles prédictifs dynamiques.

Hybridation des IA : une nouvelle perspective

Un des processus clés de la maintenance proactive est le pronostic de dégradation/défaillance des composants et des performances du système/composant : soit directement calculé par apprentissage sur un historique d'usage, soit par modélisation de la causalité dysfonctionnelle. Ainsi, l'hybridation de techniques d'IA dirigée par les données avec des techniques d'IA basée modèle est un vrai défi qui enrichit l'apprentissage avec des règles métier. De plus, les techniques TAL (Traitement automatique du langage) permettraient d'automatiser la découverte de nouvelles connaissances par analyse automatique des rapports de maintenance.

L'usage de RA/RV (Réalité Augmentée/Réalité Virtuelle) permet aujourd'hui de ne pas envoyer systématiquement des opérateurs de maintenance seniors, mais de pratiquer la maintenance en mode déporté.

Passer au zéro arrêt imprévu : une priorité pour l'industrie ou pour les systèmes critiques

Les temps d'arrêt imprévus des machines coûtent cher à l'industrie ou aux opérateurs de systèmes critiques (transport, énergie…). Ainsi, la sûreté de fonctionnement et la cybersécurité industrielle doivent se côtoyer pour identifier et analyser les risques de pannes, puis proposer une aide à la résolution du problème par un ensemble de mesures appropriées, soit en faisant appel à l'homme, soit en réalisant l'action par elles-mêmes.

De plus, pour optimiser la production, la gestion de flotte et/ou les opérations de maintenance, il est nécessaire de développer des technologies permettant des approches prédictives et proactives.

Transposition au monde de la finance

- La couverture de sinistre en temps réel calculé par l'IA prédictive avec une répercussion sur les compagnies de réassurance ;
- Le pricing en temps réel ;
- Gestion des risques (*credit scoring*).

L'aide au recrutement

Selon Harvard Business Review, les évaluations automatiques de CV seraient 25 % plus fiables que les analyses classiques RH, l'IA permettant d'étudier plus de candidatures. Ainsi, le processus RH le plus mature en termes d'utilisation de l'intelligence artificielle est le recrutement, tant dans le ciblage de candidats (traitement d'une masse d'informations structurées [bases de CV, data LinkedIn] ou non structurées [réseaux sociaux personnels et professionnels]) et l'optimisation des offres et descriptions de postes (analyse des taux de réponses des candidats) que dans l'industrialisation de la présélection (analyse d'entretien vidéo).

Au-delà de l'optimisation et/ou de la massification des traitements, de nouveaux acteurs apparaissent, intégrant les aspects de localisation et de réactivité liés au déploiement d'offres de services ponctuelles et urgentes, apportant une souplesse permettant de répondre à la fois au besoin de réactivité des entreprises, mais également à l'évolution du marché de l'emploi et l'augmentation du temps partiel multi-employeur.

Retour d'expérience

À ce jour, il s'agit principalement d'évolution incrémentale permettant de traiter plus de CV et de garantir l'homogénéité des critères de sélection de premier niveau.

Certains sites de recrutement comme Inzejob ou les réseaux sociaux professionnels comme LinkedIn ou Viadeo corrèlent des profils avec des offres d'emploi qui ne correspondent pas uniquement au métier, mais aussi à des compétences transférables.

Des applications ont déjà été déployées. Citons Proxem, Remo Platform et Yatedo Talent qui proposent déjà des solutions pour optimiser le traitement des profils, le sourcing des candidats et la mobilité interne.

Enfin, dans certains cas, une disruption est apportée sur des applications de niche, par exemple des applications smartphone traitant de besoins en ressources urgentes et très rapides associées à de la géolocalisation (restauration, manutention…)

Perspectives et futures innovations

Les RH ne sont pas un métier de la donnée, bien plus un métier de l'humain : une erreur de la machine peut impacter fortement la vie d'un candidat ou d'un collaborateur, il existe donc là un fort risque éthique. La transparence des algorithmes intégrant des principes de loyauté, de neutralité, de simplicité et d'explicabilité est essentielle, les RH ne pouvant appuyer leurs décisions sur des algorithmes dont ils ne peuvent expliciter les résultats.

Transposition au monde de la finance

- Matching cognitif et empathique entre le client et le conseiller financier.
- Matching entre employés et les membres des équipes.

2.6 POINTS SAILLANTS JURIDIQUES

Propriété des données et des algorithmes

Le Conseil d'État préconisait l'adoption d'un système fondé sur l'auto-détermination informationnelle (issu de la jurisprudence constitutionnelle allemande), c'est-à-dire un droit attaché à la personne tendant à garantir *«en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel»* et non un système fondé sur le droit de propriété des personnes sur leurs données personnelles.

Cette thèse a prospéré puisque la loi pour une République numérique a modifié l'article 1 de la loi de 1978 qui dispose désormais :

«Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi.»

L'article 57 de cette loi dispose par exemple de l'existence d'un droit d'accès des personnes aux données les concernant. Il existe également un droit à l'oubli numérique (CJUE, *Google Spain*, 13 mai 2014 précitée). Au contraire, le droit de propriété des personnes sur leurs données personnelles n'a pas été reconnu.

NB : il existe parfois de facto une obligation de révéler ses données, certaines données de santé devant par exemple nécessairement être dévoilées afin d'obtenir une assurance.

Propriété des bases de données

La directive n° 96/9 du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données vise à accorder à ces dernières une protection sur le fondement, d'une part, du droit d'auteur quand cette base est originale (art. 3 et suivants de la directive précitée) et, d'autre part, d'un droit sui generis quand la constitution de cette base résulte d'un effort substantiel d'investissement (art. 7 et suivants de la directive précitée).

Ainsi, cette protection est fondée sur la *« notion d'investissement plus proche de la logique anglo-saxonne du copyright que de celle, française, de protection par l'originalité de la création »*. À ce titre, peuvent être interdites l'extraction et la réutilisation massive de données issues d'une base de données protégée (art. 7 précité). Cette directive est transposée aux articles L. 341-1 et suivants du Code de la Propriété Intellectuelle.

Certains critiquent le développement de cette appropriation, car il représenterait un frein à la libre concurrence et au *big data*. En effet, *« certaines activités étant principalement assises sur l'exploitation de données, il est possible d'empêcher un concurrent potentiel d'entrer sur le marché en le privant de données indispensables à son développement[54] »*. Ainsi, ce système pourrait représenter un frein au développement de l'intelligence artificielle qui se nourrit de données. Cependant, le droit de la concurrence et notamment la théorie des facilités essentielles sont de nature à limiter cette impossibilité d'accès au marché[55].

54. La propriété intellectuelle et la transformation numérique de l'économie, INPI, (2016)
55. Voir par exemple F. POLLAUD-DULIAN, Abus de positions dominantes. Droit exclusif. Refus d'accorder une licence. Bases de données. Infrastructures ou installations essentielles. RTDCom 2004, p. 491.

Propriété des algorithmes

Propriété littéraire et artistique

En tant que principe mathématique, l'algorithme relève du domaine des idées qui sont de libre parcours et non protégeables par le droit d'auteur. *« Les algorithmes ne sont pas des programmes d'ordinateurs et constituent des modèles informatiques trop abstraits pour être protégés par le droit de la propriété intellectuelle ; ce n'est qu'en cas de mise en forme des algorithmes originaux que la protection par le droit d'auteur pourra être envisagée »*.

La Directive 91/250/CEE du Conseil, du 14 mai 1991, concerne la protection juridique des programmes d'ordinateur. Dans son considérant n° 14, celle-ci indique *« (…) que, en accord avec ce principe du droit d'auteur, les idées et principes qui sont à la base de la logique, des algorithmes et des langages de programmation ne sont pas protégés en vertu de la présente directive »*.

Le droit d'auteur ne permet donc pas de protéger les algorithmes. Ils peuvent néanmoins être protégés par l'intermédiaire des logiciels auxquels ils s'incorporent (CJUE 2 mai 2012, aff. C-406/10, *SAS Institute c/World Programming*), si et seulement si ces logiciels sont originaux (Civ. 1ère, 14 nov. 2013, n° 12-20.687).

En revanche, n'étant pas protégés directement, rien ne s'oppose à ce que les utilisateurs qui parviennent, de façon licite, à comprendre les algorithmes incorporés dans le logiciel puissent les répliquer (CJUE 2 mai 2012, aff. C-406/10, *SAS Institute c/World Programming)*. Cependant, cela a une influence bien moindre dans le domaine de l'intelligence artificielle puisque le degré de complexité et la diversité des influences sont tels qu'il est en pratique difficile de réaliser un procédé de *« reverse engineering »*.

Propriété industrielle

Le droit français des brevets ne permet pas non plus de protéger les algorithmes, car, en vertu de l'article L. 611-10 du code de la propriété intellectuelle :

> ***« 1. Sont brevetables, dans tous les domaines technologiques, les inventions nouvelles impliquant une activité inventive et susceptibles d'application industrielle.***
> ***2. Ne sont pas considérées comme des inventions au sens du premier alinéa du présent article notamment :***
> ***a) Les découvertes ainsi que les théories scientifiques et les méthodes mathématiques (…) ».***

Néanmoins, en droit européen, un algorithme peut être brevetable à condition qu'il soit intégré à une invention brevetable et lui apporte une contribution technique. Concernant les logiciels, la jurisprudence européenne ne semble pas apporter de réponse constante à la question de savoir si ceux-ci peuvent être considérés comme une invention au sens de la Convention sur le Brevet Européen (ci-après CBE). En tout état de cause, il faut qu'il existe

une invention comprenant un algorithme pour que ce dernier puisse être protégé. Cette protection n'est pas accordée très fréquemment. L'avantage est que, lorsqu'un algorithme est protégé par un brevet, il l'est au même titre que l'invention brevetée. L'inconvénient est que breveter un algorithme implique de dévoiler son fonctionnement.

Certains brevets intégrant de l'IA sont déposés par des créateurs de startups dans le seul but de valoriser leur entreprise. Plusieurs de ces brevets sont « faibles » et ne résistent pas à une action judiciaire, laquelle est néanmoins onéreuse en ce domaine. On peut rédiger les revendications d'un brevet de sorte que l'intelligence artificielle soit couverte par la protection du brevet. L'algorithme doit figurer dans la demande de brevet pour être protégé par le brevet, et ce dans la limite de l'invention à laquelle il s'intègre. Or, cela fige l'algorithme, par définition susceptible d'évolution. Par ailleurs, il peut être préférable dans certains cas de ne pas divulguer l'algorithme et de le garder secret.

Secret des affaires

Le secret des affaires a été envisagé pour pallier l'absence de protection directe des algorithmes. La directive 2016/943 du parlement européen et du conseil du 8 juin 2016 est venue harmoniser les différentes législations nationales relatives au secret des affaires. La responsabilité contractuelle des contractants ou délictuelle des tiers en cas de parasitisme ou de concurrence déloyale peut être engagée en cas de violation du secret des affaires. Cette protection est limitée au cas où l'information protégée est obtenue illicitement. L'administration de la preuve n'est pas aisée en cette matière, ce qui limitera la protection apportée au détenteur d'algorithme. En outre, ce dispositif ne permet pas de protéger un algorithme lorsqu'il fait l'objet d'un processus de reverse engineering licite (cf : CJUE 2 mai 2012, aff. C-406/10, *SAS Institute c/ World Programming*). Pour bénéficier de la protection, l'algorithme doit être secret, présenter une valeur commerciale et avoir fait l'objet de mesures de protection raisonnables.

Quelle que soit la protection retenue, certaines données mises en œuvre par un algorithme ne devaient pas pouvoir faire l'objet de protection dès lors que de telles données sont publiques et ont été nécessaires à la création de l'algorithme.

Modification du droit d'auteur

Une modification du droit d'auteur pour protéger l'algorithme serait, comme indiqué précédemment, contraire à la conception française du droit d'auteur qui est personnaliste. Le recours au droit voisin du droit d'auteur serait plus défendable (voir par exemple ci-dessous).

Création d'un droit voisin au droit d'auteur

La protection d'un algorithme pourrait, comme la protection juridique des bases de données, se fonder sur l'effort substantiel d'investissement de son producteur. Ce critère d'investissement pourrait être repris à propos des algorithmes pour leur assurer une protection juridique.

Rappelons que le producteur de la base de données bénéficie notamment d'une protection sui generis dont l'objet est *« d'as-*

surer la protection d'un investissement dans l'obtention, la vérification ou la présentation du contenu d'une base de données pour la durée limitée du droit ; que cet investissement peut consister dans la mise en œuvre de moyens financiers et/ou d'emploi du temps, d'efforts et d'énergie », selon le considérant n° 40 de la directive n° 96/9 du Parlement Européen et du Conseil, du 11 mars 1996 concernant la protection juridique des bases de données, texte transposé en droit français par loi n° 98-536 du 1er juillet 1998 (voir articles L. 341-1 et suivants du Code de la propriété intellectuelle).

Propriété intellectuelle d'un algorithme produit par une IA

La qualité d'auteur ne doit pas être reconnue aux robots. L'intervention humaine est en effet l'essence même du droit d'auteur. En revanche, un droit voisin du droit d'auteur est également ici envisageable.

Il faudrait toutefois *« veiller à enserrer le droit spécifique dans des limites raisonnables qui permettent de concilier la rémunération de l'investissement et le principe selon lequel les idées et informations sont de libre parcours. Il conviendrait de préciser l'objet de la protection (définition des créations générées par ordinateur, distinctes des créations assistées), la structure du droit envisagé (droit exclusif ou droit à rémunération et ses modalités d'exercice (gestion individuelle, gestion collective obligatoire), l'étendue de la protection (reprise à l'identique, partielle, substantielle ?), la durée de ce nouveau droit, et les éventuelles exceptions qui l'entourent*[56] *».*

56. A. LEBOIS, Maitre de conférences HDR à l'IEP de Rennes, Membre de l'IRDP, université de Nantes, Quelle protection juridique pour les créations des robots journalistes, Communication commerce électronique, n° 1, décembre 2015, étude 2.

La responsabilité

Déterminer la responsabilité en cas de préjudice

Il est difficile d'imputer une responsabilité juridique à une machine, mais cela est assez logique et même souhaitable. L'idée de créer une personnalité juridique au profit des robots est assez isolée et doit naturellement être combattue. D'une part, elle pourrait limiter la solvabilité du débiteur robot et déresponsabiliser ses fabricants, d'autre part, et c'est là l'argument essentiel, il semble difficilement concevable en occident, pour des raisons philosophiques et/ou éthiques, de conférer un statut identique à un être humain et à une machine.

« En toute hypothèse, la réparation ne serait réellement garantie que par la couverture du risque robotique par l'assurance, laquelle peut être souscrite par l'utilisateur/propriétaire du robot sans qu'il soit utile de faire du robot une personne juridique qui devrait s'assurer contre son propre risque. Ajoutons que l'admission d'une responsabilité des robots intelligents eux-mêmes pourrait avoir l'effet déviant de déresponsabiliser les fabricants et utilisateurs qui ne seraient plus incités à concevoir et utiliser des robots non-dangereux ou, à tout le moins, maîtrisés dans leur environnement si leur responsabilité personnelle pouvait être écartée au profit de celle des robots[57] *».*

Il est en revanche possible de déterminer a priori un ou des responsables (humains). Une des difficultés en matière d'IA est que de nombreux acteurs sont susceptibles d'intervenir, lesquels ne se connaitront pas nécessairement. Les responsabilités peuvent ainsi se trouver au niveau du choix des données d'apprentissage, de leur recueil et de leur organisation, de la conception des algorithmes, de la réalisation des logiciels, de l'interface, voire de la partie matérielle…

Lorsqu'apparaitront des dommages, il est probable qu'un recours à l'expertise sera nécessaire. Dans certains cas, le système pourra cependant se comporter d'une manière que n'auront pas pu prévoir les différents acteurs ayant concouru à sa création. Toute la question sera de déterminer si cela est de nature à exonérer ces acteurs de toute responsabilité. Il semble que plusieurs de ces acteurs puissent avoir une part de responsabilité, voire que les différentes responsabilités puissent éventuellement être engagées de manière solidaire (le mécanisme de jurisprudentiel de la responsabilité *in solidum* pourrait ici trouver un nouveau terrain d'application).

Si l'objectif est purement indemnitaire, il est possible de se rattacher à une approche « statutaire », de type responsabilité sans faute, où il s'agira de désigner *a priori* celui qui devra payer en cas de dommage, à charge pour lui de recourir à l'assurance.La propriété ne saurait entraîner une responsabilité de principe dès lors que l'intelligence artificielle faisant fonctionner un système peut échapper à son propriétaire, comme d'ailleurs à son utilisateur (qui n'est pas nécessairement un utilisateur volontaire, mais peut être contraint

57. La Semaine Juridique Edition Générale n° 48, 24 Novembre 2014, doctr. 1231, Du robot en droit à un droit des robots, Etude par G. LOISEAU professeur à l'École de droit de la Sorbonne (université Paris 1) et M. BOURGEOIS avocat au Barreau de Paris, associé du cabinet KGA Avocats Robotique. Voir dans le même sens, A. MENDOZA-CAMINADE, Le droit confronté à l'intelligence artificielle des robots : vers l'émergence de nouveaux concepts juridiques ? Rec. Dalloz 2016, p. 445.

d'utiliser le système). Une telle approche pourrait en revanche se concentrer sur « l'exploitant » tirant de l'intelligence artificielle un profit économique (certes parfois difficile à identifier) et s'inscrire dans la théorie juridique dite du « risque profit ».

Ce recours à la notion d'exploitant a déjà été utilisé. Il a par exemple été jugé par la Cour de justice de l'Union européenne que *« l'exploitant d'un moteur de recherche (Google) sur Internet est responsable du traitement qu'il effectue des données à caractère personnel qui apparaissent sur des pages web publiées par des tiers » (CJUE 13 mai 2014 affaire C-131/12 Google Spain SL, Google Inc. / Agencia Española de Protección de Datos).*[58] »

Les dispositions actuellement applicables semblent en tout cas d'un emploi malaisé. La responsabilité du fait des choses comme la responsabilité du fait des produits défectueux apparaît néanmoins comme les plus évidentes actuellement en la matière.

L'article 1242 du Code civil, al. 1er dispose en effet que l'on est notamment responsable « des choses que l'on a sous sa *garde*[59] ». La notion de garde – qui suppose traditionnellement usage, direction et contrôle – peut poser problème d'autant que le logiciel intégrant de l'IA peut être hors de contrôle du gardien (par exemple s'il est intégré à un objet connecté ou se met à jour tout seul, etc.), mais la notion de garde « juridique » est à explorer, celle-ci se fondant sur un titre juridique (tel que la propriété). Toutefois, si l'on se réfère à la garde juridique, il est clair que c'est simplement dans le seul but de trouver un responsable, quand bien même celui-ci n'aurait aucune maîtrise. La jurisprudence devra probablement évoluer également sur la notion de chose, dont il n'est écrit nulle part qu'elle doive être matérielle.

Une directive 85/374/CEE du 25 juillet 1985 sur la responsabilité du fait des produits défectueux organise par ailleurs une responsabilité sans faute des fabricants et distributeurs lorsqu'un produit cause des dommages corporels ou matériels du fait d'un défaut. Cette directive a été transposée par une loi n° 98-389du 19 mai 1998. Les dispositions nationales de transposition figurent désormais aux articles 1245 et suivants du Code civil. Ce régime spécifique de responsabilité s'applique aux produits mis en circulation par les producteurs, sociétés de grande distribution et importateurs du produit sur le territoire de l'Union européenne. Une responsabilité – subsidiaire par rapport aux producteurs – des fournisseurs professionnels, vendeurs ou loueurs est également prévue.

« Ce régime de responsabilité sans faute permet de mettre en cause la responsabilité des intervenants successifs, dès que ces professionnels sont intervenus dans le processus de production ou de distribution du produit. Le droit positif apparaît, à ce titre, parfaitement applicable à l'hypothèse d'un robot défectueux[60] *».*

Le demandeur doit prouver l'existence d'un dommage, le défaut du produit et le lien de causalité entre les deux. La qualification de défaut est large et peut englober les comportements et actes non anticipés. Le

58. www.legavox.fr/blog/ipness/chronologie-jurisprudence-francaise-europeenne-concernant-15033.htm.
59. Voir notamment sur ce sujet : N. NEVEJANS, Traité de droit et d'éthique de la robotique civile, LEH édition, 2017.
60. A. MENDOZA-CAMINADE, Le droit confronté à l'intelligence artificielle des robots : vers l'émergence de nouveaux concepts juridiques ? Dalloz, 2016. 445.

défaut peut exister même si le produit est réalisé dans les règles de l'art, selon des normes existantes ou encore après autorisation administrative, situation qui pourrait concerner, à terme, les produits intégrant une intelligence artificielle.

Est-ce que ces dispositions peuvent s'appliquer à un logiciel incorporant une intelligence artificielle ? L'article 1245-2 du Code civil désigne un produit comme tout bien meuble, précisant même que l'électricité est un produit. La Commission européenne a d'ailleurs déclaré que la directive devait s'appliquer aux logiciels. (Réponse ministérielle, 15 novembre 1988, JOCE, 8 mai 1989, C 144, page 142.). Mais il est vrai qu'une réponse ministérielle française considère que les cas d'application de ces dispositions à des logiciels devraient être exceptionnels (réponse ministérielle numéro 15677, JOANQ, 24 août 1998).

À notre connaissance, aucune décision ne s'est prononcée sur cette question. Alors qu'est nécessaire un « dessaisissement volontaire » du producteur au sens de l'article 1245-4 du Code civil, il n'est pas certain qu'un logiciel, qui ne serait pas intégré dans un support physique, relève de ces dispositions, mais cela, naturellement, peut se plaider. Notons qu'une résolution du Parlement européen du 16 février 2017 comporte un considérant n° 29 qui est ainsi rédigé : *« considérant que le cadre juridique actuel sur la responsabilité du fait des produits, en vertu duquel le fabricant d'un produit est responsable en cas de dysfonctionnement, et les règles définissant la responsabilité en cas d'actions dommageables, en vertu desquelles l'utilisateur d'un produit est responsable de tout comportement causant des dommages, s'applique aux dommages causés par un robot ou une intelligence artificielle ».*

En revanche, un logiciel qui intégrerait une intelligence artificielle et serait embarqué sur un robot autonome ou même un support physique devrait pouvoir plus facilement relever de ce régime. Dans un tel cas, en cas de dommage causé par le défaut d'un produit incorporé dans un autre, le producteur de la partie composante et celui qui a réalisé l'incorporation sont solidairement responsables (article 1245-7).

Il est possible que soit invoqué, dans des litiges à venir, l'article 1245-10 dernier alinéa du Code civil prévoyant que le producteur d'une composante n'est pas responsable s'il établit que le défaut est imputable à la conception du produit dans lequel cette partie a été incorporée ou aux instructions données par le producteur. Cette notion peut aussi poser problème dans le cas de robots qui téléchargeraient en ligne leur logiciel, leur mise à jour ou que l'utilisateur lui-même pourrait décider de modifier en téléchargeant, au-delà du système d'exploitation qui peut être fourni avec la machine, des applications sur des sites « tiers »... (Il faudra alors raisonner au cas par cas).

Reste le « risque de développement », dont on peut anticiper l'invocation par le producteur dans la mesure où l'état des connaissances scientifiques et techniques est en constante évolution dans ce domaine.

« On ne peut (...) ignorer que le droit de la responsabilité est devenu, dans une large mesure, le captif du droit des assurances. La résolution adoptée par le Parlement européen est sur cette ligne de temporalité, considérant que de nouveaux instruments ne pourront être mis en place qu'à un horizon de dix à quinze ans (Résolution du 16 févr. 2017, pt 51). C'est reconnaître que, pour l'heure, les conditions ne sont pas ré-

unies pour déterminer et mesurer précisément l'ensemble des risques. Durant cette période intermédiaire, les instruments du droit positif peuvent être encore mobilisés, au besoin en les adaptant s'agissant par exemple de l'exonération pour risques de développement dans le cadre de la responsabilité du fait des produits défectueux[61] *».*

L'article 1245-10, 4° du Code civil prévoit en effet que *« Le producteur est responsable de plein droit à moins qu'il ne prouve : (…) Que l'état des connaissances scientifiques et techniques, au moment où il a mis le produit en circulation, n'a pas permis de déceler l'existence du défaut (…) »*.

Il faudra patienter avant de savoir comment les juridictions appliqueront à l'intelligence artificielle responsabilité du fait des produits défectueux et en particulier comment seront interprétées les dispositions relatives au risque de développement, risque certes imprévisible, mais en réalité assurable grâce à différentes techniques.
Dans l'immédiat, la position plutôt attentiste du secteur assurantiel sur ce sujet semble néanmoins compréhensible en l'absence de recul permettant les nécessaires calculs actuariels.

Déterminer la responsabilité dans le cas d'incidents faisant intervenir immédiatement l'IA seule ou l'humain et l'IA

Il faut ajouter à cette complexité inhérente à l'outil celle qui résulte de son utilisation. La situation où l'IA seule intervient a été abordée précédemment. Celle où l'IA constitue l'un élément de la décision humaine doit aussi être envisagée. La notion de faute pourrait réapparaitre ici.

La difficulté tient à ce que, comme le dit de manière éclairante Jean-Paul Cailloux, *« le logiciel est le bourreau alors que le (système expert) est le juge »*[62]. On doit comprendre par là qu'une défaillance d'un logiciel se voit immédiatement et qu'une erreur est en principe parfaitement identifiable. En cas de recours à un système expert faisant intervenir une IA, il peut être particulièrement difficile de déceler une erreur, même pour un professionnel du domaine concerné. La solution pourra être différente selon que l'humain a bien ou mal utilisé le système.

Bonne utilisation du système : l'utilisateur peut avoir pris une décision erronée sur la base d'un résultat apporté par l'intelligence artificielle qui l'était déjà. S'en était-il rendu compte ? Devait-il s'en rendre compte ? Pouvait-il s'en rendre compte ? Il faudra pouvoir accorder sa confiance au système expert, car c'est sa raison d'être, mais cette confiance devra être raisonnable… Cette appréciation de la confiance à accorder au système devrait être fonction notamment de la présentation de l'IA fournie, de l'expérience de l'utilisateur, de sa formation, etc.

Mauvaise utilisation du système : l'erreur du système pourra provenir de l'introduction de mauvaises données, d'une erreur de manipulation. Dans les cas où le sys-

61. L'intégration de l'intelligence artificielle dans l'ordre juridique en droit commun : questions de temps – A. BENSAMOUN – G. LOISEAU – Dalloz IP/IT 2017. 239.
62. J.-P. CAILLOUX, La responsabilité des auteurs de systèmes experts, questions et incertitudes du droit français et du droit américain, in Droit et intelligence artificielle Romillat, 2000, p. 136 et ss. : système expert, de conseil et d'aide à la décision.

tème continue d'apprendre au fur et à mesure de son utilisation, une bonne pratique serait probablement d'assurer une traçabilité des usages les plus sensibles (danger pour l'intégrité notamment, risque systémique important, etc.). En tout cas, on devrait être responsable de ce que l'on apprend à une machine. Le concepteur quant à lui doit réfléchir à l'autonomie qu'il laisse à l'utilisateur pour modifier le système.

La Fédération Française de l'Assurance (FFA) préconise une approche graduelle, pragmatique et sectorielle sur toute future initiative en la matière. Elle souhaite notamment que cette question soit étudiée en distinguant trois cas d'usage de ces technologies dans la mesure où chacun d'eux présente un contexte très différent des deux autres.

1er cas d'usage

La première application d'ores et déjà effective de l'intelligence artificielle et de la robotique est celle destinée à automatiser des processus de production, que cela soit dans le domaine industriel ou celui des services. Nous sommes là dans des relations entre professionnels avec d'un côté un fournisseur de technologies et de l'autre un industriel ou un fournisseur de services utilisateur de ces technologies dans ses processus de fabrication. La relation de « professionnel à professionnel » place les deux parties dans une situation équivalente de connaissance des risques induits par l'introduction de ces nouvelles technologies. Il est par conséquent inutile de rajouter au droit existant des protections supplémentaires dans la mesure où un consommateur particulier final n'est pas directement exposé par un manquement ou par une défaillance. La complexité des technologies et celle des contrats entre professionnels induite par le nombre des intervenants n'est pas une caractéristique exclusive de l'intelligence artificielle.

La FFA estime par conséquent, que dans les cas d'usage de technologies faisant appel à l'intelligence artificielle ou à la robotique et qui ne concernent que des professionnels (relations « B2B »), il n'y a pas lieu de rajouter un encadrement supplémentaire à celui existant (juillet 2017).

2e cas d'usage

Il convient ensuite de dissocier les technologies embarquées dans des véhicules automobiles. Pour ce qui est des dispositifs de délégation partielle ou totale de conduite d'un véhicule, il apparait qu'aussi bien les régimes encadrant la responsabilité civile automobile (loi dite Badinter) que leur assurance obligatoire sont compatibles.

L'arsenal juridique existant garantit un très haut niveau de protection des utilisateurs et un taux d'équipement en assurance très élevé au regard des dommages potentiels.

Aussi pour les technologies faisant appel à la robotique ou à l'intelligence artificielle embarquée dans des véhicules terrestres à moteur, la FFA estime qu'il n'y a pas lieu là encore de rajouter un encadrement supplémentaire à celui existant.

3e cas d'usage

C'est dans les applications de ces technologies à des produits ou services directement destinés à des consommateurs particuliers (« B2C ») hors automobile que

la question d'une évolution éventuelle des régimes de responsabilité en cas de dommages corporels et/ou matériels dus à l'intelligence artificielle peut se poser.

Si de nombreux usages de ces technologies d'intelligence artificielle se profilent aujourd'hui, il est difficile à ce stade d'anticiper les principaux domaines où l'intelligence artificielle sera utilisée, comment, et avec quel horizon, pour que la question de la protection de l'utilisateur puisse être clairement cernée.

Par ailleurs, les capacités d'adaptation et d'apprentissage des algorithmes régissant cette intelligence artificielle et la part d'imprévisibilité dans leur comportement qui échapperait au contrôle direct de leur fabricant ou de leur gardien sont trop incertaines pour pouvoir apprécier la nécessité de régimes spécifiques.

Ces constats amènent la FFA à estimer qu'il serait prématuré d'envisager toute création ex nihilo d'un régime de responsabilité spécifique au robot et à l'intelligence artificielle ou de nouvelles obligations d'assurance, et ce d'autant plus qu'il existe à ce stade un marché d'assurance pour les IA et qui pourrait couvrir les nouveaux risques associés. La FFA juge que de telles initiatives présentent aujourd'hui un ratio « coût/bénéfice » défavorable, tout en sachant qu'il évoluera probablement à terme.

Avant de légiférer, il parait préférable de cerner au préalable les questions juridiques inédites que soulèveront la mise en œuvre et l'utilisation de solutions d'intelligence artificielle avec des robots. Or, ces questions juridiques inédites ne sont pas avérées ou bien identifiées. Si par exemple apparaissaient des questions d'ordre public relatives à la détermination des choix à opérer dans le cadre de solutions d'intelligence artificielle associées à des moyens de transport, une réflexion devrait être menée, éventuellement dans un cadre international.

À court terme, la FFA préconise plutôt pour ce qui est de l'intelligence artificielle :

- Le développement d'un observatoire recensant les accidents possibles afin d'appréhender au mieux le risque ;
- La certification ou homologation des IA en forte interaction avec l'humain, voire l'établissement d'autorisations préalables de mise sur le marché ;
- Une nécessaire traçabilité des données (boîtes noires, EDR…) afin de déterminer les responsabilités en jeu.

Le droit de la responsabilité civile devrait en tout cas sans trop de difficulté être en mesure d'absorber ces nouveaux enjeux. À ce jour, le droit actuel en ce domaine est encore très incertain, en l'absence de jurisprudence identifiée. Le thème relatif à la propriété de l'IA semble plus balisé.

2.7 POINTS SAILLANTS ORGANISATIONNELS ET TECHNIQUES

Faire savoir : communiquer, sensibiliser, former

La plupart des collaborateurs ne connaissent l'IA que par les médias qui véhiculent une image contrastée et souvent exagérée de la technologie et de ses capacités. Il est donc important de mieux faire connaître l'IA à tous les niveaux de l'entreprise, à l'image de grands groupes d'autres secteurs (énergie, transport, défense, par exemple) qui ont pris d'importantes initiatives internes de sensibilisation et de formation de leurs équipes sur l'IA.

Sensibiliser et former est donc un passage obligé qu'il convient de compléter par d'autres dispositions, en particulier le recrutement ou la montée en compétences de spécialistes à double compétence : science des données et métier de la banque et de l'assurance.

Un Comité Numérique au sein du Conseil d'Administration

Enjeux

Face aux enjeux de la transformation, plusieurs grands groupes intègrent une réflexion stratégique. Un exemple intéressant est celui du groupe Schneider Electric qui a créé un Comité Numérique au sein de son Conseil d'Administration. La mise en place d'un Comité Numérique au sein du Conseil d'Administration permet de mettre en œuvre une gouvernance numérique au plus haut niveau de l'entreprise et d'impliquer une réflexion au niveau de la gouvernance et des risques.

Les points clés à l'origine de la création du Comité Numérique au sein du Conseil d'Administration ont été motivés par le fait que le numérique était éparpillé. Or, le Conseil d'Administration avait besoin d'une vision d'ensemble :

- Nécessité de se doter d'une très forte compétence digitale : le Comité Numérique s'est mis naturellement en place avec un « Studies Committee » qui étudie tous les sujets transversaux du numérique et en relation avec les autres Comités ;
- Exemples : audit pour la cybersécurité, M&A *(Mergers & Acquisitions), digital transformation* des ressources, intégration des *millenials*, mise à jour des compétences, espaces de travail, offres au numérique, *pricing, go to market*, distribution, formation…

Le Comité est constitué de quatre membres et d'un secrétaire, le CIO-CDO du Groupe.

Recommandations

Afin que chaque entreprise cotée ou non cotée, PME, ETI ou grande entreprise disposant d'un Conseil d'Administration puisse bénéficier de ce nouvel organe de gouvernance numérique, une évolution du code Afep-Medef est aujourd'hui nécessaire. Historiquement, ce code ne recommande que trois Comités : Audit, Nominations et Rémunérations. Il convient désormais d'y ajouter le Comité Numérique.

Les aspects organisationnels

Les relations entre IA, travail, emploi et compétences ont été abordées dans les autres rapports mentionnés ci-dessus. On considère souvent l'IA comme un outil d'aide et au service d'un conseiller/opérateur humain qui garde le contrôle. En conséquence, la réflexion sur l'évolution des métiers pourra être menée notamment au sein du « lab. de transformation du travail » qui devrait être créé suite aux recommandations de la mission Villani.

Il y a un point d'attention sur l'intelligence humaine qui se modélise : le risque de perte de la connaissance humaine. En matière de priorités, comme dans d'autres secteurs, les opérateurs ont à faire le choix entre le développement interne ou l'acquisition de technologies sur étagères. De manière très naturelle, il convient de garder la maîtrise des technologies sur le *core business* afin de garder connaissances et compétences propres et de se reposer sur des solutions externes pour les fonctions support.

La présence d'un grand nombre de startups technologiques disposant d'une offre en IA dont la viabilité à long terme n'est, par définition, pas garantie entraînera probablement l'apparition de tiers de confiance pouvant assurer une certaine pérennité et évolutivité des produits. Par ailleurs, les startups ont besoin d'accès à des ressources de calcul qu'elles n'ont pas les moyens d'acquérir : une solution nationale est fortement souhaitée à des tarifs abordables.

L'apprentissage automatique

L'apprentissage automatique est clairement la technologie qui soutient la plupart des applications de l'IA (le secteur n'est pas exceptionnel en la matière), en raison du volume et de la diversité des données disponibles qui couvrent toutes les activités de la chaîne de valeur, de l'accès à des plateformes de calcul de très haute puissance pour réaliser l'apprentissage et des progrès de ces dernières années sur les architectures et les algorithmes d'optimisation.

Les points saillants sont les mêmes que ceux qui ont été identifiés dans d'autres domaines industriels :

- qualité et couverture des données d'apprentissage ;
- passage à la très grande échelle ;
- prise en compte de contraintes, notamment de respect de la vie privée ;
- capacité d'oubli pour des IA connectées à des systèmes en évolution permanente ;
- coopération entre les représentations continues (réseaux de neurones notamment) et symboliques (arbres de décision, graphes, sémantique…) ;
- la question de l'explication, déjà évoquée ci-dessus, pour assurer la confiance dans le système.

Le traîtement automatique de la langue

Le TAL est utilisé notamment pour les agents conversationnels et pour le traitement en masse de documents (production d'analyses, de synthèses…) et, moins souvent, intervient aussi en génération de nouveaux textes. Enfin, les outils du TAL sont mis à contribution pour la traduction automatique, un besoin important pour la profession, notamment pour la présentation des clauses contractuelles dans la langue cible.

Les principaux défis en TAL sont la nécessité de développer la modalité voix, encore peu utilisée : STT *(Speech to Text)*, TTS *(Text to Speech)* et l'amélioration de la compréhension des textes prononcés ou écrits, notamment pour comprendre le contexte et la multi-intention. Enfin, il est souvent fait appel à des modules TALN développés initialement pour l'anglais : il devient important de disposer de technologies comprenant nativement le français.

Les hybridations des technologies IA

Les IA devenant de plus en plus présentes dans les systèmes bancaires et assurantiels, une couche d'orchestration entre des IA basées sur des technologies différentes va devenir indispensable. Ce type d'interaction n'est pas naturel et va demander des développements complémentaires. Les solutions intégrées provenant d'un fournisseur unique ne sont pas souhaitables dans tous les cas. Par exemple, la Commission Européenne a récemment publié un appel à propositions pour la réalisation d'une plateforme européenne d'intégration des technologies d'IA, ce qui est également une recommandation du rapport #FranceIA.

Un autre aspect est celui de l'intégration de données externes alternatives qui va nécessiter la mise en place de solutions techniques pour inter-opérer les solutions « natives » du secteur avec des données et des modules externes au domaine bancaire.

La confiance dans la relation client

La question de la confiance est évidemment essentielle pour des systèmes amenés à prendre des décisions ou faire des recommandations ayant un impact important sur les individus. Pour cela, il faut principalement améliorer la transparence des algorithmes d'intelligence artificielle au moyen de toutes les solutions techniques possibles :

- interfaces humain-machine permettant d'interpréter les raisonnements ;
- production d'explications, de preuves et de garanties ;
- mise en place de systèmes fondés sur la réputation lorsque les solutions algorithmiques ne sont pas suffisantes ;
- réalisation de documentations techniques permettant de comprendre les algorithmes utilisés, en particulier dans les solutions clé en main des fournisseurs de technologies.

Les systèmes capables de détecter les fausses informations *(fake news)* sont également intéressants pour les applications d'analyse et de synthèse de contenus. La confiance est également fragilisée lorsque la protection de la vie privée n'est pas assurée : pour cela, il est indispensable de respecter la réglementation qui s'applique, en particulier la RGPD, effective en Europe à partir de fin mai 2018. Il est nécessaire de disposer de solutions d'anonymisation des données servant à l'entraînement ou à la prise de décision des IA. Enfin, l'explicabilité est également essentielle (voir DIP 15). La responsabilité de prise de décision demande à être étudiée attentivement, en particulier lors-

qu'une décision se révèle mauvaise et cause des dommages à des personnes ou à des organisations.

Reste enfin la question du juste positionnement du curseur entre conformité, qui demande à la fois des traitements globaux, et hyper-personnalisation pour répondre le mieux aux attentes des clients. Des travaux spécifiques sur le sujet sont souhaités.

Garantir dans le temps la performance, la cohérence et la robustesse de la solution à base d'IA

Comme tout équipement technologique ou logiciel, une IA en production doit être accompagnée de prestations de maintenances évolutives ou correctives pour prendre en compte les évolutions fonctionnelles et les bugs lors de développement.

Cependant, une IA, notamment lorsque sont mises en œuvre des techniques de machine learning, doit faire l'objet d'une maintenance spécifique permettant de s'assurer que son fonctionnement ne dérive pas au cours de temps, ce qui entraînerait immanquablement des résultats non conformes aux attentes ou objectifs attendus. En effet, très souvent, une IA est mathématiquement un système dynamique dont les résultats à l'instant « T » dépendent des résultats précédents à partir d'algorithmes itératifs prenant en compte les données générées produites ou utilisées.

Il est donc indispensable de réaliser des opérations de contrôle de cohérence et de robustesse permettant d'identifier des écarts éventuels par rapport à des valeurs/comportements étalons et de réaliser les corrections éventuelles tout au long du fonctionnement de l'IA. Ces opérations de contrôle et de maintenance doivent être pensées et conçues *by design*, dès

la phase de spécification et de conception de l'IA, notamment dans le cadre de solutions mettant en œuvre des réseaux de neurones dont le comportement au cours de temps n'est pas à ce jour modélisable et fait actuellement l'objet de nombreuses recherches.

De plus, il est indispensable d'implémenter dès la conception des fonctions garantissant la transparence, la traçabilité, la neutralité et la pertinence des activités/exécutions de l'IA. De nombreuses réflexions et développements sont actuellement menés sur ces sujets.




La blockchain
au service
de l'industrie
financière

3. La blockchain au service de l'industrie financière

3.1 PRÉAMBULE

Les institutions financières françaises s'intéressent déjà depuis plusieurs années à la technologie décentralisée des chaînes de blocs ou blockchains, et ceci est d'autant plus vrai depuis trois ans. Selon une étude PwC « *Blockchain is here. What's your next move ?* », 600 dirigeants dans le monde indiquent leur prise de conscience forte sur ce sujet, et 84 % des cadres interrogés rapportent des initiatives de blockchain en cours, dont 15 % des initiatives déjà établies.

À travers des formations métiers et techniques, la plupart des grandes institutions ont procédé à une acculturation et à une première évangélisation de leurs équipes. Plusieurs prototypes (*POC/Proof Of Concept*) ont été réalisés dont certains sont en phase d'industrialisation, même s'ils sont encore peu nombreux fin 2018. Cela a permis de mieux comprendre cette technologie, ses opportunités et ses contraintes, tant en termes de métiers que de maîtrise de ses aspects techniques.

Plusieurs grandes institutions financières françaises font partie du peloton de tête mondial de cette technologie et presque toutes y travaillent. Le passage du prototype à l'opérationnel, la performance des protocoles, la maîtrise du modèle économique, la gouvernance, la conformité et la sécurité sont les enjeux d'aujourd'hui. Des impacts sur les produits et les organisations apparaissent en filigrane.

À cette fin, le Pôle FINANCE INNOVATION a recueilli les avis de plusieurs experts au sein de ces institutions françaises ainsi que des spécialistes en informatique, en droit et en organisation des entreprises. L'objet de ce livre blanc est d'apporter un éclairage sur les points d'accélération afin d'aider ces institutions à conforter leur avance et à progresser au rythme nécessaire face à l'évolution rapide de cette technologie, et ce, grâce à un écosystème porteur et ouvert

3.2 DÉFINITIONS DE LA BLOCKCHAIN

Afin de permettre une lecture précise et claire de ce livre blanc, il est utile de rappeler les principales définitions et éléments constituant cette technologie.

Définition du DLT et de la blockchain

Un DLT (en anglais* Distributed Ledger Technology*/technologie de registre distribué) est un registre synchronisé simultanément sur un réseau de participants en pair à pair sans administrateur central.

La chaîne de blocs ou blockchain est un registre distribué. Il est courant de parler de DLT comme synonyme de blockchain.

La blockchain est une technologie de stockage et de transmission d'informations, transparente et sécurisée grâce à un mécanisme de consensus de résolution entre les

participants associé à des processus de cryptographie. Par extension, une blockchain permet de constituer une base de données sous la forme d'un registre, en finance un livre de comptes, distribué entre toutes les adresses du réseau et permettant de retracer de façon immuable et transparente toutes les opérations effectuées.

Elle est constituée d'une succession de blocs contenant chacun des informations sur les transactions effectuées entre deux ou plusieurs participants. Chaque transaction est vérifiée par des algorithmes avant d'être validée et enregistrée dans un nouveau bloc qui s'ajoute à la chaine. Les informations inscrites ne peuvent pas être altérées, car la traçabilité des informations est garantie par la constitution de la blockchain. En effet, chaque bloc garde une trace de la transaction précédente et se lie au bloc suivant en respectant l'ordre chronologique.

Les transactions enregistrées sur une blockchain correspondent généralement à des changements d'état (changement de valeur d'un compte, transfert d'un actif financier matériel ou immatériel d'un acteur à un autre, etc.) ainsi que des horodatages d'évènements ou de documents.

Une des premières définitions officielles de la blockchain en France définit cette technologie en octobre 2017 sous le terme de « dispositif d'enregistrement électronique partagé (DEEP[63]) ». Le terme d'enregistrement est à prendre au sens fort : il est définitif, immuable, ineffaçable.

Globalement, les chaînes de blocs ou blockchains sont des infrastructures numériques qui permettront le développement de nouveaux services, comme les infrastructures Internet ont permis de créer en une dizaine d'années un ensemble de nouveaux usages et une nouvelle économie. En presque dix ans, un véritable écosystème blockchain, qui ne travaille pas que sur la seule problématique des crypto-monnaies, s'est construit regroupant plusieurs milliers de structures (entreprises, fondations ou simples regroupements d'individualités autour d'un projet).

63. www.kiosque.bercy.gouv.fr/alyas/search/print/lettre-daj/8555.

Plusieurs sous-ensembles de technologies distinctes

Les systèmes construits sur une blockchain s'appuient sur cinq sous-ensembles de technologies aux propriétés très différentes. Leurs interactions doivent être finement analysées pour juger du niveau de sûreté, de gouvernance et de pérennité d'un système :

- **Des technologies « dures » de cryptographie :** signatures électroniques, condensat ou hash, chiffrage asymétrique, appuyées par des règles formelles de construction du consensus entre les systèmes distribués ;
- **Des technologies des sciences sociales et économiques :** théorie des jeux, mécanismes d'incitation, comportement de la communauté/multitude, motivations et objectifs réels des participants au consensus ;
- **Des technologies de programmation** basées sur de nouveaux langages permettant de construire des modules opérant sur ces chaînes avec les forces (traitements automatisés, infalsifiables) et faiblesses usuelles (bogues, hacks facilités par la nouveauté de ces technologies, difficultés d'adéquation avec des spécifications non totalement formalisées) ;
- **Des interfaces** pour intégrer une blockchain dans l'environnement du système d'information usuel, généralement basé sur des technologies classiques en développant des interfaces homme-machine et d'entrées/sorties des informations ;
- **Des concepts plus avancés de cryptographie ou de consensus** complémentaires des blockchains, par exemple la « Preuve sans divulgation » ou « *Zero Knowledge Proof* », qui permet de prouver qu'une proposition est vraie sans dévoiler toutes les informations contributives à cette preuve.

Les caractéristiques globales du système (sécurité, résilience, puissance de traitement, etc.) doivent s'évaluer sur l'ensemble des composantes et pas uniquement sur les caractéristiques de la seule blockchain placée au cœur de l'ensemble.

Une typologie de blockchains selon la nature publique ou privée de leur gouvernance

- **Les blockchains publiques**, parmi lesquelles Bitcoin et Ethereum, offrent à chacun la liberté de s'intégrer dans le réseau sans aucune restriction d'accès. Les chaînes opérées sur des milliers de nœuds présentent généralement une bonne résilience et un accès universel aux données enregistrées. La gouvernance est implicite pour tous les acteurs avec le rôle particulier des développeurs du cœur du système et des mineurs[64] qui assurent le travail de contrôle des transactions.
- **Les blockchains privées** offrent la possibilité de mettre en place et de gérer des restrictions d'accès à des participants déterminés et d'organiser une gouvernance spécifique contrôlée par une entité centralisée dans le réseau. Il n'existe aucun mécanisme de consensus et les règles de fonctionnement sont spécifiques aux accords passés entre les membres participants (différents niveaux d'autorisation sont possibles : accès en lecture seule, en écriture). Les solutions qui répondent actuellement aux enjeux de blockchains privées sont par exemple Hyperledger Fabric d'IBM, Corda de R3 CEV ou encore une infrastructure basée sur Ethereum, mais montée spécifiquement sur blockchain privée.

64. Le minage est l'activité d'un participant au consensus d'une chaîne de blocs consistant à conserver le contenu de la chaîne, vérifier le contenu d'un nouveau bloc puis son ajout à la chaîne en respectant les protocoles définis.

Pourquoi utiliser une blockchain ?

Dans un premier temps il est important d'évaluer **la pertinence de l'utilisation d'une blockchain**. De nombreux projets se focalisent sur cette technologie bien qu'il ne s'agisse pas toujours de la solution la plus adaptée. Parfois il est préférable d'identifier les raisons de ne pas avoir un système unique et centralisé, plutôt que de se concentrer sur les avantages de la blockchain.

Quelques critères semblent dominants pour s'orienter vers une technologie blockchain :

- Un grand nombre de participants indépendants : la blockchain gagne en pertinence dans des écosystèmes complexes où les différents acteurs qu'ils soient partenaires ou concurrents collaborent sur une même chaîne de valeur et sont dépendants les uns des autres.
- Un besoin de confiance fort : le caractère immuable de la blockchain en fait un candidat parfait pour partager des données et en contrôler les modifications et mises à jour entre partenaires.
- L'intermédiation à supprimer : la suppression des intermédiaires doit être pensée notamment en termes de coût, complexité et délais d'exécution des interactions.

Dans un second temps, il convient de choisir le type de blockchain, publique ou privée. Cela passe par la détermination des règles de gouvernance en répondant à quelques questions : y a-t-il des enjeux de confidentialité ? Quels droits de lecture ou d'écritures ? Besoin d'une base de données cryptée ?... (voir Annexe 3).

Comment ça marche : l'exemple du bitcoin

Sans vouloir décrire toutes les options architecturales des blockchains, le décryptage de la première chaîne Bitcoin permet de matérialiser les principes énoncés ci-dessus.

L'objectif de la chaîne Bitcoin est d'échanger une monnaie/actif numérique en interdisant les doubles dépenses (un propriétaire de bitcoin ne peut céder une même valeur deux fois en parallèle) tout en gérant précautionneusement la création monétaire.

Les participants ont donc construit une chaîne de blocs où chaque bloc est lié par l'inclusion de son condensat ou hash (résumé cryptographique) dans le bloc suivant. Ainsi toute modification impacte l'ensemble des blocs suivants et l'immuabilité d'une transaction s'accroît avec les ajouts successifs de blocs ultérieurs. Les identités des émetteurs et récepteurs d'une transaction sont identifiées par une clé publique, la clé privée restant sous le seul contrôle de l'utilisateur. Le montant de la transaction est enregistré et en clair pour être lisible par tous.

Ces données permettent de s'assurer de la propriété antérieure du montant de la transaction par l'émetteur (et donc l'interdiction de sa double dépense) grâce à l'ensemble des mineurs, les validateurs volontaires du réseau. Le blockchain bitcoin compte aujourd'hui plusieurs centaines de milliers de mineurs répartis

dans le monde. Cette diffusion large des transactions et du registre ouvert en lecture sur Internet confère à l'ensemble sa résilience. Le rôle de mineur peut être tenu par tout propriétaire d'un ordinateur apte à installer un nœud de traitement disponible en open source sans aucune autorisation préalable.

L'unicité d'ajout d'un bloc est assurée par un dispositif aléatoire de choix du nœud qui réussit à résoudre un problème « à fonction mono directionnelle » (solution complexe donc longue à trouver par essais-erreurs, mais facile à vérifier par la communauté). L'approche aléatoire basée sur la puissance de calcul pour maximiser la vitesse des essais-erreurs vise à permettre l'application des règles du logiciel même si une partie des nœuds du réseau souhaitent en faire autrement ; les nœuds conformes conserveront la maîtrise des règles tant que leur puissance de calcul permettra de s'imposer statistiquement.

L'immuabilité est obtenue par l'association de la distribution du registre sur un très grand nombre de nœuds et d'un système de création de nouveau bloc résistant jusqu'à un certain point à l'intrusion de nœuds malveillants.

La création des crypto-actifs est liée à la création des blocs et donc strictement régulée dans le temps avec une réduction asymptotique du nombre de bitcoins ajoutés en circulation : à chaque cycle, un quota de nouveaux bitcoins est ainsi versé au propriétaire de l'adresse qui a imposé le nouveau bloc de transactions.

La convertibilité de cette monnaie/actif numérique en devises courantes fin 2010 a conféré à l'ensemble une gouvernance implicite solide en faisant converger les intérêts individuels des acteurs vers une réussite globale du jeton inclus dans le logiciel.

Un temps de cycle d'environ 10 minutes est maintenu par l'évolution incluse dans l'algorithme de la difficulté du problème à résoudre pour imposer son bloc à la communauté. La taille maximale du bloc a été fixée initialement à 1 Mo pour satisfaire autant de transferts du réseau mondial Internet et éviter trop de divergences entre ces nœuds asynchrones. Ces caractéristiques permettent d'atteindre une capacité maximale théorique pour l'heure de sept transactions par seconde, trois en pratique. Cette taille de bloc et ces performances limitées sont en cours d'évolution vers des capacités supérieures.

Depuis sa création début 2009, plusieurs améliorations sont venues résoudre les faiblesses de la solution originelle et ont été généralement acceptées par tous les acteurs. Néanmoins, deux divergences notables ont déjà donné lieu à la création de chaînes parallèles.

.

3.3 LA CRYPTO-ÉCONOMIE

Crypto-économie, crypto-actifs, crypto-monnaies, mais de quoi parle-t-on ? Que signifient ces termes ? Quels usages recouvrent-ils ?

L'émergence des crypto-actifs[65] est une des conséquences de la digitalisation de la valeur, c'est-à-dire de la capacité de représenter numériquement un actif et de le transférer en toute sécurité entre individus et sans aucun intermédiaire grâce à la technologie. Les représentations digitales de valeur sont appelées des « jetons » ou plus fréquemment des « tokens ». La cryptographie moderne permet, le cas échéant, de faire cette opération de manière anonyme. On peut donc créer des monnaies et des actifs financiers digitaux digitaux « au porteur[66] ».

La création des crypto-actifs repose sur la technologie blockchain qui, par sa nature décentralisée, inviolable et transparente, permet le transfert des jetons en peer-to-peer sans intermédiaire.

Il est courant aujourd'hui de parler de monnaie virtuelle, de monnaie électronique, de monnaie cryptographique ou encore de monnaie numérique sans que l'on sache bien ce qui se trouve derrière de tels termes. Pour la plupart des personnes qui ne sont pas des experts des questions monétaires, il est même probable que toutes ces notions n'en forment qu'une seule. L'idée (ou plutôt l'impression) qui prédomine actuellement est celle d'une monnaie dématérialisée dont le niveau d'abstraction rend le monde de la banque et les mécanismes de la finance difficilement compréhensible par le grand public.

Cette famille des monnaies virtuelles s'oppose à une autre famille qui est celle des monnaies fiduciaires et scripturales. Dans beaucoup d'institutions bancaires notamment, les monnaies fiduciaires et scripturales sont perçues comme les seules monnaies légitimes. Toutefois, leur importance tend à diminuer de façon spectaculaire. Avec l'apparition de l'ordinateur, l'arrivée d'internet, celles de la blockchain, de l'intelligence artificielle et enfin du traitement quantique, l'univers des monnaies virtuelles augmente significativement et se positionne à côté du territoire des monnaies classiques. Dans une perspective historique, les monnaies virtuelles ne datent donc pas d'hier, mais il convient plus que jamais de savoir représenter de façon juste et précise cette nouvelle famille monétaire. Nous proposons ici un ensemble de définitions permettant de mieux les distinguer en faisant ressortir le mouvement historique de dématérialisation ET de décentralisation qui est le fil conducteur de toutes ces nouvelles expériences monétaires.

La monnaie électronique

Selon l'article L315-1 du code monétaire et financier, la monnaie électronique se définit de la façon suivante : « *La monnaie électronique est une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement définies à l'article L. 133-3 et qui est acceptée par une*

65. La Banque de France a statué en juillet 2018 pour retenir la qualification de « crypto-actif » et non de crypto-monnaie.
66. Rapport Landau, Les crypto-monnaies, juillet 2018.

personne physique ou morale autre que l'émetteur de monnaie électronique. Les unités de monnaie électronique sont dites unités de valeur, chacune constituant une créance incorporée dans un titre».

La monnaie électronique conserve un lien avec les monnaies traditionnelles dès lors que les fonds sont exprimés dans la même unité de compte (euro, dollar…) et que la monnaie est acceptée par d'autres personnes que l'émetteur (en France, le porte-monnaie électronique *Monéo* en était l'exemple le plus marquant). Elle se distingue des services de paiement sans contact (du type *ApplePay*) dès lors que s'agissant de la monnaie électronique, l'émetteur remet au porteur de la solution de paiement des unités de valeur prépayées qui sont matériellement stockées directement sur la carte bancaire ou sur un porte-monnaie électronique en ligne. Ces unités de valeurs sont ensuite utilisées pour effectuer des opérations de paiement auprès de tiers autres que l'émetteur. Le remboursement des unités de monnaie électronique est effectué à la valeur nominale des unités.

La monnaie virtuelle

Elle peut se définir comme une unité de compte stockée sur un support électronique créée par une personne (physique ou morale) et destinée à comptabiliser les échanges. Elle est généralement créée par une société pour un usage spécifique dans un univers restreint. Dès lors, elle ne rencontre pas parfaitement les critères de qualification de la monnaie électronique et ne relève donc pas de la réglementation européenne applicable. On distingue différents types de monnaie virtuelle :

- les monnaies virtuelles non convertibles en devises ne pouvant être utilisées que dans des jeux vidéos par exemple,
- les monnaies virtuelles avec un flux unidirectionnel pouvant être achetées avec de la devise légale, mais non reconvertibles en devise légale (ex. : points de fidélités, bons d'achat),
- les monnaies virtuelles avec un flux bidirectionnel avec un cours d'achat et de revente pouvant s'exprimer en monnaie classique (ex : bitcoin et toutes les crypto-monnaies créées sur la blockchain).

Les monnaies virtuelles ont pour point commun d'être définies par une unité de compte n'ayant pas de statut légal et de ne pas être régulées par une Banque centrale ni émises (créées) par des établissements financiers réglementés.

La crypto-monnaie, dite aussi crypto-actif, crypto-devise, monnaie cryptographique

Elle se présente sous la forme d'un jeton (*token*) échangeable entre particuliers sur le réseau Internet. Les opérateurs, les fichiers et les transactions sont cryptés de façon à ce que personne ne puisse avoir la maîtrise du système. Les jetons sont créés de façon endogène, comme récompense d'un processus décentralisé de validation. Le terme « crypto-actif » est fortement suggéré par les institutions d'émission, notamment la BCE et la Banque de France qui différencie les crypto-monnaies des titres de reconnaissance de dette. Ces banques définissent les crypto-monnaies comme *« tout instrument contenant sous forme numérique des unités de valeur non monétaire pouvant être conservées ou être transférées dans le but d'acquérir un bien ou un service, mais ne représentant pas de créance sur l'émetteur »*.

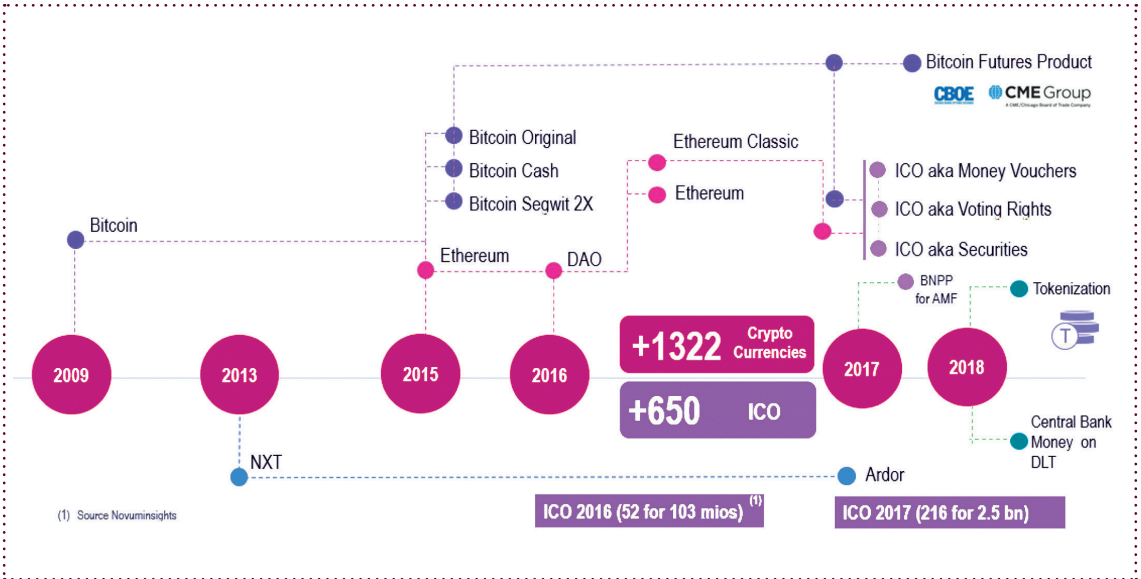
La plus connue des crypto-monnaies, qui utilisent toutes la technologie blockain, est le bitcoin. Les crypto-monnaies décentralisées ont pour point commun d'être définies par une unité de compte n'ayant pas de statut légal, de ne pas être régulées par une Banque centrale et de ne pas être émises (créées) par un émetteur unique identifié. En effet, la création de ces crypto-monnaies de type bitcoin résulte de l'utilisation d'un logiciel libre via un réseau décentralisé de type peer-to-peer.

La monnaie numérique ou monnaie intelligente

Elle se présente aussi sous la forme d'un jeton (*token*) qui se différencie de toutes les formes de monnaies antérieures dites « fiat » (c.-à-d. émises par un État) ou crypto du fait qu'il permet de renouveler et d'élargir exponentiellement le champ des usages et des opérations accessibles à la monnaie. Traditionnellement, une monnaie est un instrument mono-usage de paiement déplacé en fonction des échanges. La monnaie numérique innove, car son support technologique lui permet d'embarquer un logiciel démultipliant le nombre de fonctionnalités accessibles aux utilisateurs. On parle de monnaie intelligente ou de monnaie dynamique dès lors qu'il devient possible de faire entrer dans l'instrument monétaire en les automatisant une quantité illimitée d'opérations jusqu'à présent étrangères à la monnaie.

Le web 1.0 a permis aux usagers de faire eux-mêmes leurs virements et leurs gestions de comptes. Avec le web 2.0, ils ont ensuite financé eux-mêmes leurs projets grâce au *crowdfunding*. Le web 3.0 permet aujourd'hui à tout usager de participer à la validation des transactions monétaires en devenant mineur sur une blockchain. Le web 4.0 permettra demain à tout usager de créer lui-même sa propre monnaie pour en faire le vecteur des valeurs qu'il désire promouvoir. C'est au développement de cette dernière branche du web 4.0 que travaille aujourd'hui le projet français de *smart tokenization Money by Design*.

On peut prédire déjà que le business modèle du *smart token* aura une courbe d'adoption assez semblable à celle du smart phone qui a transformé un appareil ne servant qu'à téléphoner en un instru-



ment intelligent doté de fonctionnalités illimitées. L'extension des usages allant avec l'intensification de ces mêmes usages, il est assez aisé d'imaginer le bénéfice utilisateur qui résultera d'une monnaie :

- dont les unités de compte peuvent être librement conçues par chacun ;
- dont la valeur peut faire l'objet d'une programmation au moyen d'algorithmes ;
- dont les échanges peuvent être régulés en fonction de la volatilité, de la vitesse, de la durée, du réseau, de la législation, de l'utilisation ;
- dont les caractéristiques fonctionnelles permettent de l'utiliser comme outil de vote…

De ces quelques fonctionnalités nouvelles, comme de toutes celles qui composeront le futur logiciel monétaire du monde, résultera un nouveau méga-marché dans lequel disparaîtront les distinctions classiques existant entre financement, opérations monétaires et actifs technologiques.

L'émission de jeton dans le cadre des Initial Coin Offerings (ICO)

Les *Initial Coin Offerings* (ICO) peuvent, selon l'AMF, être définis comme des opérations de levées de fond effectuées à travers une technologie de registre distribué ou blockchain. Ces opérations donnent lieu à une émission de jetons pouvant être ensuite, selon les cas, utilisés pour obtenir des produits ou services, échangés sur une plateforme (marché secondaire) et/ou pouvant rapporter un profit.

Cette nouvelle forme de financement, qui ressemble par certains aspects aux canaux de financement plus traditionnels (offre publique, capital-risque, *crowdfunding*), présente toutefois des caractéristiques propres, bénéficiant par exemple des effets de réseau et de la liquidité potentielle issue d'une possible cotation du jeton sur un marché secondaire.

En conséquence, ce caractère hybride des jetons le rend difficile à qualifier juridiquement. Au niveau mondial, ce mode de financement demeure encore marginal, représentant au total 22,2 milliards de dollars de levées de fonds par émission de jetons, principalement en 2017 et durant les trois premiers trimestres 2018 (respectivement 6,8 et 15,2 milliards de dollars).

Il existe actuellement dans le monde environ 2100[67] crypto-actifs différents pour un montant total d'environ 250 milliards de dollars. Les principaux sont le bitcoin avec 42 % des volumes de transactions, suivi de l'ether, 18 %, puis du ripple, 7 %.

Plusieurs types de jetons existent également, aux caractéristiques et usages différents. Les plus fréquents sont les **jetons d'usage** (*utility tokens*) aux multiples applications : droit d'usage d'un bien ou service, droit d'accès, moyen de paiement, unité de valeur d'échange au sein d'une application ou d'un écosystème donné… Commencent à apparaitre des jetons assimilés à des valeurs mobilières donnant droit à un revenu ou à une portion d'un actif matériel ou immatériel : les **jetons d'investissement** (*security tokens*). En 2019, les émissions de ce type de jeton devraient se développer. Plusieurs projets de tokenisation d'actifs immobiliers ou d'œuvres d'art sont à l'étude.

67. www.coinmarketcap.com du 19 janvier 2019.

Création et levée de fonds en crypto-monnaies	Échange de crypto-monnaies	Conservation de crypto-monnaies
• Mineurs rémunérés en crypto-monnaies nouvellement créées ; • Start-ups ou jeunes entreprises innovantes levant des fonds en crypto-monnaies contre *tokens* par *Initial Coin Offering (ICO)*.	• Intermédiaires (mise en relation sans risque de contrepartie - *dealers* ; • Plateformes d'échange (détention ou contrôle de fonds avec risque de contrepartie - *brokers*) ; • Distributeurs physiques de crypto-monnaies (ATM).	• *Cold wallet* ou *hardware wallet* : appareil électronique physique de stockage, sur le modèle d'un coffre-fort physique ; • Hot wallet : portefeuilles fonctionnant sur des appareils (smartphone, ordinateur ou tablette) connectés à Internet.

Source : rapport Landau, juillet 2018

Le tableau ci-dessus montre la chaîne de la valeur des acteurs de la cryto-finance.

Les acteurs de cette technologie sont les mineurs, les plateformes d'échange, les conservateurs (*wallets providers*) et les fournisseurs de services d'information financière, de conseil en investissement, de trading…

Toutefois, plusieurs risques entourent cette nouvelle crypto-finance que nous résumons dans les points suivants :

- Escroqueries subies par les épargnants : les fraudes se font à partir de sites Internet inspirant confiance mais illégaux. Ceux-ci demandent aux particuliers d'envoyer leurs fonds sur des comptes bancaires à l'étranger pour investir en bitcoin ;
- Fraudes subis par les investisseurs ICO qui subissent la perte de leurs investissements (ex. : les porteurs du projet de l'ICO vietnamienne Pincoin se sont volatilisés emportant avec eux les 600 millions dollars investis). De plus, l'origine des fonds investissant dans les ICO est souvent douteuse et s'apparente à du blanchiment d'argent ou à de l'évasion fiscale, favorisés par l'anonymat des investisseurs. Les quatre principaux pays en termes de montants levés sont la Russie, Singapour, la Chine et Hong Kong ;
- Incidents survenus sur les plateformes d'échanges : un grand nombre d'incidents est survenu sur les plateformes d'échange de crypto-actifs, qu'il s'agisse de falsification de clés privées, d'introduction de logiciels malveillants ou de faille de sécurité des serveurs.

Les évolutions récentes

Début 2018, le rythme des projets basés sur la blockchain ne semble pas ralentir et la régulation du marché par les autorités politiques et financières se met progressivement en place, tant pour l'usage des DLT et des ICO que pour les usages des crypto-actifs. Sur le plan technique, des architectures très variées, dérivées des modèles initiaux de blockchains, sont imaginées pour satisfaire des contraintes propres à des marchés précis.

Les propositions d'usages sont plus matures et se concentrent sur un portefeuille d'applications demandant la coordination d'un ensemble d'acteurs autour d'un processus commun, avec déjà des premières mises en production de prototypes testés en 2017.

Depuis la fin de l'été 2018, la chute des cours des crypto-actifs a entraîné la chute du nombre des ICO et l'échec de nombreuses levées de fonds. Les investisseurs cherchent aujourd'hui à sécuriser leurs investissements et s'intéressent particulièrement aux *security tokens* as-

similés à des valeurs mobilières, au détriment des ICO organisant l'émission de jetons ne pouvant pas être qualifiés d'instrument financier comme les *utility tokens*.

2019 verra l'émergence des STO (*Security Token Offerings*). Il s'agira d'émissions réalisées par des sociétés existantes, cotées ou non, qui émettront des tokens indexés sur des actifs matériels ou immatériels de la société ou donneront droit à une part de capital ou des revenus. Plusieurs sociétés du CAC 40 ont de tels projets à l'étude. Les STO allient les avantages de souplesse et rapidité des ICO tout en apportant une meilleure sécurité à l'investisseur, car le token offert, assimilé à une valeur mobilière, rentre dans une réglementation bien connue.

Le livre blanc a identifié plusieurs DIP qui permettront de développer la crypto-économie et de protéger ses utilisateurs...

DIP 19 : favoriser la recherche sur la crypto-économie

Les projets de recherche peuvent s'organiser autour de quatre thématiques :

La cryptographie

Elle a un quadruple usage dans les architectures de blockchain :

- Assurer les propriétés fondamentales du registre comme l'immuabilité, l'ordonnancement des blocs et l'identification des intervenants ;
- Apporter une partie de la solidité du consensus dans le cas de la preuve de travail ;
- Garantir la confidentialité sur tout ou partie des données inscrites dans le registre ;
- Fournir des fonctions supplémentaires autour du registre.

Les algorithmes de cryptographie inclus dans la plupart des blockchains actuellement proposées sur le marché depuis les années 1970 peuvent/doivent être constamment améliorés pour continuer à assurer les fonctions demandées par les blockchains tout en prenant en considération l'amélioration de la puissance des calculateurs (loi de Moore) pouvant servir à la cryptanalyse. Une fois utilisé, tout algorithme de cryptographie donne lieu à des études de cryptanalyse pour en détecter les limites. En parallèle, la puissance des calculateurs continue à croître au rythme de la loi de Moore. Les algorithmes se trouvent ainsi remis en cause régulièrement comme dernièrement SHA1[68]. L'emploi de blockchain dans des contextes financiers demandant une haute sécurité repose essentiellement sur les caractéristiques du cryptage mis en œuvre.

Par ailleurs, l'avènement annoncé de calculateurs quantiques particulièrement adaptés à certains calculs intervenant en cryptologie peut brutalement remettre en cause les caractéristiques de ces algorithmes comme le chiffrage asymétrique au cœur de l'identité des intervenants dans une blockchain. Des solutions de cryptographie quantique sont en cours d'élaboration, mais leurs applications aux blocs antérieures restent à définir.

En parallèle, l'adjonction d'algorithmes, par exemple les preuves à divulgation nulle de connaissance (i.e. *Zero Knowledge Proof*), a considérablement amélioré les fonctionnalités des blockchains en ouvrant des possibilités de contrôle des transactions tout en assurant la confidentialité des données. De nouveaux apports fonctionnels peuvent être offerts par d'autres classes d'algorithmes de cryptographie qu'il faudra redécouvrir et adapter au contexte des blockchains employées dans les fintechs.En parallèle, la simplification des algorithmes actuels de cryptographie peut être réalisée par les chercheurs, la recherche de mise en œuvre efficace pouvant améliorer, à coûts identiques, certains paramètres des blockchains (latence, capacité maximale, etc.).

Le consensus

La notion de **consensus** est au centre

68. SHA-1 (Secure Hash Algorithm) est une fonction de hachage cryptographique conçue par la National Security Agency des États-Unis (NSA) et publiée par le gouvernement des États-Unis comme un standard fédéral de traitement de l'information (Federal Information Processing Standard du National Institute of Standards and Technology (NIST)) en 1993. Elle produit un résultat (appelé « hash » ou condensat) de 160 bits. Cette fonction a évolué depuis en SHA-2, 3.

de la décentralisation des blockchains. Il doit à la fois garantir l'égalité des parties prenantes tout en assurant l'unicité des ajouts au registre. Le consensus résulte le plus souvent d'une complémentarité entre un algorithme fixé dans le logiciel et des règles implicites ou explicites de gouvernance entre les acteurs de la blockchain.

Des exemples opérationnels sont donnés par les chaînes publiques qui résistent depuis maintenant plusieurs années, mais des limites apparaissent dans la sécurité de notion de consensus distribué. Par exemple, la couche réseau pair à pair apparaît comme particulièrement fragile et les règles implicites des chaînes publiques demanderaient à être formalisées pour en apprécier les conditions de pérennité et leurs limites.

L'utilisation de blockchains en consortiums très larges doit encore faire preuve de sa résistance aux attaques qui ne manqueront pas d'intervenir au fur et à mesure des mises en œuvre dans des secteurs stratégiques. La mise en œuvre de blockchain de consortium impose donc un pilotage de ces architectures pour en détecter le plus tôt possible les risques, les fragilités et les attaques.

Le sujet doit être abordé dans le domaine de l'économétrie appliquée aux relations au sein des groupes d'acteurs autour d'une même blockchain et selon une approche plus classique sur les systèmes informatiques distribués.

Des smart contracts aux langages de modélisation des contrats et des processus

En 2014, Vitalik Buterin appliqua la notion de ***smart contract*** **(fonctions auto-exécutantes)** à une blockchain en lançant Ethereum. Plusieurs utilisateurs se sont emparés du concept en proposant des applications concrètes qui montrent tout le potentiel de ces programmes capables de traitements sur le registre avec les mêmes caractéristiques : traitements distribués pour des logiciels archivés de façon immuable dans le registre avec une confiance distribuée assurée par l'ensemble des parties prenantes.

Ces *smarts contracts* ne sont littéralement ni « smart » ni des contrats à proprement parler, mais restent une technologie prometteuse. Leur histoire récente a montré des limites avec des accidents aux conséquences chiffrées en millions de dollars : le code logiciel étant immuable, la moindre erreur ou divergence entre les spécifications et la réalisation présente des impacts majeurs sur l'évolution du contenu du registre. Ce risque limite aujourd'hui un large usage de ces outils dans des applications réelles pourtant porteuses de productivité, de qualité et de nouveaux services dans des environnements opérationnels répartis entre plusieurs entités. Les blockchains de consortiums doivent apporter des niveaux de sécurité, de puissance de traitement satisfaisants et aux caractéristiques démontrables dans ces environnements distribués sans devoir réaliser et attendre des tests exhaustifs qui prendraient plusieurs années.

Des outils de simulation, de vérification et de preuve formelle des logiciels employés dans les *smart contracts* doivent être développés et expérimentés en tirant profit des centres de recherche français et de leur écosystème aux compétences reconnues au niveau mondial. Ces outils passeront par la création ou l'amélioration des langages spécifiques (langage contrôlé ou *« domain specific language »*) autorisant ainsi vérification et preuve formelle. Les étapes suivantes passeront par la spéci-

fication et le développement de langage de modélisation couvrant des concepts d'open workflow et de modélisation de contrats (ex. : DAML, voir DIP 25).

Cela permettra une approche plus aisée pour les opérationnels et les fonctions support (juridique, contrôle interne, conformité et régulateur). Le workflow des processus est défini pour ce langage avec devoirs et obligations de l'ensemble des parties participantes à l'ensemble de la chaîne. L'inscription des transactions et des événements sera enregistrée dans le GDL (*Global Synchronization Layer*) de la chaîne utilisée.

De nouvelles architectures

L'approche globale pour une blockchain de consortium peut s'appuyer sur une architecture plus variée que les réalisations en chaînes publiques, à la fois par une nécessaire intégration dans les systèmes d'information des parties prenantes et par des choix différents en matière de compromis entre sécurité, distribution décentralisée, passage à l'échelle et latence.

Le compromis choisi privilégiant la stabilité de la chaîne Bitcoin et la sécurité des échanges par rapport aux possibilités de puissance de traitement des transactions peuvent être finement adaptés de certains cas d'usage interne à un groupe de parties prenantes. Par ailleurs, plusieurs blockchains coopéreront nécessairement dans une même entreprise pour construire des services plus complexes que les mises en œuvre publiques.

Des solutions pour l'interconnexion et l'interopérabilité de plusieurs blockchains entre elles doivent pouvoir émerger puis être validées et testées. Le bloc séquentiel n'est pas la seule solution de représentation du registre et des solutions de graphes acycliques, palliant certaines faiblesses des premières architectures, sont proposées : ces chaînes basées sur des graphes acycliques affichent des puissances au-delà du millier de transactions par seconde. D'autres structures peuvent émerger, associées à des caractéristiques nouvelles et largement plus performantes que celles de blockchains initiales.

Recommandations

Un programme de formation et de vulgarisation

Un programme de formation et information pourra être lancé par le Pôle FINANCE INNOVATION et des laboratoires de l'INRIA, l'université PSL et les universités de Saclay sur des sujets comme les fonctions de base de cryptographie, l'informatique distribuée et la crypto-économie. Les laboratoires français d'informatique, de cryptographie et d'économie sont parfaitement au niveau pour offrir des savoir-faire qui permettront d'apporter des fonctions nouvelles aux fintechs sous réserve de la création de liens avec les industriels et institutions du secteur et une coopération effective autour de projets concrets.

Des programmes de recherche croisant les compétences

L'innovation viendra de la mise en contact et de la confrontation des porteurs de cas d'usages précis en fintech avec les pôles de recherche en cryptologie, en informatique distribuée et en économétrie de l'INRIA, de PSL, de la TSE et X sur la base d'un programme de recherche construit sur les éléments cités au paragraphe précédent.

Le croisement des compétences est impératif pour le succès de ces programmes. Cela implique de disposer des compé-

tences nécessaires pour chacun des maillons de la chaîne de valeur qui utilise la blockchain et donc de fournir un effort important de formation dans tous les domaines de cette technologie, de la modélisation au codage, du contrôle et des tests au pilotage de la mise en application opérationnelle, du juridique à la conformité.

Par ailleurs, le besoin en compétences est varié. De nombreux enseignements de la blockchain ont été mis en place (X, PSL Mines, CNAM, universités de la Sorbonne et de Clermont-Ferrand, Eureka, ESGI, etc.), mais restent peu connus et devraient faire l'objet d'une promotion plus active, voire d'une « certification ». Universités, grandes écoles, lycées technologiques, organismes de formation professionnelle et internes aux entreprises, SSII et OPCA doivent être mobilisés et former dès à présent les enseignants et experts de demain afin que la France soit aux avant-postes des technologies digitales, dont la blockchain, notamment dans le domaine financier.

Un recensement/prévision des métiers émergents de la blockchain est amorcé et doit fournir les grandes lignes nécessaires des spécialisations à venir :

- Métiers techniques : développeurs blockchain et *smart contract*, ingénieurs des systèmes distribués, experts en cryptographie et sécurité réseaux décentralisés, designers de solutions blockchain ;
- Métiers de la finance : analystes crypto-actifs et ICO, gérants de fonds en crypto-actifs, traders sur des plateformes d'échanges crypto, métiers de conservation des crypto-actifs ;
- Métiers juridiques : experts juridiques en technologie ;
- Métiers de la conformité : chargé de la conformité blockchain, auditeur blockchain.

DIP 20 : développer les ICO (Initial Coin Offering) en protégeant l'investisseur

Les principes qui véhiculent les ICO

En l'absence de réglementation sur le sujet (et dans l'attente du vote définitif de la loi PACTE, voir partie 4 relative aux enjeux réglementaires), les ICO sont aujourd'hui guidées par l'application de bonnes pratiques créées par les utilisateurs et porteurs de projets, empruntant à ce qui se fait plus classiquement en matière d'émission d'instruments financiers ou dans le cadre d'IPO (*Initial Public Offering*, soit l'introduction en bourse). La plupart de ces bonnes pratiques sont reprises par l'AMF qui modifiera son règlement général et qui publiera une instruction permettant de détailler la nature et les modalités de l'organisation et de la structuration d'une ICO afin qu'elle puisse recevoir son visa[69].

L'objectif reste de fournir un maximum d'informations aux souscripteurs de jetons afin que, dans cet univers marqué par des incertitudes tant juridiques que réglementaires, ils puissent investir en toute connaissance de cause de leurs droits, de leurs obligations et des risques liés. L'objectif est également de sécuriser, autant que possible, la collecte, l'utilisation et la conservation des crypto-monnaies par les émetteurs ainsi que l'émission des jetons attribués aux investisseurs.

Enjeux

- La nécessaire prudence des banques en matière d'ouverture et de fonctionnement de compte de sociétés ayant réalisé une ICO ne permet pas pour le moment la normalisation de ces dernières. Certaines ICO ont pu présenter à ce jour les aspects d'un effet de « bulle », aussi est-il nécessaire de bien distinguer les levées de fonds des tentatives de détournement qui ont été constatées ;
- €Les bonnes pratiques applicables dans le cadre d'une ICO devront être affinées et précisées pour supprimer le déficit d'information actuel que subissent les investisseurs, notamment dans les domaines suivants : modalités de souscription des jetons, règles de conversion des crypto-monnaies et d'attribution des jetons, modalités de séquestre et de restitution des crypto-monnaies le cas échéant, gouvernance post-ICO, gestions de la liquidité et de la volatilité des jetons et du marché secondaire ;
- L'absence de maturité des acteurs et des techniques utilisées dans le cadre de la réalisation des ICO et la multiplication des projets ne facilitent pas l'adoption et la normalisation de ce type de financement malgré son succès. Une moralisation des acteurs est nécessaire. Les acteurs impliqués dans le cadre d'une ICO doivent pouvoir être évalués, notés et contrôlés. Les fraudes doivent être détectées plus facilement et les fraudeurs identifiés et découragés.

Recommandations

- La normalisation des relations entre les banques et les émetteurs réalisant

69. Pour aller plus loin, voir partie 4 « Enjeux réglementaires ».

une ICO passe par la satisfaction des obligations de connaissance client (en anglais, KYC « *Know Your Customer* ») et des procédures de LCB-FT (lutte contre le blanchiment des capitaux et le financement du terrorisme). Cela peut être réalisé par une normalisation des procédures KYC et LCB-FT réalisées dans le cadre des ICO et une clarification de l'information adressée par les places de marchés aux banques lorsque des crypto-actifs convertis en monnaie scripturales sont virés par ces places de marché sur les comptes des émetteurs : mise en place de procédures de connaissance client (KYC) basées sur un reporting unifié (émetteur/échange/banque) imposant aux places de marché (ou aux prestataires de services de paiement avec lesquelles elles ont signé des accords de coopération) de communiquer l'information adaptée aux contraintes réglementaires de connaissance client et de LCB-FT. Cette normalisation passe également par la nécessité de procéder à l'identification des origines des fonds dans le cadre d'une ICO, trop rarement réalisée ;

- Dans un souci de normalisation du fonctionnement des ICO, il revient au régulateur de préciser et d'imposer aux émetteurs l'adoption de techniques spécifiques aux particularités des jetons permettant la gestion de leur liquidité, de leur volatilité et de leur évaluation. Il convient également de préciser les mécanismes de séquestre, de conversion, de restitution et d'utilisation des réserves ainsi que des modalités de réalisation d'audit post-ICO permettant la constatation de la réalisation de milestones assurant le déblocage des crypto-monnaies collectées dans le cadre de l'ICO.

Enfin, la moralisation des acteurs intervenant dans le cadre d'une ICO peut être encouragée par :

- l'obtention d'un agrément du régulateur ou d'associations professionnelles représentatives sur la base d'une évaluation et du respect d'un certain nombre de conditions d'honorabilité et d'expérience ;
- pour d'autres, l'adoption d'une charte de bonnes conduites ;
- en tout état de cause, par l'identification, la classification des fraudeurs et la sanction des agréés qui contreviendraient à leurs obligations, comme il est aujourd'hui envisagé dans le projet de loi PACTE.

Recommandations à court terme

- Normaliser les relations bancaires avec les mises en place de procédures et de méthodes permettant de gérer la liquidité des jetons via des accords avec des teneurs de marchés (*market makers*) et apporteurs de liquidité en lien avec les places de marché ;
- Caractériser l'utilité, les conditions et les modes d'utilisation des réserves de jetons (transparence) ;
- Préciser les mécanismes de conversion monnaies nationales/crypto-actifs/jetons assurant une actualisation des cours plutôt que la prise en compte d'un cours moyen crypto/euro ou bitcoin/euro ou d'un cours fixé à l'avance ;
- Officialiser et démocratiser des mécanismes de fonctionnement des « *stablecoins* », c'est-à-dire un jeton adossé à un actif sous-jacent (par exemple une monnaie fiat) et permettant de limiter la volatilité des jetons ;
- Mettre en place de mécanismes de suspension des échanges dans le cas d'une trop forte volatilité des jetons.

Recommandations à plus long terme

- Mettre en place une méthode et une procédure de rating des jetons par des agences d'évaluation certifiées, obéissant à des cahiers des charges précis et obéissant à des règles strictes de gestion de conflits d'intérêts ;
- Instaurer l'équivalent d'un fichier FIBEN (Fichier Bancaire des Entreprises) pour noter les émetteurs ayant initié des ICO. En parallèle, officialisation par l'AMF d'une liste noire ou « *scams* » ;
- Créer une certification des prestataires de services proposant des audits post-ICO incluant un cahier des charges des modalités de périodicité et de déroulement de l'audit ainsi que le contenu du reporting et des modalités de publication (charte audit post-ICO) ;
- Développer la moralisation des conseillers et des ambassadeurs (sur la base de ce qui a été fait pour les apporteurs d'affaires en matière de gestion d'actifs) via l'édiction d'un code de bonne conduite.

Focus
Les principes de valorisation des ICO

Depuis le lancement des ventes de jetons ou d'opérations d'ICO ces dernières années, l'idée de mettre au point des méthodes d'évaluation permettant de déterminer avec précision le prix futur d'un jeton est devenue un sujet d'intérêt et de débat croissant. Des experts tentent de créer des modèles précis de prévision des prix des jetons et se heurtent à de multiples problématiques :

- Tout d'abord, l'analyse empirique manque en effet cruellement et créer un modèle de prédiction, quel qu'il soit, exige des preuves empiriques rigoureuses. La plupart des ICO financées sont encore en cours d'élaboration. Comme certains de ces projets ne seront publiés qu'en 2019 ou 2020, l'évaluation actuelle repose sur un grand nombre d'hypothèses (pénétration du marché, courbes d'adoption par les clients…) ;
- €Deuxièmement, la plupart des modèles d'évaluation actuellement à l'étude (et utilisés) sont essentiellement des versions réajustées de modèles d'évaluation de titres financiers. Or, les jetons ne présentent pas les mêmes caractéristiques et, de plus, sont tous différents ;
- Troisièmement, les jetons ont des propriétés monétaires et des objectifs fonctionnels, ce qui constitue une valeur économique intrinsèque. Chaque projet utilisant des jetons fonde sa communauté ayant ses propres attributs d'approvisionnement en devises et sa vitesse de circulation qui souvent ne sont pas pris en compte dans la construction des modèles d'évaluation ni même clairement abordés dans le *white paper* des projets.

Méthodologie modulaire d'évaluation des tokens

Compte tenu des problèmes énumérés ci-dessus, la communauté blockchain doit reconnaître la nécessité d'un nouveau modèle d'évaluation pour ce véhicule d'investissement émergent. Une telle méthodologie nécessite un cadre établi avec ses propres définitions et de déterminer au préalable les variables du modèle.

Des chercheurs de BNP Paribas et de la CDC Recherche (Caisse des Dépôts et Consignations) ont développé une nouvelle méthodologie de valorisation des jetons. Ils ont abordé la question de l'analyse des caractéristiques techniques des ICO en se concentrant sur les *smart contracts* qui, en constituant le modèle de gouvernance de l'ICO, ont un impact direct sur l'offre et donc le prix des jetons. La démarche s'inspire de celle de Benjamin Graham[70] qui a permis de séparer la valeur intrinsèque d'une action de sa valeur spéculative.

Le rapport « *Cryptoasset valuation : identifying the variables of analysis* » détaille donc les variables techniques à prendre en compte lors de l'analyse d'un livre blanc (*white paper*) de l'ICO par les investisseurs et détaillant les limites des smart contracts. À l'aide des données fournies par ChainSecurity et Stratumn, une liste

70. Benjamin Graham est l'auteur du livre « Security Analysis » et « The Intelligent Investor » est souvent considéré comme le père de l'investissement intelligent.

de variables techniques est fournie afin de construire un modèle d'évaluation respectant la granularité de l'écosystème, laquelle comprend :

- attributs de base du codebase (langue et version) ;
- système de gestion d'identité pour la vente des tokens ;
- facteurs d'échelle ;
- conformité aux normes ERC20 ;
- présence de conditions négligées ;
- utilisation de modificateurs ;
- limites des fonctions ;
- valeurs de rétribution des fonctions ;
- débits excédentaires et insuffisants ;
- réentrée et réorganisation des attaques ;
- variables liées à GITHUB/Etherscan, etc.

Cette liste de variables techniques pourrait être utilisée pour construire des modèles d'évaluation symbolique adaptés au contexte, examinant et comparant les méthodes d'évaluation actuelles.

En revanche, le rapport ne fournit pas de modèle d'évaluation et s'attache plutôt à ce qui doit être privilégié pour commencer à créer les éléments constitutifs des modèles d'évaluation des jetons.

La deuxième partie du rapport se concentre sur l'identification des variables monétaires nécessaires à l'élaboration d'une méthodologie de valorisation des jetons.

L'ultime objectif est de déterminer les variables utiles à l'évaluation des jetons est de créer une Méthodologie Modulaire d'Évaluation. Comme les jetons sont très différents selon le type de service fourni, un modèle d'évaluation « taille unique » n'est pas réaliste. Un modèle d'évaluation modulaire accompagné d'une liste exhaustive de variables est donc à privilégier en choisissant les plus adaptées au respect des spécifications des jetons. Ce n'est qu'en obtenant de tels paramètres et en construisant une boîte à outils de variables qu'il sera possible d'établir une taxonomie standard et d'aider les investisseurs dans leurs décisions de placement.

L'absence d'un cadre structurel permettant aux investisseurs de déterminer la pertinence d'un investissement a favorisé la baisse de confiance dans les ventes de jetons qui ont diminué. Aujourd'hui, la plupart des investissements dans des ICO sont devenus des accords d'agrément et le financement du capital-risque gagne rapidement du terrain. En octobre 2018, le financement des ICO et du capital-risque traditionnel était pour chacun de 600 millions de dollars. Pour remédier à cette situation et permettre aux ICO d'agir comme le nouveau véhicule d'investissement qu'elles sont, un nouveau cadre d'évaluation doit être créé, testé et développé et auquel la communauté crypto doit avoir accès.

DIP 21 : sécuriser les portefeuilles numériques et adapter les fonctionnalités de conservation des crypto-actifs

Une des problématiques fondamentales sur le marché des crypto-actifs aujourd'hui concerne la notion de conservateur, c'est-à-dire la possibilité pour une entreprise de sécuriser des crypto-actifs (via la conservation des clés privées) au nom de ses clients. Comment les portefeuilles de crypto-actifs peuvent-ils répondre à ces besoins ? Quels sont les enjeux en termes de régulation à considérer ?

Enjeux

Les enjeux sont les suivants :

Sécurité du portefeuille
La sécurité du portefeuille en crypto-actifs est essentielle : si une entreprise qui conserve des fonds pour le compte de ses clients est la cible d'une action malveillante, les fonds peuvent être perdus.

Audit de l'entreprise
Une entreprise qui se voit confier des fonds doit, à tout moment, pouvoir être auditée par une autorité régulatrice vérifiant le stock et la propriété des crypto-actifs qu'elle conserve.

Retrait des fonds
Un tel mécanisme de conservation doit pouvoir garantir que les clients peuvent récupérer leurs fonds dans des limites de temps raisonnables.

Recommandations

Sécurité du portefeuille
Notre première recommandation est l'utilisation d'un portefeuille le plus sécurisé possible. On citera ici deux possibilités :

- la première est l'utilisation d'un portefeuille hors ligne « *cold wallet* » qui n'est pas accessible en ligne à tout moment. Il peut s'agir ainsi d'un portefeuille stocké sur une clé USB conservée dans un coffre et qui n'en est sortie que lorsqu'une transaction doit être effectuée. Cette solution a comme désavantages que le portefeuille n'est pas immédiatement disponible pour effectuer la transaction et qu'il peut être mis en défaut si la clé USB est connectée à un ordinateur infecté.
- La deuxième possibilité est l'utilisation d'un portefeuille sécurisé physique. On pourra citer notamment les solutions de l'entreprise française Ledger, notamment le Ledger Nano S ou le Ledger Vault.
- Une couche de sécurité additionnelle qu'il faut considérer est la possibilité de créer des portefeuilles multi-signatures. Dans ce cas, pour envoyer les fonds, le conservateur doit signer une transaction avec son portefeuille et le client avec le sien. Cette solution est la meilleure en termes de sécurité, dans la mesure où le conservateur ne peut en aucun cas s'accaparer les crypto-actifs sous sa garde. Cette solution présente deux désavantages : si l'un des deux portefeuilles est perdu, les fonds sont à jamais inaccessibles et la nécessité de demander deux signatures pour chaque transaction implique un délai supplémentaire.

Audit de l'entreprise

- En matière d'audit, il est souhaitable que la réglementation puisse imposer la mise en place de pistes d'audit permettant à l'établissement conservateur de démontrer à tout moment qu'il dispose bien des crypto-actifs qui lui ont été confiés et qu'il est en mesure d'établir la correspondance entre chaque portefeuille de crypto-actif géré et le client à qui il appartient (le titulaire du portefeuille).
- Dans ce cadre-là, il peut être envisagé de créer une licence ou un agrément de « dépositaire » de crypto-actifs, permettant de fournir au public une liste des établissements et prestataires de services qui respectent des standards de sécurité et de fiabilité et sont soumis à la réglementation française (voire européenne).

3.4 ÉCOSYSTÈME ET PLATFORMES EN PLACE

DIP 22 : identifier et décliner les bonnes pratiques de consortia pour développer des solutions de place

L'étude des différents cas d'usage montre que les initiatives individuelles n'ont pas de valeur ajoutée significative pour les entreprises et que les initiatives de place sont plus prometteuses. Une blockchain de consortium est contrôlée par un ensemble de nœuds présélectionnés représentant des acteurs ayant un intérêt à collaborer ensemble sur une même chaine de valeur.

Il existe plusieurs initiatives de consortia de blockchains, la plus connue étant le projet R3 (Corda). Néanmoins, elles sont confrontées à plusieurs difficultés :

- **Stratégiques :** rassembler autour d'un même projet informatique plusieurs entreprises parfois concurrentes, ayant des agendas et des processus différents, constitue un véritable enjeu. Intervient de plus un retour sur investissement (ROI) pas toujours justifié par rapport au système centralisé qui fonctionne déjà et non encore amorti ;
- **Techniques :** la technologie open source, pas toujours mature, ne garantit pas la scalabilité et la confidentialité des données.

L'objectif de ce DIP est d'identifier les bonnes pratiques pour réussir un projet de place au sein d'un consortium. Cela passe par l'expérimentation d'un cas d'usage sous forme de *Proof Of Concept*. Une fois validé, on peut envisager son passage à l'échelle et son industrialisation.

Expérimenter le cas d'usage sous forme d'un proof-of-concept

Avec le lancement de POC (*Proof Of Concept*), de MVP (*Minimum Viable Product*) ou encore d'applications pilotes, l'enjeu est **d'identifier les besoins métiers** auxquels le projet blockchain doit répondre. Un cas d'usage simple, adapté à une architecture distribuée sur un périmètre restreint et à coût limité afin de s'approprier la technologie, permet de tester la faisabilité technique et de valider les choix architecturaux. La validation du PoC permet parfois de convaincre des sponsors ou partenaires de rejoindre le projet. Après avoir validé le besoin métier, il faut le traduire en spécifications et formaliser la proposition de valeur qui passe par le calcul du ROI.

Le principe d'un consortium nécessite de réunir plusieurs participants, une dizaine au moins pour le démarrage. L'un des facteurs déterminants de succès est le partage d'intérêts et d'objectifs communs avec une feuille de route allant jusqu'à la phase d'industrialisation.

Cela implique de déterminer les règles de gouvernance en répondant à quelques questions (quels enjeux de confidentialité, droits de lecture ou d'écritures, besoin d'une base de données cryptée… ?) afin de permettre de sélectionner la blockchain la plus appropriée et d'éviter les changements de cap ou les malentendus en cours de route. Il est enfin essentiel d'allouer les ressources matérielles et

humaines nécessaires, à commencer par les compétences. La maîtrise de la technologie blockchain est indispensable pour réussir cette première phase de PoC dans de bonnes conditions : développeurs, architectes de solutions distribuées, experts en cybersécurité des blockchains et des *smart contracts*. Cela passe par le recrutement, la formation ou le partenariat avec des spécialistes (startups, consultants expérimentés).

Du PoC à l'industrialisation

Plusieurs projets sont restés à l'étape du PoC du fait de nombreux freins, notamment juridiques, techniques et de gouvernance, cette dernière devant être réglée avec le consortium.

La recommandation est de créer une **structure ad hoc** pour la mise à l'échelle du PoC en définissant les caractéristiques dans le tableau ci-dessous.

La forme juridique

La forme juridique importe peu, mais les acteurs doivent définir le cadre contractuel de cette structure :

- Le statut juridique de la structure.
- Les acteurs, leur rôle et leurs responsabilités.
- L'évolution future de la structure.
- Le processus d'intégration des nouveaux membres non fondateurs.
- Les droits de la propriété intellectuelle.
- Les modalités de financement de la structure : coûts de développement, d'implémentation, de fonctionnement et de maintenance.
- Le modèle économique pour l'accès à la blockchain et le mode de rétribution de chacun (tarification à la transaction, abonnement annuel etc.).
- Vérifier la conformité à la réglementation en vigueur ou à venir. Pour les cas d'usage B2C qui impliquent la relation avec le client, Il y a des contraintes supplémentaires sur le traitement des données personnelles et la protection du consommateur.
- Si besoin obtenir dès la phase d'expérimentation l'accord ou la labélisation des autorités de régulation (Banque de France, AMF, ACPR, CNIL…).

Interfaçage et interopérabilité

- Prévoir l'intégration dans les systèmes d'information de chacun des acteurs du consortium.
- L'interfaçage permet de collecter des informations à travers des API, applications mobiles, capteurs connectés ou portails web.
- Prévoir les possibilités d'interopérabilité entre blockchain (il n'y aura pas une seule blockchain universelle).

Choix de la blockchain et implémentation

Le choix publique vs. privée ?

- Vérifier que les choix technologiques du prototype sont toujours valides et les adapter au besoin.
- S'assurer que la blockchain choisie est mature avec une communauté installée, notamment pour le cas des blockchains open source (le dynamisme et la réactivé d'une communauté peut être déterminante) afin d'apporter la confiance nécessaire sur la pérennité de la solution.
- Mise en place de procédures de tests robustes pour assurer la cybersécurité des programmes développés (notamment pour les *smart contracts*).
- Disposer d'une veille technologique et d'un benchmark partagé et régulièrement mis à jour des principales solutions (Corda, Ethereum, Hyperledger…).
- Faciliter l'usage pour le client final en particulier sur les modalités d'accès et la gestion des clés.
- Anticiper l'intégration informatique de la plateforme au sein des DSI des acteurs : sociétés de gestion, investisseurs, distributeurs, dépositaires, administrateurs de fonds…
- Favoriser une démarche projet itérative et agile en pour l'implémentation.
- Adopter un standard de données existant (ACORD[70] dans B3i par exemple).

Données et confidentialité

- Déterminer les droits de lecture ou d'écriture.
- La réglementation en vigueur et certains prérequis métier peuvent parfois présenter d'importantes limites sur ces sujets mais il existe aujourd'hui des solutions qui permettent de lever partiellement ou complètement ces contraintes comme les empreintes numériques ou les *zero-knowledge-proofs* qui conservent de façon confidentielle certaines données inscrites sur une blockchain publique.

Gouvernance

Dans le cadre du consortium, le partenaire technologique qui représente la structure ad hoc aide à la définition et à l'application des règles de gouvernance.

- Définir les acteurs de cette structure ad hoc. Il est important que les acteurs qui ont réalisé le prototype restent impliqués dans la création de la structure afin de garder une continuité et capitaliser sur l'expérience acquise.
- Définir les rôles des acteurs et les modalités d'échange des flux financiers et de données.
- Définir les droits d'accès, de lecture et d'écriture.
- Définir les modalités de partage des coûts d'implémentation et de la gestion du changement entre les participants au consortium (coût de mise en production du prototype ; coût d'intégration dans chacun des systèmes d'information des participants ; coût de formation et de montée en compétence sur la technologie des équipes, coûts d'expérimentation liés au manque de connaissance et de recul sur la technologie).

Il est recommandé d'intégrer les acteurs au fur et à mesure et non simultanément.

Capacité transactionnelle, scalabilité et services associés

- Les volumes de transactions à traiter par seconde et la capacité d'une blockchain à accueillir de nouveaux participants peuvent fortement varier d'une solution à l'autre et doivent être étudiés dès la phase de conception.
- Il est également important d'envisager les différents services associés pour garantir le bon fonctionnement du réseau, par exemple le back-up des clés privées des utilisateurs ou des outils de rapport et d'audit pour l'utilisation des données.

71. www.acord.org/standards-architecture/acord-data-standards.

Autres points critiques

Disposer des compétences nécessaires

- Monter en compétence sur les technologies (acculturation, évangélisation). La blockchain est une technologie relativement nouvelle en perpétuelle évolution et il est primordial de s'informer constamment sur les évolutions technologiques et législatives ;
- Identifier des talents techniques et les accompagner dans l'expertise ;
- Constituer une équipe pluridisciplinaire : il est essentiel de combiner les expertises métiers, technologiques, juridiques et managériales ;
- Collaborer avec des organismes publics (BPI…) ou professionnels (FBF, FFA, AFG) ou participer aux initiatives européennes (JEDI) ;
- Anticiper les contraintes réglementaires : du fait de leur évolution, le projet risque de ne pouvoir être déployé. Il faut donc être attentif aux réglementations en fonction du cas d'usage, qu'il soit B2B ou B2C. À noter que, pour ce dernier, il existe plus de contraintes réglementaires relatives à la protection du consommateur final. De plus, l'enregistrement des données personnelles sur des blockchains publiques peut également poser problème dans le cadre du RGPD (voir partie 4 sur les enjeux juridiques). Les autorités de régulation comme la Banque de France, l'AMF ou la CNIL émettent de nombreuses notes informatives.

Assurer la maintenance de la solution

À la différence d'un programme classique, les blocs de la blockhain sont exécutés sur un ensemble de participants du réseau, rendant complexe le processus de débogage de l'application. Les modifications apportées restent en effet inscrites dans la blockchain, aussi un *smart contract* bogué restera stocké. Il faudra en créer un nouveau et attendre la propagation des changements pour corriger la situation, à la différence des applications classiques où les versions antérieures sont directement écrasées par les nouvelles.

Ne pas négliger la cybersécurité

Le caractère immuable et partagé de la blockchain peut entrainer de graves conséquences en cas de failles ou d'erreurs, en particulier pour les *smart contracts*. Les audits de ces derniers doivent être réguliers, tant les erreurs et failles peuvent avoir de lourdes conséquences (cf. le projet sur le DAO).

Focus
Le projet Madre, blockchain de la Banque de France pour le registre des identifiants créanciers SEPA : les facteurs de succès

La Banque de France a déployé en décembre 2017 la première blockchain d'une Banque Centrale. Grâce à elle, la Banque de France délivre les Identifiants Créanciers SEPA aux banques en quelques secondes, au lieu d'environ 15 jours précédemment. Les Identifiants Créanciers SEPA sont destinés aux entreprises qui souhaitent réaliser un prélèvement direct sur les comptes de leurs clients.

Le projet a été initié mi-2016 dans le LAB de la Banque de France dans le cadre de sa démarche d'innovation. La mise en production a été faite 18 mois plus tard, conjointement avec deux premières banques de la Place. À ce jour, six banques disposent d'un nœud de cette blockchain et trois autres banques seront raccordées début 2019.

Plusieurs facteurs ont permis le développement rapide du projet et de dépasser la phase du POC pour une mise en œuvre opérationnelle :

Un cas d'usage adapté à une technologie distribuée…

Le cas d'usage retenu était relativement simple, ce qui a représenté un facteur de succès certain. La volumétrie est modérée (une centaine d'identifiants créée par jour) et la gestion distribuée est adaptée au processus métier : la Banque de France est passée d'un mode de gestion où elle était propriétaire du registre à un mode de gestion en co-propriété avec les banques, ce qui correspond au schéma de responsabilité de ce référentiel de place.

Une technologie qui contraint à sortir du cadre…

Par nature, la blockchain change le cadre de réflexion et de questionnement. Elle facilite des approches disruptives et un changement de modèle.

Une démarche de co-construction agile et la volonté d'aller vite

La Banque de France a mené les différentes phases du projet : prototypage dans le LAB, développement de l'application et tests avec les banques, mise en production en mode agile avec une équipe regroupant des compétences métiers, techniques et juridiques. Dans un souci de co-construction et pour pallier le manque de maturité de l'ensemble des acteurs, toutes les difficultés ont été partagées en temps réel et le processus de résolution de problème mené de manière conjointe entre tous. Une startup (Blockchain Partner) a apporté ses compétences sur la technologie et a été associée à toutes les phases du projet.

Le LAB de la Banque de France a permis d'accélérer le projet, en faisant travailler startup et interlocuteurs métiers autour d'un objectif commun et en s'assurant que le produit était nécessaire et suffisant pour une mise en production. Si l'on considère qu'innover n'est pas seulement avoir de nouvelles idées, mais aussi aban-

donner les anciennes, la vitesse imprimée au projet peut également être considérée comme un facteur clé de succès : elle oblige à l'adaptation sans pour autant laisser la possibilité de revenir à un cadre de référence existant.

Une gouvernance simple du processus métier

La mise en œuvre d'une blockchain, mettant en œuvre par nature un mode distribué, nécessite de définir des règles de gouvernance claires pour définir les responsabilités des acteurs dans la gestion opérationnelle du dispositif. Un facteur de succès est de considérer un cas d'usage où la gouvernance en place n'est pas trop complexe. C'est le cas de la gestion des Identifiants Créanciers SEPA, dans lequel le schéma de fonctionnement et de partage de responsabilités reste relativement simple et basé sur la relation contractuelle entre les acteurs.

Un leadership affirmé

Forte d'un appui au plus haut niveau de l'entreprise, la Banque de France a joué ce rôle de leadership en proposant ce cas d'usage aux banques et en conduisant l'ensemble des étapes jusqu'à la mise en production effective. Sous l'impulsion de son Chief Digital Officer et des responsables du projet, elle a montré, dans une démarche d'innovation ouverte, un mode de fonctionnement différent dans le cadre de la gestion de registres de place.

La Banque de France a montré en déployant MADRE qu'elle était un acteur central de l'innovation dans le secteur financier. Elle a acquis une compétence avancée sur la mise en œuvre de la technologie blockchain, ce qui lui permet d'engager des discussions avec les acteurs bancaires pour envisager de nouveaux cas d'usages, liés au partage sécurisé d'autres informations avec les banques.

Il faut noter que ce projet est un cas simple n'intégrant pas les freins usuels d'une mise à l'échelle : la scalabilité puisqu'ils sont moins d'une vingtaine, la confidentialité des données puisqu'il s'agit d'identifiants SEPA et qu'il ne stocke pas de données personnelles.

L'application de la blockchain à l'industrie de l'assurance

L'industrie de l'assurance est un secteur majeur de l'économie, d'une part par le montant de la prime globale collectée qui a atteint 5 trillions de dollars en 2017[72] et, d'autre part, par le rôle important qu'elle joue dans la protection des personnes et des entreprises.

Néanmoins, malgré une hausse globale des primes, les résultats techniques pâtissent en raison de la dégradation sensible de la sinistralité, du poids de la réglementation et d'une baisse des primes dans des marchés matures et très concurrentiels[73].

Ainsi, plusieurs études dont le rapport McKinsey sur les évolutions de l'assurance à horizon 2030, paru en avril 2018[74], et l'étude de Ryan sur les secteurs prêts pour la disruption, parue en janvier 2018[75], ont identifié les assurances comme l'un des cinq principaux secteurs prêts à faire l'objet de transformations profondes grâce aux nouvelles technologies. La blockchain est perçue comme la technologie idéale pour transformer un secteur en recherche de solutions afin d'améliorer son efficacité opérationnelle.

Plusieurs cas d'usage ont été identifiés. Dans la gestion de sinistres où la blockchain est idéale pour apporter une preuve, la situer dans le temps et même la géolocaliser, des initiatives telles que

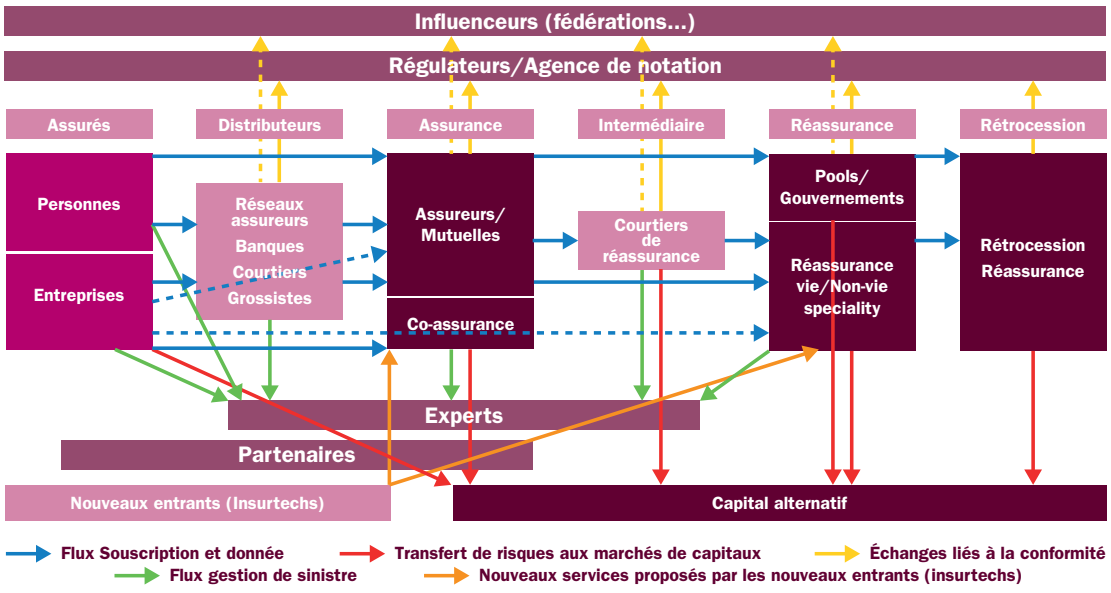


Figure 8 : la cartographie des acteurs et flux de l'assurance (source : Fathia Grandjean, 2018)

72. Swiss Re (2018) www.swissre.com/media/news_releases/nr_20180705_sigma_3_2018.html.
73. Aon (2017): Reinsurance market outlook, September 2017.
74. McKinkey (2017) www.mckinsey.com/industries/financial-services/our-insights/insurance-2030-the-impact-of-ai-on-the-future-of-insurance.
75. Ryan (2018) www.inc.com/kevin-j-ryan/industries-ready-for-disruption-2018.html.

Chainly[76] pour l'Auto et Monuma[77] pour les objets de valeur ont été analysées. La blockchain a également été testée sur des *smart contracts* pour digitaliser un contrat d'assurance ou de réassurance (ex. : la digitalisation de Cat Swap[78] et Cat Bonds depuis 2017[79]). On notera également les initiatives portées par un consortium tel que celui de la loi Hamon[80] en France, d'un consortium italien pour une plateforme d'assurance pour les risques entreprise[81] ou encore d'un consortium international B3i[82] visant à digitaliser les contrats de réassurance.

Trois grands types de flux

La chaîne de valeur de l'assurance représentée par le schéma ci-dessus illustre un grand nombre d'acteurs et d'échanges, classés en trois grandes catégories :

- Ceux liés à la relation client et à la souscription du risque, que ce soit en B2C ou B2B, et qui impliquent les assureurs et d'autres parties prenantes (courtiers, distributeurs, partenaires…) ;
- Ceux liés à la gestion des sinistres entre clients, assureurs, parties prenantes et réseaux d'experts ;
- Les institutionnels : régulateurs, agences de notation…

Les points critiques améliorables avec la blockchain

- **La souscription d'une police d'assurance est caractérisée par des échanges récurrents de données à la volumétrie conséquente :** une des principales caractéristiques de l'assurance est la notion de renouvellement. Une police d'assurance (B2C) ou un traité de réassurance (B2B) est généralement conclu pour une durée de un an et se renouvelle chaque année. À chaque souscription ou renouvellement, des volumes importants de données sont échangés pour pouvoir évaluer le risque et le tarifer. Ces échanges volumineux nécessitent des traitements lourds et surtout longs pour aller du client aux preneurs de risque ultimes. Les données sont souvent caduques ou nécessitent encore une mise à jour dès leur réception en bout de chaîne par les réassureurs et les rétrocessionnaires.
- **Une relation client tendue dans un environnement concurrentiel et une matière assurable limitée :** dans les marchés matures des États-Unis et de l'Europe occidentale, les assureurs multiplient les initiatives pour réduire les prix, augmenter les couvertures et améliorer la relation et les services apportés aux clients, mais ceux-ci restent encore peu satisfaits.
- **Une gestion de sinistre coûteuse et exacerbée par la fraude :** l'augmentation de la sinistralité pèse lourdement sur le résultat technique des acteurs de l'assurance. En 2015, la fraude à l'assurance a représenté un coût d'environ 2,5 M€ pour l'assurance dommages seule, soit environ 5 % des primes, et le chiffre continue de progresser[83].
- **Le coût de plus en plus lourd de la conformité :** les entreprises et mu-

76. www.packndrive.com.
77. www.monuma.fr.
78. www.artemis.bm/blog/2016/06/15/nephila-allianz-work-on-blockchain-catastrophe-risk-trading.
79. www.artemis.bm/blog/2018/09/10/solidum-in-first-blockchain-cat-bond-listing-on-an-exchange.
80. www.ffa-assurance.fr/en/content/trial-inter-insurer-blockchain-exchange-secure-data.
81. www.capgemini.com/news/industry-consortium-creates-first-blockchain-basedsolution-for-the-corporate-insurance-market-in-italy-to-improve-customer-service-in-therisk-assessment-phase.
82. www.b3i.tech/home.html.
83. www.argusdelassurance.com/institutions/lutte-contre-la-fraude-265-m-recuperes-par-les-assureurs-en-2015.

tuelles d'assurance et leurs partenaires sont soumis à de nouvelles réglementations qui pèsent sur l'activité. Solvabilité II, DDA, RGPD, pour ne citer qu'eux, sont autant de chantiers qui pèsent sur les ressources des assureurs.

Recommandations

Favoriser des plateformes de place intégrant les différents acteurs de la chaîne de valeur (intermédiaires, assureurs, réassureurs) autour de grandes typologies de cas d'usage (IARD, assurance-vie…) via une approche consortium.

L'objectif d'une telle plateforme de place est de mesurer en temps réel l'état des engagements et des sinistres de chacun des acteurs. Cette plateforme doit également disposer d'une infrastructure ouverte pour permettre à d'autres acteurs de l'écosystème de s'intégrer (insurtechs pour améliorer les parcours client via des solutions de déclaration de sinistre, réparateurs pour estimer les coûts du sinistre, acteurs traditionnels pour la partie contractuelle et transactionnelle).

Cette plateforme permettra notamment :

- **Des échanges instantanés, transparents et fluides :** la souscription de la police s'effectuera via un *smart contract* accessible par l'assureur et le distributeur de manière **instantanée** et, par la suite, par le réassureur qui aura une vision transparente des risques dans les portefeuilles transférés. En cas de sinistre, les données d'un constat de dommage seront également visibles de manière instantanée par toutes les parties prenantes. En cas d'aggravation du risque suite à un accident corporel par exemple, **la mise à jour de l'information** sera **dynamique** et transmise en quelques secondes plutôt qu'à la mise à jour de portefeuille qui peut prendre plusieurs mois. Cette actualisation permettra une meilleure évaluation des sinistres, une tarification juste, une évaluation des engagements en temps réel ainsi qu'une estimation plus précise des provisions et des besoins en réassurance ;
- **L'implication des principaux acteurs du marché facilitée** par le choix dans un premier temps de cas d'usage « non compétitifs » où chacun trouvera des avantages (ex. : fédérer l'ensemble des initiatives liées à la gestion de sinistre et la prévention de la fraude sur une blockchain unique pour éviter de renforcer la compétition, tel qu'observé dans le cas de la Loi Hamon[84]) ;
- **L'extension de la couverture à d'autres pays**, vu le caractère international de l'assurance.

84. www.ffa-assurance.fr/en/content/trial-inter-insurer-blockchain-exchange-secure-data.

Recommandation sur l'interopérabilité des blockchains

Promise à un fort potentiel, la multiplicité des protocoles et des applications de la technologie peut constituer un obstacle à ce que la blockchain s'impose de façon pérenne et universelle. La mise en œuvre de plateformes ad hoc favorisant l'interopérabilité devrait à cet effet se répandre.

Enjeux

La maturité technique

Voici bientôt dix ans que la blockchain existe. À l'origine, elle était utilisée pour effectuer des transactions en crypto-actifs avec le plus connu, le bitcoin et son protocole associé, Bitcoin. D'autres protocoles ont par la suite été développés, certains basés sur le modèle de preuve de travail (*proof of work*), d'autres sur celui de preuve de participation (*proof of stake*), d'autres encore sur de nouveaux types d'algorithmes de consensus (PoA, DPoS etc.).

Une nécessité pour la pérennité

Les atouts des blockchains peuvent être minorés opérationnellement si des standards d'interopérabilité ne sont pas définis à court terme. Reposant sur des logiques de réseaux, les blockchains vont devoir communiquer entre elles et agréger les utilisateurs afin de prendre leur pleine mesure.

Un enjeu non exclusivement technique

De nombreuses initiatives sont d'ailleurs annoncées pour favoriser l'interopérabilité entre blockchains, comme le partenariat annoncé entre Entreprise Ethereum Alliance et Hyperledger le 1er octobre 2018[85] ou la solution BlockSY qui adopte une stratégie Multi et Cross Chain[86].

L'interopérabilité n'est pas qu'un enjeu technique, mais aussi économique et juridique. Il découle de celui de la création de plateformes agnostiques[87] aux protocoles. Pour favoriser l'interopérabilité, la standardisation et la régulation des échanges pourront s'effectuer à l'échelle d'une industrie ou plus largement au niveau international. Le bénéfice permettra alors de faire communiquer et interagir les blockchains entre elles. Au-delà de l'aspect technologique, l'accent est également mis sur le fait que la régulation internationale est nécessaire (au niveau européen d'abord) et que le lancement d'initiatives publiques peut être un levier de standardisation.

À l'instar d'Internet et ses protocoles d'échanges, il est urgent et nécessaire d'établir des standards ou des normes d'interopérabilité afin de pouvoir construire les couches applicatives. Ce développement peut constituer un levier pour les blockchains en créant et en combinant de nouveaux services comme, par analogie, Internet a permis de généraliser le e-commerce.

Recommandations

- Favoriser l'émergence de standards techniques par des acteurs privés (ex. :

85. www.hyperledger.org/announcements/2018/10/01/enterprise-ethereum-alliance-and-hyperledger-to-advance-the-global-blockchain-business-ecosystem.
86. www.blocksy-wiki.symag.com.
87. En informatique, un état agnostique est une ressource généralisée au point d'être interopérable au sein de systèmes distincts.

Symag Blocksy, notamment avec le Pôle de recherche de Sofia Antipolis, Stratumn…) ou para-publics (ISO, Afnor…) pour l'interopérabilité entre protocoles blockchains ;

- Promouvoir le déploiement des plateformes françaises d'interopérabilité et d'interfaçage utilisateurs (Crédit Impôts Recherche, etc.) ;
- Développer les tests et utilisations par l'État de solutions blockchain pour les traitements fiscaux, électoraux, monétaires et l'amélioration de la vie quotidienne des citoyens et entreprises (actes, cartes grises, etc.).

3.5 LES TRANSFORMATIONS PORTÉES PAR LA BLOCKCHAIN

L'efficacité opérationnelle

La première blockchain d'envergure, celle du bitcoin, s'est fait connaître grâce aux possibilités de paiement qu'elle offrait. Historiquement, la création du protocole Bitcoin est corrélée avec l'émergence de la crise financière de 2008. L'idée initiale était de disposer d'un système de cash électronique pair-à-pair, c.-à-d. ne nécessitant d'intermédiaire de confiance quelconque, une banque la plupart du temps.La perte de confiance dans les institutions a matérialisé la nécessité, pour ceux qui ne voulaient plus en être dépendants, de disposer d'un nouveau moyen de transférer de l'argent de pair à pair et de manière transparente et sécurisée : le Bitcoin était né.

Ce protocole de système de cash électronique pair-à-pair proposé par Satoshi Nakamoto affiche dès fin 2008 son ambition de pouvoir remplacer l'architecture bancaire traditionnelle là où le *«coût de la médiation augmente les frais de transaction, limitant dans la pratique la taille minimale d'une transaction et empêchant la possibilité des petites transactions occasionnelles*[88] *».* La généralisation de l'utilisation de la blockchain devrait permettre à la fois d'effectuer des mouvements internationaux à moindres frais et de faciliter le développement des micro-paiements.

88. Nakamoto, S. (2008). Bitcoin : A Peer-to-Peer Electronic Cash System, disponible sur www.bitcoin.org/bitcoin.pdf.

DIP 23 : déployer l'utilisation de la blockchain pour les mouvements internationaux

Un vaste marché

Le marché des mouvements internationaux est un marché très important. La Banque Mondiale estime que les paiements internationaux (ou remittances) de travailleurs ayant migré à l'étranger vers leurs familles d'origine représentent environ 441 milliards de dollars[89] en 2015 pour les pays en voie de développement, soit environ trois fois les statistiques officielles des 25 pays recensés, et pour certains pays plus de 10 % de leur PIB (Philippines, Liban, Sénégal…)[90] avec un impact très fort sur certaines communautés (accès à la santé, l'éducation, etc.). Le flux total de ces paiements s'élevait alors à 601 milliards de dollars pour l'ensemble du globe[91], un chiffre qui sous-estime probablement la réalité.

Les inefficiences des systèmes en place

Les frais de transaction prélevés sur les paiements internationaux restent encore très élevés, avec une moyenne globale actuelle à presque 8 % du montant de la transaction pour les petits montants, parfois bien plus entre pays en voie de développement ou difficiles d'accès, comme l'Afrique subsaharienne ou les îles du Pacifique[92]. De plus, certaines transactions peuvent mettre plusieurs jours à être complétées par opposition à des temps beaucoup plus courts pour les blockchains même publiques (p. ex. une dizaine de minutes tout au plus pour l'inscription dans un bloc et la première confirmation).

Les difficultés d'adoption pour les particuliers

L'utilisation par les particuliers de blockchains publiques telles que Bitcoin pour effectuer des paiements internationaux n'est pas sans poser différents problèmes et risques :

- la volatilité des crypto-actifs par rapport aux monnaies nationales de l'émetteur et du destinataire ;
- la non-possibilité de recours face à une éventuelle erreur (p. ex. mauvaise adresse du destinataire) ;
- la perte des clés privées ;
- …

De plus, la demande croissante pour l'utilisation d'une blockchain publique (p. ex. celle du bitcoin) peut amener à des congestions temporaires du réseau qui peuvent faire exploser les frais de transaction associés. Dans ce cas, il peut être encore plus économique d'utiliser le réseau bancaire traditionnel. Enfin, les réseaux de paiement actuels bénéficient encore de l'inertie des habitudes et de la très faible acceptabilité des crypto-actifs par les marchands ; ainsi, il existe encore peu d'utilisateurs prêts à abandonner leurs cartes de crédit.

89. Migration and Remittances - Factbook 2016 – Foreword, p.vii. Third Edition. www.worldbank.org/en/research/brief/migration-and-remittances.
90. https://data.worldbank.org/indicator/BX.TRF.PWKR.DT.GD.ZS?year_high_desc=true).
91. Migration and Remittances - Factbook 2016 - Highlights, p.xii. Ce même rapport dit que le «vrai [chiffre est vraisemblablement] beaucoup plus important»..
92. Migration and Remittances - Factbook 2016 - Highlights, p.xii. Ce même rapport dit que le «vrai [chiffre est vraisemblablement] beaucoup plus important».

Les opportunités pour de nouveaux marchés et de nouveaux entrants

On estime qu'il y a aujourd'hui encore dans le monde 1,7 milliard de personnes majeures dites « non bancarisées » (c.-à-d. qui n'ont ni compte en banque, ni de fournisseur mobile de monnaie[93]). Certains services, comme BitPesa au Kenya[94], utilisent la pénétration croissante des smartphones afin de fournir à leurs clients à la fois l'équivalent d'un compte bancaire et un service de paiement international de/vers l'étranger qui ne s'appuie pas sur l'infrastructure bancaire des pays traversés. On note un fort développement de différents intermédiaires et d'outils ergonomiques, des crypto-échanges aux *wallets*, afin de fournir aux usagers :

- une interface simple avec leur compte bancaire en monnaie nationale fiduciaire ;
- des transferts intégrés et simples en crypto-actifs une fois sur le réseau.

Par exemple, l'application de paiement Circle utilise la technologie blockchain pour transférer rapidement l'argent de ses clients autour du monde. Ces derniers n'ont affaire qu'à de la monnaie nationale et ne voient pas l'architecture *back end* de blockchain qui permet à Circle de garantir des paiements internationaux avec de faibles commissions de change.

Les monnaies virtuelles des banques centrales

Il faut également noter que les paiements internationaux et les transferts entre banques devraient pouvoir bénéficier du déploiement des monnaies virtuelles des banques centrales. Plusieurs projets nationaux sont en cours. Par exemple, le projet Ubin en Asie, qui inscrit sur un registre distribué des jetons considérés comme équivalents au dollar singapourien (SGD), est à suivre attentivement alors que de nombreuses banques centrales travaillent sur ce sujet.

Micro-paiements et smart contrats

Le développement des jetons/crypto-actifs et des blockchains rend aussi possible une multitude de micro-paiements liés à des usages de consommation de plus en plus granulaires (p. ex. payer pour une chanson par opposition à un album) et distribués (la chanson achetée sera simultanément disponible sur tous les appareils connectés du consommateur). Structurés par des *smart contracts*, les micro-paiements devraient permettre une consommation de plus en plus adaptée et intelligente (p. ex. des droits d'auteur indexés sur des métriques d'usage pourraient être immédiatement répartis entre artistes d'un collectif en fonction de termes encapsulés dans un *smart contract*). Pour le moment, le modèle économique de solution de petits paiements par blockchain reste à démontrer face aux grands systèmes centralisés et en temps réels européens, comme STET Core par exemple.

Recommandations

Le monde des paiements devrait connaître une révolution sur les 5-10 prochaines années en :

- Facilitant l'utilisation de la blockchain pour des micro-paiements organisés par des smart contracts à partir de quelques cas d'usage ;

93. P.4. The Global Findex Database – 2017 – Measuring Financial Inclusion and the Fintech Revolution. World Bank Group. Il est à noter que ce chiffre semble en baisse avec notamment l'introduction croissante des smartphones dans des pays où l'infrastructure bancaire est encore très morcelée ou inexistante.
94. https://www.bitpesa.co.

- Lançant des enquêtes auprès des utilisateurs pour évaluer l'inertie de leurs habitudes, la dynamique de leurs préférences et en déployant des heuristiques d'ergonomie optimale ;
- Développant une grille d'analyse comparative pour les différents modes de paiement (ex. temps de transaction, frais du réseau et des opérations de conversion, possibilité de recours en cas d'erreur opérationnelle, etc.) et en comparant les solutions existantes et leurs différents canaux pour des cas d'usage précis (ex.. envoyer de l'argent du Mexique en Corée du Sud).

DIP 24 : création d'un crypto-euro propre à la zone euro pour les paiements de gros et de détail

Il existe aujourd'hui plus de 2000 crypto-actifs différents sur le marché. Les plus connus restent encore ceux du top 10 des capitalisations avec le bitcoin en tête de liste, le « père des crypto-actifs ». Tous n'ont pas le même objectif et la vocation à être un moyen d'échange de valeur, mais pour le bitcoin, il s'agit de son ADN.

De l'autre côté, les crypto-actifs sont parfois en compétition avec les monnaies nationales dites souvent « fiats ». Les monnaies nationales sont soit fiduciaires, c'est-à-dire sous la forme de billets et de pièces, soit scripturales sous la forme d'écritures informatiques tenues dans les systèmes d'information centralisés des banques. En Europe, selon les chiffres de l'OCDE, 91 % de la masse monétaire est scripturale. Ces monnaies sont émises par les États et leur création et leur gestion déléguées aux banques centrales. Les cours des monnaies nationales sont influencés en partie par les politiques monétaires des États, les balances des échanges commerciaux entre pays et fixés par les marchés de change. En Europe, c'est la Banque Centrale Européenne qui est en charge de l'euro pour le compte des 19 pays de la zone euro. Pour autant, même si la BCE pilote tout le processus monétaire, ce sont ensuite les banques commerciales des États qui gèrent les flux d'argent entre les particuliers ou les entreprises grâce aux systèmes de paiement et par les mécanismes du crédit. Ainsi, les banques commerciales relaient la politique monétaire de la banque centrale, participent à la création monétaire et tiennent les comptes des particuliers et des entreprises qui n'ont pas de comptes ouverts auprès de la banque centrale et n'ont pas accès à la monnaie banque centrale. Seuls les établissements de crédit détiennent des comptes auprès de la banque centrale et ont accès à la monnaie banque centrale.

Il existe deux types de paiement électronique, ceux dits de détail et ceux de gros. Les premiers portent sur les transactions de petits montants, typiquement le paiement par chèque, carte de crédit ou virement. Les deuxièmes concernent les transactions sur de gros montants, par exemple les transferts interbancaires. Les systèmes de paiement peuvent fonctionner sur une base RBTR (règlement brut en temps réel) ou bien faire appel à la compensation.

Enjeux

Les enjeux sont essentiellement de deux ordres. Dans quelle mesure un crypto-euro reposant sur une blockchain et accessible aux particuliers et entreprises permettrait de résoudre certaines limites du système bancaire actuel ? Pour le marché de gros, le principal intérêt d'un crypto-euro serait de permettre aux marchés financiers s'appuyant sur des plateformes blockchain de réaliser un règlement livraison en monnaie banque centrale comme c'est actuellement le cas pour les marchés réglementés.
Afin de pouvoir mettre en œuvre un crypto-euro (sous une forme ou une autre), différents écueils devront être résolus :

- Les crypto-actifs comme le bitcoin ont une volatilité extrêmement élevée et ne répondent pas toujours aux trois principes fonctions d'une monnaie : intermédiaire d'échange (capacité d'éteindre les dettes et les obligations, notamment fiscales), réserve de valeur et unité de compte ;
- Les transactions sur le bitcoin sont pseudonymes, les utilisateurs sont cachés derrière un couple clé privée/clé publique qui ne permet pas de disposer de l'identité des membres réalisant les transactions. L'obligation de KYC sur la blockchain Bitcoin n'est pas gérée et pose des problèmes de compliance en regard de la réglementation en vigueur dans le système bancaire ;
- Le recours à un crypto-euro se substituant au paiement en espèces (liquide) pour les particuliers pose en outre un problème politique : doit-il garder le caractère anonyme des paiements effectués en espèce ou bien (pour les problématiques KYC soulevées plus haut) doit-il devenir traçables par les autorités ? La fin du cash papier pose de graves problèmes de protection de la vie privée ;
- Par construction, les blockchains (publiques en tout cas) reposent sur le principe même de transparence des transactions, ce qui pose donc un problème de confidentialité ;
- Enfin, les blockchains sont aujourd'hui des systèmes de règlement brut en temps réel (RBTR) impliquant de s'assurer que le cash (ou les titres) sont bien disponibles pour un bon dénouement des transactions. Or, le système financier actuel repose sur des mécanismes de crédit qui peuvent parfois être risqués, mais permettent aussi d'apporter de la liquidité pour que le système continue à fonctionner, notamment en cas de stress bancaire. Ces considérations sont à prendre en compte dans toute réflexion sur le développement d'un crypto-euro.

Il convient actuellement de noter, en relation avec l'actualité récente (voir la suspension de l'accord avec l'Iran ou encore les amendes records infligées à la BNPP ou à Siemens) que l'émergence des crypto-actifs questionne le statut de référence/étalon international dont jouit le dollar américain depuis l'abandon de l'étalon-or dans les années 1970. Il peut y avoir un enjeu de souveraineté crucial pour la France et l'Europe de considérer l'idée d'un étalon monétaire international non dépendant d'un État pour pouvoir agir en toute indépendance sur le plan économique et géopolitique. Plus spécifiquement, des enjeux se concentrent sur l'utilisation d'un futur crypto-euro dans la distribution de détail et dans le commerce de gros.

Le crypto-euro

Les particuliers et entreprises ne peuvent disposer d'un compte à la banque centrale et donc des garanties qu'elle apporte aux fonds qui lui sont confiés, même si les clients qui déposent leur épargne dans les banques commerciales ont des garanties sur leurs dépôts au cas où la banque ferait faillite, l'État couvrant jusqu'à certains montants les fonds déposés. Cependant, en cas de faillite de l'État et donc du système monétaire local, cela ne fonctionne plus.

Le taux de bancarisation en Europe est d'environ 70 %. Une part importante des transactions se fait en espèces et est donc non-traçable, ce qui pose de nombreuses questions en matière de blanchiment, de trafic et d'évasion fiscale. La mise en place d'un crypto-euro permettrait

d'augmenter le taux de personnes bancarisées en leur fournissant un moyen de réaliser des paiements à moindre coût, totalement sécurisé et transparent tout en augmentant la traçabilité des transactions à l'échelle européenne et donc en limitant les risques de blanchiment et d'évasion fiscale.

Les délais des paiements (de gros ou de détail) pouvaient, jusqu'au déploiement en cours des virements instantanés, être longs (parfois plusieurs jours) et a fortiori coûteux pour les banques commerciales du fait des mécanismes de compensation nécessaires dans le processus quotidien d'échanges interbancaires. Ces coûts se répercutent sur les frais bancaires pour les clients.

Un euro-jeton utilisé pour dénouer des transactions effectuées sur des plateformes blockchain

- Les mécanismes de règlement livraison sur les marchés financiers sont déjà très efficaces et permettent de dénouer des transactions en monnaie banque centrale (Systèmes T2S et Target 2 ;
- Les plateformes en cours de développement sont toutes confrontées à cet écueil et réfléchissent à l'usage de monnaie banque commerciale pour dénouer la partie devise des transactions. Le recours à la monnaie banque commerciale pourrait être vu comme une régression par rapport à la situation actuelle, car moins sûre. Un tel recours pose de toute manière la question de l'interfaçage d'une blockchain aux systèmes de paiement existants ;
- La création de nouvelles plateformes blockchain de tenue de registre et de transactions permettant d'échanger des instruments financiers pose la question du recours à la monnaie banque centrale pour dénouer les transactions effectuées sur ces plateformes ;
- Le développement d'un crypto-euro pouvant servir pour dénouer la partie cash des futures plateformes blockchain constituerait une réelle avancée.

Recommandations

La création d'un jeton servant de monnaie officielle, émis par la Banque Centrale Européenne, un « jeton-euro », semble être la meilleure réponse à apporter pour répondre aux enjeux soulevés. (Le Canada a déjà fait une tentative intéressante en ce sens, mais elle a été suspendue pour le moment en juin 2017).

Pour cela, différentes actions sont possibles :

- Continuer les expérimentations technologiques sur les limites actuelles de la technologie (pseudonymat, publicité des transactions notamment).
- Penser aussi aux implications politiques plus larges et participer à l'élaboration du cadre adéquat pour en débattre ;
- Mobiliser les infrastructures de marché sur le sujet des marchés financiers : Euronext, Euroclear, LCH Clearnet, STET, Liquidshare;
- Accompagner les réflexions de la Banque de France en collaboration avec la BCE pour favoriser le leadership français sur la question des « Monnaies Digitales de Banque Centrale ».

DIP 25 : développer un modèle standardisé basé sur les smart contracts et appliqué aux transactions boursières

Le processus actuel implique de nombreux acteurs, étapes et flux selon le schéma ci-dessous :

- Exécution d'une transaction : les courtiers agissent pour le compte d'un acheteur et d'un vendeur pour soumettre des ordres à la bourse ;
- La compensation : les ordres sont envoyés à la chambre de compensation pour la résolution du contrat ;
- Règlement et livraisons : le règlement/livraison des titres est réalisé.

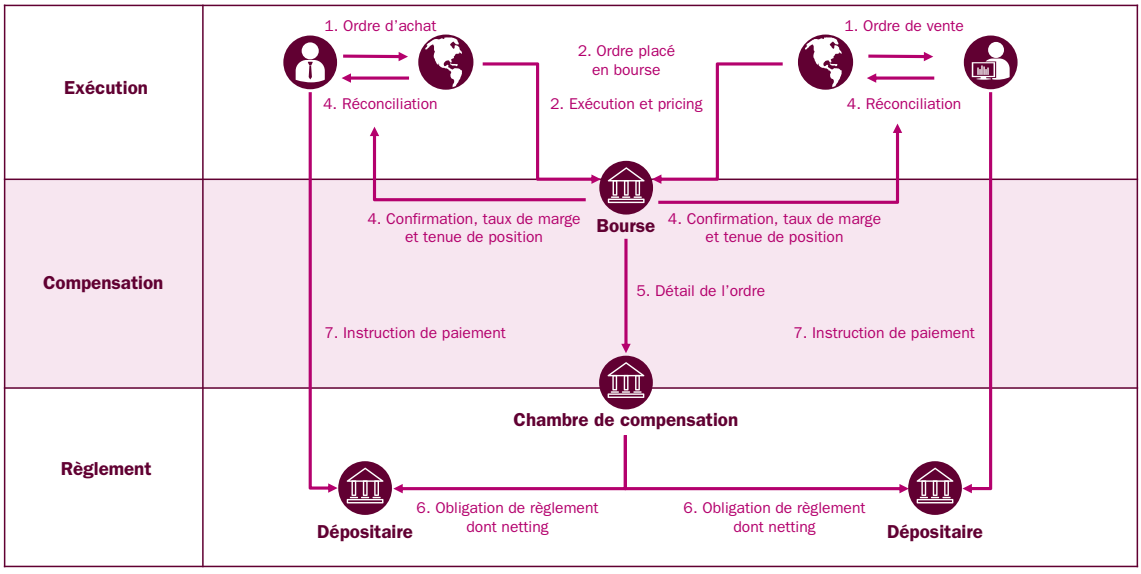
Enjeux

- Plusieurs versions de la transaction sont enregistrées sur les différents systèmes utilisés par tous les participants ;
- Le processus de règlement et de livraison est long, environ deux à trois jours, ce qui mobilise capital et liquidité ;
- Les informations et les instructions sur les comptes changent régulièrement : de nouveaux comptes sont ouverts, fermés et les dépositaires changent…
- Le risque opérationnel est accru (interprétation erronée, exécution incorrecte).

Recommandations

Les transactions, dont le volume et la complexité augmentent, doivent être correctement traitées afin de réduire les risques pour tous les acteurs impliqués (cf. figure ci-dessous).

En raison du nombre d'intermédiaires, une nouvelle approche serait de **définir un modèle de workflow standardisé sur l'ensemble du processus de bout en bout basé sur les *smart contracts***. Celui-ci serait validé et partagé par l'ensemble des participants. L'implémentation pourra gérer les transactions automatisées en utilisant un enregistrement source unique et synchronisé.



Ce modèle s'appuierait sur un langage de modélisation de *smart contracts* et modéliserait l'ensemble des transactions granulaires de bout en bout en y intégrant les droits et obligations de toutes les parties. Ce langage doit codifier sans ambiguïté des accords complexes, concrets et réels. Il en résulte un processus précis, rapide et sans frictions pour tous les participants à la transaction, avec les avantages suivants :

- Tous les participants sont soumis à des processus et des règles de marché communs permettant une interprétation et une application cohérentes ;
- L'harmonisation et l'automatisation des *workflows* réduisent les erreurs et les couts opérationnels ;
- Les règlements sont mieux sécurisés en introduisant des contrôles de prétransaction ;
- Les émetteurs peuvent annoncer et signer de manière cryptographique des événements, réduisant ainsi les risques d'interprétation erronée ou d'exécution incorrecte et supprimant le besoin de validation par des tiers ;
- Les participants sont notifiés simultanément en temps réel dès qu'un événement se produit ;
- Les processus et les délais complexes sont mieux modélisés.

En conséquence, le déroulement des transactions est rationalisé, la correction est assurée et chaque participant est certain de disposer des informations à jour grâce à la source immuable, fiable et unique figurant dans le grand livre. Dans le même temps, la conception du grand livre garantit la confidentialité, les données n'étant visibles que pour les parties ayant le droit de lecture.

L'implication de tous les acteurs devrait être progressive, en commençant dans un premier temps par les processus de compensation et de règlement/livraison et, dans un second temps, en adressant les courtiers dont les comptes blockchain passeraient des commandes pour leurs clients sous forme de *smart contracts*.

Une blockchain privée, dans laquelle les nœuds seraient contrôlés par un consortium composé de courtiers et des chambres de compensation, est à considérer. Même si cette dernière solution sera plus complexe et nécessitera une coordination entre un grand nombre de participants, elle apportera le plus grand avantage en termes de réduction du temps nécessaire au cycle de vie des transactions de quelques jours à quelques minutes.

D'autres fonctionnalités peuvent être ajoutées : la chambre de compensation peut par exemple définir un délai d'exécution ou créer des comptes sur marge pour les membres compensateurs, avec des règles personnalisées définies dans les *smart contracts*.

En outre, la blockchain sert à la fois de plateforme de compensation et de plateforme de règlement, éliminant ainsi le besoin de réconciliation entre différents acteurs.

3.6 L'OPTIMISATION DU PARTAGE DE L'INFORMATION ENTRE ACTEURS

DIP 26 : utiliser la blockchain pour gérer l'identité et l'authentification

Nous vivons actuellement grâce à la digitalisation une rupture dans notre matière d'interagir avec les individus, les sociétés et les services. Face à ces changements dans nos échanges, nos modes de gestion de notre identité et d'authentification montrent de sérieux points de faiblesses et une obsolescence dangereuse.

Les témoignages de fraudes, usurpations d'identité, falsifications, fuites de données, etc. se multiplient et sont autant d'arguments d'évolution. En parallèle, la réglementation et les États s'adaptent et se durcissent pour prendre en compte ces nouvelles pratiques et protéger au mieux les données personnelles des citoyens. De même, ces derniers prennent progressivement conscience des risques numériques et font preuve d'une défiance croissante vis-à-vis de tout service qui collecterait leurs données personnelles. Côté entreprises, les nouvelles règles leur imposent de rassembler de plus en plus de preuves authentiques et d'informations sur leurs clients pour *s'assurer que ces derniers sont bien ceux qu'ils prétendent être* et se prémunir des fraudes et usurpations d'identité.
La situation devient donc de plus en plus contradictoire avec, d'un côté, des clients qui souhaitent et doivent protéger leurs données personnelles et, de l'autre, des entreprises qui leur réclament de plus en plus d'informations pour leurs activités et qui recours de plus en plus à des procédures d'authentifications afin de se conformer à la réglementation et se protéger des cyberattaques.

Enjeux

La mise à disposition de services et parcours 100 % digitaux tend à devenir la norme pour l'ensemble des entreprises orientées consommateurs (B2C). Le consommateur doit pour chacun de ces services fournir un certain nombre d'informations personnelles, de preuves d'identité et d'autres documents justificatifs, ce qui complexifie l'expérience utilisateur. La collecte et la détention de telles informations sont fortement réglementées, notamment dans le cadre du RGPD et des règles bancaires de connaissance client.

Dissémination et duplication des données clients

À chaque fois qu'il souscrit à une nouvelle offre, le client doit envoyer au fournisseur de service l'ensemble des informations personnelles et pièces justificatives requises. Il devient rapidement impossible de savoir :

- Avec qui les informations ont été partagées ;
- Quelle est la politique de protection et d'utilisation des données mise en place par le service ;
- Quels documents ont été fournis ;
- Quand a eu lieu la dernière mise à jour ;
- ....

Par ailleurs, la donnée en elle-même étant devenue un actif d'une grande valeur, les

fournisseurs de services n'hésitent pas à demander à leurs utilisateurs des informations qui n'ont que peu de lien avec leurs activités et les services offerts.

Complexification de l'expérience utilisateur

Les processus de renseignement et vérification d'identité sont devenus systématiques et plus ou moins répétitifs aux yeux des consommateurs. Pour chaque connexion à un nouveau site web ou application mobile, le client renseigne les mêmes informations personnelles et fournit les mêmes pièces justificatives, rendant l'expérience utilisateur de plus en plus pénible. L'amélioration et la fluidification de ces processus sont d'ailleurs un défi que rencontrent les grandes entreprises face à l'arrivée de startups qui profitent de ces points de friction pour intégrer de nouveaux marchés, grâce à la promesse d'expériences utilisateurs inédites.

Hausse de la vulnérabilité

Le partage massif des informations et documents personnels nécessaires à la validation de l'identité augmente d'autant le nombre d'entreprises et serveurs pouvant être attaqués. Chaque fournisseur de service est censé être responsable du stockage et de la protection de ces données.

La fuite de données et les cyberattaques ne sont que le reflet de la faiblesse de ces mesures de protection et des lacunes existantes. Le risque de cyberattaques est d'ailleurs devenu ces derniers mois l'une des principales craintes des entreprises. Aucun secteur technologique n'est épargné, ainsi, par exemple des clés privées en ligne donnant accès aux actifs, voire à l'identité des détenteurs de crypto-actifs, ont été visées par des cyberattaques et ont pu être dérobées. À ce jour, les clés privées stockées hors ligne semblent protégées de ces attaques.

Recommandations

Face à ce nouveau paradigme, il devient urgent de :

- Redonner aux individus la pleine possession et le contrôle de leurs données personnelles en leur fournissant des applications leur permettant de les gérer et de les contrôler en toute sécurité ;
- Assurer aux entreprises des niveaux d'authentification élevés pour lutter contre la fraude ;
- Garantir l'irréversibilité des anonymisations de données notamment par croisements multibases ;
- Permettre la conservation et une utilisation simple des clés privées donnant accès à l'identité et aux actifs enregistrés dans une blockchain ;
- Favoriser pour les entreprises la transparence complète sur l'utilisation de leurs données clients ;
- Permettre le partage d'informations authentifiées entre plusieurs acteurs, sans s'appuyer sur une plateforme centrale.

Aucun système ni aucune institution n'ont aujourd'hui réussi à mettre en place une solution digitale centralisée qui permette d'atteindre l'ensemble de ces prérequis. En effet, les entreprises sont très réticentes à partager leurs données-clients et à faire confiance à des tiers.

Les solutions implémentées dans les technologies blockchain pourraient permettre également de répondre à ce besoin de décentralisation, tout en garantissant sécurité, confiance et transparence pour l'ensemble des participants. En effet, couplées à d'autres technologies existantes

(coffre-fort électronique sur le cloud, cryptographie asymétrique, preuve sans divulgation/*Zero Knowledge Proof*, etc.) elles permettraient de créer des identités numériques et des méthodes d'authentification qui respectent la vie privée des consommateurs et répondent aux exigences des institutions et des entreprises.

Pour rendre possibles le déploiement et l'acceptation de ces identités numériques, il est fondamental que l'initiative et l'innovation soient poussées par les États ou des acteurs indépendants de confiance et non par des fournisseurs de service qui y verraient un but lucratif.

Des innovations et expérimentations ont déjà été lancées, renforçant la nécessité pour l'Europe et la France de préserver leur souveraineté. Il existe déjà une gestion des identifiants numériques au travers de France Connect, de l'ANTS et de la Direction Générale des Finances Publiques (site www.impots.gouv.fr) pour les particuliers. Le projet de Carte d'Identité Numérique française en cours de mise en place devrait permettre de faciliter d'ici deux ou trois ans l'usage de telles pièces dans les blockchains.

Parmi les options possibles, les expérimentations suivantes permettraient de valider les différents concepts et briques technologiques et de rester dans la course à la maîtrise de ces technologies disruptives. Plusieurs pays ont fait en la matière des annonces récentes :

- Utiliser une technologie qui permette la gestion de l'identité par l'individu et qui soit reconnue par l'autorité de nommage garantissant la confidentialité/anonymat selon le contexte ;
- Construire un modèle d'identifiants attributifs (et non déclaratifs), intégré par l'État, qui permette d'opérer directement sur un service en ligne accessible de n'importe où, n'importe quand et à partir de tout terminal (*smartphone*, ordinateur…) ;
- Utiliser la technologie blockchain pour gérer les étapes critiques (accès, transferts, traitements) liées à la gestion de données personnelles (bancaires, médicales…) et créer des applications plus performantes, moins redondantes, interopérables par conception et intrinsèquement respectueuses de la confidentialité de l'individu ;
- Utiliser des jetons à usage unique, irréfutables et infalsifiables, pour réaliser les opérations d'identification et d'authentification de documents et certifier les demandes d'accès (services de paiement, gestion de contrats, etc.).

Les secteurs de la santé, des banques et des assurances, particulièrement sensibles à la protection des données et soumis à des réglementations strictes, sont parmi les meilleurs candidats pour réaliser de premiers tests, comme :

- Gérer les obligations de connaissance client résultant des exigences législatives et réglementaires imposées aux institutions financières (KYC – voir ci-après),
- Demander à l'État (ASIP) de gérer les carnets de vaccination des citoyens sur une blockchain (permissionnée ou de consortium),
- Déployer des services à forte valeur ajoutée pour le citoyen et utilisant des données médicales chiffrées, à l'instar du projet Kidner sur le don croisé de rein (recherche de correspondance sans divulgation de données critiques pour découvrir une possibilité de transplantation et diminuer le temps d'attente sur liste),
- Mettre en place des bases de données

– et non des silos de données – à l'intégrité élevée, permettant :

- de diminuer les risques de corruption ou de mauvaises pratiques (par exemple, en matière d'essais cliniques, pour permettre une validation sécurisée de chaque étape du protocole) ;
- d'améliorer les performances des avancées en intelligence artificielle (80 % de la performance de l'IA est liée à la qualité du registre de données utilisées) ;
- d'améliorer les capacités de mobilité des patients (n'importe quel médecin, si autorisé par le patient, peut accéder au dossier médical peu importe où, même si le patient n'est pas dans sa ville d'origine ou s'il arrive inconscient aux urgences).

DIP 27 : améliorer la connaissance client (KYC) en créant une infrastructure de place

Identité, authentification et connaissance client/intermédiaire

L'identité numérique des clients est utilisée fréquemment par les établissements financiers, les grands facturiers, les assureurs et les organismes publics. Pour les entreprises et les banques, d'autres données d'identification sont utilisées et varient selon les besoins et le traitement subséquents.

Il est donc demandé fréquemment aux clients particuliers ou entreprises de saisir à de multiples reprises les mêmes données lors de la contractualisation ou des opérations relatives à un contrat. Cela est fastidieux pour les clients et coûteux pour les organismes devant saisir, vérifier et confirmer les données ainsi saisies et stockées. Les risques de fausses déclarations, d'erreurs de saisies, de manque de vérification et de perte sont non négligeables.

Par ailleurs, l'obligation de connaissance client (KYC) ou de connaissance des intermédiaires (KYI) s'impose aux établissements financiers. Elle nécessite la saisie, mais surtout la vérification des données d'identité et d'identification. Ce processus est fastidieux et onéreux, tant pour les clients que pour les établissements. De plus, ce sont généralement toujours les mêmes informations qui sont requises.

Il y a donc un besoin à ce jour non satisfait d'un moyen d'échange d'identité client, simplifié, fiable, rapide, infalsifiable, inviolable, stable, traçable et à bas coût, permettant l'authentification du client ou des intermédiaires et la conformité aux règles de KYC.

Le point clé est le point d'entrée initial des données, lequel doit être absolument fiable et reconnu comme tel. Cela peut être l'État, les banques, les assureurs, certains facturiers qui ont la possibilité d'effectuer les vérifications nécessaires sur la personne, sa résidence, sa situation financière élémentaire, comme cité antérieurement.

Les solutions centralisées sont lourdes et coûteuses. Toutefois, les grands groupes échangeant entre leurs entités des données clients (avec leur consentement) sont également intéressés par des solutions facilitant l'enrôlement des clients.

Les blockchains publiques, mais surtout privées, répondent aux contraintes évoquées plus haut.

Le projet de place du consortium LabChain, dont le premier cas d'étude a été consacré à l'identité numérique et aux problématiques KYC[95], a été lancé en ce sens par la CDC avec la participation de nombreux acteurs financiers. Plusieurs pays ont par ailleurs avancé en la matière (Estonie, Espagne avec Alastria et Niuron). La plupart des grands groupes bancaires ont une réflexion ou des tests en cours via des blockchains,

95. www. bitcoin.fr/labchain-un-premier-cas-detude.

pour la plupart privées, sur les échanges de connaissances clients ou intermédiaires (SWIFT) ou avec de nouvelles structures (Granada, KYCTrust CapGemini/R3, etc..).

Les points critiques sont nombreux, mais non insurmontables

- La solution technique : le choix du protocole de la blockchain, à priori privée, afin de pouvoir contrôler les ayants droit à entrer les données et éviter leur stockage hors UE. Les règles de consensus restent à définir. Le choix des algorithmes de cryptage est également un élément de la fiabilité du système tout comme le choix du stockage de données et des droits d'accès ;
- La différence de besoin entre la connaissance clients particuliers et entreprises ;
- La définition commune des données : une première liste a déjà été faite pour les particuliers par le LabChain de la CDC. Des questions restent à traiter : notes issues de fichiers types FICP, PPE, IBAN de compte client en vue des prélèvements, etc. ;
- Le modèle économique : mesure du coût des saisies, facturation des bénéficiaires, rémunération des fournisseurs, partage des coûts d'infrastructure entre les participants du réseau privé (les blockchains privées sont a priori à privilégier pour éviter les coûts et la volatilité des crypto-actifs des blockchains publiques comme celle du bitcoin) ;
- Les participants fournisseurs de données : qui autorise-t-on ? Avec quels engagement et responsabilité ?
- La conformité au RGPD en matière de droit à l'effacement, lequel peut sembler contradictoire avec l'immuabilité des données enregistrées sur la chaîne ;
- Les bénéficiaires : par nature, tous les fournisseurs/contrôleurs d'entrée des données et les entreprises de l'Union Européenne répondant aux contraintes RGPD et acceptant les règles techniques et économiques de l'échange. Faut-il donner accès aux GAFA et au commerce en ligne ou se limiter aux aspects financiers ou publics ?
- La capacité à vérifier les entrées clients et les faux positifs pour laquelle l'intelligence artificielle pourrait être utilisée en complément ;
- La cybersécurité du système face aux attaques et aux détournements notamment des clés privées ;
- La volonté des acteurs majeurs à participer et se faire confiance, notamment dans le cadre d'un consortium national (les données clients constituent une ressource pour chaque banque, lesquelles ne souhaitent pas les mettre en commun avec leurs concurrentes).

Recommandations

- Mettre à disposition une solution simple sur mobile et PC permettant d'activer sa clé privée et de suivre ses consentements : des solutions existent déjà à l'état de test sur mobile pour les particuliers ;
- Établir une charte d'usage et de surveillance/gouvernance et la création de nœud d'audit, notamment pour le régulateur ;
- Mettre en place une/des infrastructure(s) de place permettant d'échanger les identités et leurs preuves, reconnue(s) par l'État et respectant les réglementations Connaissance Client/LCB-FT/RGPD et en permettant le contrôle ;
- Définir un cadre juridique organisant la mise en œuvre et l'utilisation d'une infrastructure de place pour rassurer les acteurs sur la conformité de leur participation au dispositif ;
- Définir un standard interbancaire de données clients particuliers et entreprises en vue des échanges ;

- Créer une structure de contrôle des participants à la chaîne des échanges.
- Définir des normes de sécurité et cybersécurité de la chaîne et des smarts contracts ;
- Accélérer le déploiement, après retour sur le pilote développé par le LaBchain, auprès des établissements financiers pour la connaissance des particuliers et l'étendre aux personnes morales ;
- Disposer d'une réglementation permettant l'usage de la blockchain pour l'échange de données d'identité des clients et compatible avec la réglementation sur les données personnelles ;
- Créer une gouvernance adéquate (AFNOR ou ISO), éventuellement sur le modèle du GIE CB/Paylib pour gérer les normes, les agréments et les facturations.

DIP 28 : la traçabilité appliquée au commerce international trade finance)

Les principaux acteurs du trading et du financement de matières premières sont à la recherche de rentabilité et de sécurité dans leurs transactions, principalement en raison d'un manque de confiance entre les acteurs. L'accent était mis sur les processus post-transaction (« post trade ») du fait de :

- L'absence d'une expérience utilisateur post-transaction totalement intégrée en raison de la fragmentation du marché et d'un nombre élevé d'intermédiaires dans le monde entier ;
- L'inefficacité opérationnelle due à l'échange de documents originaux en version papier, à des données redondantes et aux duplications des réconciliations. L'étude BCG[96] de 2017 a montré que seulement 10 à 15 % des traitements des données par les principaux acteurs avaient une valeur ajoutée, le reste étant principalement constitué de duplication et de réconciliation de données dans divers systèmes d'information privés ;
- Un processus chronophage, augmentant ainsi le besoin en fonds de roulement, notamment pour les négociants ;
- Un métier risqué entraînant des provisions élevées et des pertes financières. Cela nécessite une importante expertise de chaque acteur pour se prémunir de documents falsifiés, de fausses déclarations, de déclarations de biens en double, etc..

Avant 2017, de nombreuses initiatives privées ont sans succès tenté de s'attaquer à ces problématiques, chaque acteur ne pouvant lutter que contre ses propres inefficacités.

Recommandations

Avec le recul, quelques bonnes pratiques peuvent être retenues pour mener à bien ce type de projet :

- S'appuyer sur la co-création, source de richesse et offrant un taux d'efficacité beaucoup plus élevé en s'attaquant aux inefficacités du secteur plutôt qu'aux inefficacités individuelles de chaque membre du consortium ;
- Structurer l'approche avant de lancer les travaux est déterminant pour créer dès le départ un référentiel partagé et imaginer ensemble une solution commune ;
- Mener la réflexion et développer une expérimentation avec le même groupe de participants afin de créer plus de valeur au sein du consortium. Cela implique un projet plus long, mais assure un cadrage plus concret de la solution en amont du choix de mise en œuvre ;
- Mélanger les deux approches et structurer un projet de groupe ainsi : identifier les points de difficulté et la vision commune, imaginer ensemble la solution et expérimenter conjointement avant de choisir la manière dont le groupe souhaite implémenter la solution ;
- Créer un groupe avec des objectifs, un mandat et une organisation clairs et dotés de ressources dédiées, dispo-

96. Boston Consulting Group.

sant d'une expérience des technologies blockchain, des modèles économiques et d'architecture de plate-forme digitale, du métier et de la gestion de projet ;

- Utiliser la blockchain s'appliquant naturellement aux objets digitalisés pour assurer la traçabilité de biens physiques et développer des solutions adaptées à la diversité des produits à suivre (RFID, étiquettes, patch… sur des emballages, conteneurs, véhicules…).

Focus
Retour d'expérience de grandes banques françaises dans le financement du commerce international et le crédit documentaire

Après une première étape réussie de prototypage, l'utilisation de la blockchain a nécessité la mobilisation de tous les acteurs du consortium, tant sur le volet technologique que sur celui du business model, avec une avancée concomitante sur les deux sujets.

Deux projets menés en parallèle

Un premier prototype a été réalisé et présenté lors de la semaine de « International Petroleum » à Londres en février 2017 par un premier groupe d'acteurs du négoce et du financement de matières premières. Il a permis de rassembler les principaux acteurs du marché pétrolier. La question était alors : suite à cette expérimentation, le DLT peut-il être un levier permettant de répondre aux problèmes anciens de cette industrie ? Plusieurs banques françaises ont activement contribué à des consortia internationaux (Voltron, Marco Polo, UTN…). L'objectif était de :

- Confirmer que les principaux acteurs partagent les mêmes problèmes listés ci-dessus;
- Comprendre et tester l'appétence du secteur pour résoudre conjointement ces problèmes.

Cela a permis de :

- Évaluer la possibilité de numériser le contrat de vente et son financement sur une infrastructure distribuée;
- Évaluer la maturité de la technologie pour la mise en production à l'échelle de l'attente des acteurs et identifier les exigences non fonctionnelles de mise en service;
- Encadrer et structurer l'approche (animation d'ateliers, suivi de planification et développement du prototype) avec des équipes communes aux ressources dédiées.

Ces plateformes digitalisent le contrat de vente, automatisent son traitement et le contrat de financement (lettre de crédit) et traitent une transaction en direct avec les principaux acteurs du processus (vendeur, acheteur, banques, inspection, transporteurs et agences gouvernementales).

Le constat d'un prototype de la Société Générale fait apparaitre une amélioration d'un facteur 5 de l'efficacité du processus de bout en bout grâce à la saisie unique des données par le propriétaire des données, le partage en temps réel des informations et une sécurité accrue grâce à la transparence de la DLT.

Les bonnes pratiques:

- S'appuyer sur la co-création, source de richesse et offrant un taux d'efficacité beaucoup plus élevé en s'attaquant aux inefficacités du secteur plutôt qu'aux inefficacités individuelles de chaque membre du consortium,
- L'approche adoptée par les consortia était très importante pour favoriser une compréhension commune, un terrain d'entente au sein du groupe pour penser ensemble et faire grandir la confiance.

3.7 ENJEUX RÉGLEMENTAIRES

Dispositions réglementaires impactées par la technologie blockchain

Dispositions réglementaires et bancaires

Initialement créées pour permettre de la création de la crypto-monnaie bitcoin, les technologies blockchain se sont répandues principalement pour les usages connexes d'échange de valeurs sans intermédiaire de confiance et de levée de fond (Initial Coin Offerings/ICO).

Face à l'importance croissante, à l'engouement, et aux enjeux financiers de ces usages très spéculatifs qui ont entraîné des tentatives de fraude, une reconnaissance et une réglementation deviennent indispensables pour ne pas geler l'innovation et gêner les investisseurs par des discours trop alarmistes.

Certaines autorités de régulation ont fait part de leurs inquiétudes quant à la volatilité du cours des crypto-monnaies, telles que :

- La FCA (Financial Conduct Authority – régulateur anglais) a pu mettre en avant le risque fort de fraude et de volatilité de ces crypto-actifs ;
- L'Organisation internationale de Commission de Valeur (OICV) a également communiqué sur le risque spéculatif ;
- L'Autorité des Marchés Financiers (AMF) et l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) ont mis en garde les épargnants sur les risques d'investissement sur des actifs spéculatifs à forte appréciation et volatilité tels que le bitcoin[97].

La France, qui aspire à devenir une référence en tant que place d'innovation pour les blockchains, crypto-actifs et ICO, entend donc mettre en place un nouveau cadre réglementaire sécurisant pour le développement d'un écosystème français robuste.

Il convient de rappeler à titre liminaire que l'adoption en septembre 2018 de l'article 26 du projet de loi Projet de loi relatif à la croissance et la transformation des entreprises (dite loi PACTE) par l'Assemblée Nationale, ainsi qu'une partie de ses amendements, ne constitue que le point de départ du processus législatif du projet de loi PACTE qui pourra faire l'objet d'évolutions au gré des futures lectures effectuées dans le cadre du processus législatif.

L'Assemblée nationale a adopté le 28 septembre l'amendement n° 2492 rectifié de la loi PACTE, lequel propose entre autres une définition des actifs numériques comprenant les jetons ainsi que les crypto-actifs[98]. La définition d'actifs numériques qui est proposée permet de délivrer une appréciation nationale des notions de jetons et de crypto-monnaies. Le texte crée également deux nouvelles

97. Communiqué de presse AMF, Achats de Bitcoins : l'AMF et l'ACPR mettent en garde les épargnants, 4 décembre 2017 (hwww.amf-france.org/Actualites/Communiques-de-presse/AMF/annee-2017?docId=workspace%3A%2F%2FSpacesStore%2Fc2dfeaab-35c0-4fdf-9a1b-d4601eff2097).
98. Voir annexe.

catégories d'acteurs :

- Les émetteurs de jetons ;
- Les prestataires de services sur actifs numériques.

Enfin, le projet de loi PACTE tend également à lever l'une des principales difficultés pour les nouveaux acteurs du secteur des crypto-actifs : l'accès aux services bancaires. À ce titre, il est proposé de garantir un accès sans entraves aux services de comptes de dépôt et de paiement proposés par les établissements de crédit (i) aux émetteurs de jetons ayant obtenu le visa de l'AMF et aux Prestataires de services sur actifs numériques (qui seront enregistrés à auprès de l'AMF ou qui auront obtenu l'agrément de l'AMF).

1. ICO : pour une protection des acteurs et des investisseurs

Le projet de loi PACTE contient en son article 26 une proposition de réglementation des ICO. Le gouvernement souhaite ainsi protéger les investisseurs contre les abus qui se sont multipliés lors des ICO en mettant en place des contrôles, lesquels seraient effectués par l'AMF.

Par application de ce texte, constituerait donc un jeton « tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien ».

La mise en place d'une ICO (ou offre au public de jetons) consiste à proposer au public, sous quelque forme que ce soit, de souscrire à ces jetons. Préalablement à toute offre de jetons au public, les émetteurs de l'ICO peuvent solliciter un visa de l'Autorité des marchés financiers. Le visa de l'AMF, bien que non obligatoire puisque le choix est laissé aux émetteurs de le solliciter ou non, devrait être de nature à rassurer les investisseurs en leur permettant de distinguer les acteurs légitimes et à inciter ces derniers à mener leurs projets en France[99].

Les émetteurs qui auront demandé le visa de l'AMF devront satisfaire certaines exigences mises en place par le texte. L'Autorité des marchés financiers vérifiera si l'offre envisagée présente les garanties exigées d'une offre destinée au public et, notamment pour l'émetteur des jetons, sa constitution sous la forme d'une personne morale établie ou immatriculée en France, la communication à l'AMF du document d'information et des projets de communications à caractère promotionnel destinées au public, la mise en place de moyens permettant le suivi et la sauvegarde des actifs recueillis dans le cadre de l'offre, l'information des souscripteurs sur les résultats de l'offre et, le cas échéant, de l'organisation d'un marché secondaire des jetons. Ces obligations pourront être complétées à l'avenir par modification du règlement général de l'AMF.

Les dispositions du projet de loi PACTE assouplissent les conditions d'investissements dans les crypto-actifs en (i) créant un visa attestant du sérieux des ICO et en (ii) autorisant les fonds spécialisés à investir dans les crypto-actifs.

Recommandations

Pour développer la réglementation en matière d'ICO :

99. Projet de loi pour la croissance et la transformation des entreprises, Étude d'impact, p. 346.

- La possibilité de procéder à un cantonnement des fonds reçus pour le compte des utilisateurs sur un compte dédié, afin de préserver la sécurité des moyens de paiement ainsi fournis et de protéger les usagers, similaire à celui imposé par l'ACPR pour les établissements exemptés d'agrément soumis à déclaration ;
- La possibilité de disposer d'un compte sous la forme de compte de cantonnement/assurance/garantie aux fins pour les émetteurs, agréés ou non, de disposer d'un accès similaire aux services bancaires, tout en garantissant une séparation entre les biens propres de l'émetteur et ceux qu'il aurait recueillis à l'issue d'une ICO ;
- D'une manière générale, un élargissement du droit au compte octroyé aux émetteurs de jetons bénéficiant d'un visa de l'AMF à l'ensemble des plateformes.

Ces recommandations supposent intrinsèquement une clarification du statut juridique des échanges décentralisés et la mise en œuvre d'une coopération entre les autorités de régulation d'un côté et les différentes communautés de l'écosystème de la blockchain de l'autre.

2. Cryptoactifs et lutte anti-blanchiment/ financement du terrorisme

Le caractère anonyme des crypto actifs contribue malheureusement à son utilisation dans le cadre du financement d'activités criminelles et du contournement des règles relatives à la lutte contre le blanchiment des capitaux. En conséquence, les transactions effectuées en crypto actifs se voient soumises aux directives européennes relatives à la lutte contre le blanchiment et le financement du terrorisme (4e Directive de Lutte contre le Blanchiment des Capitaux et le Financement du Terrorisme, modifiée par la 5e Directive anti-blanchiment adoptée le 30 mai 2018).

La 5e Directive soumet donc aux obligations LCB-FT les acteurs proposant (i) des services d'échange de crypto-actifs contre de la monnaie ayant cours légal et (ii) les acteurs proposant la conservation pour le compte de leurs clients des clés cryptographiques privées permettant de détenir, stocker ou transférer les crypto-actifs.

Au-delà des risques LCB-FT, la conservation des crypto actifs est également sujette à des cyber risques importants et n'offre aucune protection en matière de sécurité de ces avoirs. Comme le souligne la Banque de France, il existe des risques avérés de piratage des portefeuilles électroniques permettant le stockage des crypto actifs. Dans ce contexte, les détenteurs n'ont aucun recours en cas de vol de leurs avoirs par des pirates informatiques.

Les épisodes répétés de fraudes importantes (piratage de Coincheck en janvier 2018 pour 534 millions de dollars, faillite en 2015 de MtGox 3, première plate forme mondiale d'échange de bitcoins), illustrent la vulnérabilité de l'écosystème des crypto actifs et le niveau élevé des risques associés, en l'absence de mécanismes de garantie[100].

Depuis 2014 en France, l'activité des plateformes de conversion des crypto actifs contre monnaie ayant cours légal, qui jouent le rôle d'intermédiaire entre acheteur et vendeur, est considérée comme un service de paiement[101] nécessitant un

100. https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_fr.pdf.
101. https://acpr.banque-france.fr/sites/default/files/20140101_acpr_position_bitcoin.pdf.

agrément de prestataire de service de paiement. Toutefois, comme rappelé en 2018, cette exigence découle du rôle d'intermédiaire et de la gestion pour le compte de tiers de comptes tenus et libellés dans une monnaie ayant cours légal, non de la prestation associée aux crypto-actifs à proprement parler.

Au-delà de cette approche, la Banque de France et l'ACPR[102] préconisent depuis quelque temps, un élargissement de l'encadrement réglementaire applicable aux prestations associées aux crypto-actifs, par la mise en place d'un statut de prestataires de services en crypto-actifs.

Ce sera donc chose faite avec le projet de loi PACTE qui vise à mettre en place un régime relatif aux intermédiaires sur les marchés des actifs numériques et à leur appliquer les dispositions de la cinquième directive relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme. Il tend à instaurer un environnement favorisant l'intégrité, la transparence et la sécurité des services concernés, tout en assurant un cadre réglementaire sécurisant pour le développement d'un écosystème français robuste.

Au-delà de la transposition de la directive anti-blanchiment, le projet de loi crée une nouvelle catégorie de prestataires financiers spécifique au secteur des crypto-actifs : les Prestataires de services sur actifs numériques.

Cette nouvelle catégorie de prestataires concerne les acteurs proposant les services sur actifs numériques suivants :

- Le service de conservation pour le compte de tiers d'actifs numériques ou d'accès à des actifs numériques, le cas échéant sous la forme de clés cryptographiques privées, en vue de détenir, stocker et transférer des actifs numériques (ex. : les wallets d'actifs numériques) ;
- Le service d'achat ou de vente d'actifs numériques en monnaie ayant cours légal ;
- Le service d'échange d'actifs numériques contre d'autres actifs numériques ;
- L'exploitation d'une plateforme de négociation d'actifs numériques ;
- Les services suivants : la réception et la transmission d'ordres sur actifs numériques pour le compte de tiers ; la gestion de portefeuille d'actifs numériques pour le compte de tiers ; la prise ferme d'actifs numériques ; le placement garanti/non garanti d'actifs numériques.

Les prestataires de services sur actifs numériques sont enregistrés par l'Autorité des marchés financiers qui vérifie si leurs dirigeants et leurs bénéficiaires effectifs possèdent l'honorabilité et la compétence nécessaires à l'exercice de leurs fonctions.

Pour la fourniture à titre de profession habituelle d'un ou plusieurs des services sur actifs numériques, les prestataires établis en France peuvent solliciter un agrément auprès de l'Autorité des marchés financiers. Cette faculté apporte une réponse pragmatique au défi posé par le marché émergent des crypto-actifs, tout en tenant compte du faible nombre d'acteurs présents en France à ce stade. Le caractère facultatif de l'agrément permet d'envoyer un signal positif quant à la capacité des autorités publiques à prendre en compte

102. https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_fr.pdf.

l'évolution rapide de ce marché et d'attirer d'ores et déjà les acteurs sérieux.

La délivrance de l'agrément sera assurée par un guichet unique auprès de l'AMF qui sollicitera l'avis de l'ACPR sur certaines questions. Les obligations imposées aux acteurs qui sollicitent l'agrément font l'objet de règles adaptées aux différents métiers visés, ce afin de tenir compte des risques et spécificités propres à chacun d'entre eux. La nomenclature des prestataires de services sur actifs numériques couvre en outre un large champ d'activités afin de permettre à un maximum d'acteurs de solliciter un agrément.

Dans un délai de deux ans à compter de la promulgation de la loi PACTE, le Gouvernement, après avoir recueilli les avis de la Banque de France, de l'Autorité de contrôle prudentiel et de résolution et de l'Autorité des marchés financiers, remettra au Parlement un rapport visant à évaluer la mise en œuvre des dispositions de la loi et notamment concernant la nécessité ou pas de rendre obligatoire l'agrément, au vu de l'avancement des débats européens et du développement international du marché des actifs numériques.

Recommandation

- La création d'un statut de prestataires de services sur actifs numériques permettant de les soumettre à des règles portant notamment sur la sécurité des opérations et sur la protection de la clientèle et la lutte contre les infractions BC-FT.

Protection des données

La blockchain, par son absence de centralisation et la multiplicité de ses acteurs, rend difficile la conformité au RGPD, mais surtout complexifie l'identification des rôles de chacun en matière de traitement de données.

La CNIL (Commission Nationale de l'Informatique et des Libertés) a communiqué en septembre 2018 ses premiers éléments d'analyse sur l'utilisation de la blockchain dans le contexte des données personnelles. Elle propose une réflexion sur trois questions, ponctuée de propositions techniques pour une mise en conformité optimale de l'utilisation de la technologie avec le cadre réglementaire existant.

À titre liminaire, il convient de rappeler les données à caractère personnel identifiées par la CNIL comme pouvant être contenues dans une blockchain[103].

- Les identifiants des participants et des mineurs, à savoir la suite de caractères alphanumériques constituant la clé publique du compte du participant. Bien qu'inutilisables sans leur association avec la clé privée que le participant est le seul à connaitre, les identifiants sont nécessairement publics pour permettre l'utilisation de la blockchain ;
- Les données complémentaires : toutes autres données complémentaires stockées sur la blockchain variant suivant l'objet de celle-ci (ex. : enregistrement de diplômes, cartes d'identité…).

i. La qualification des intervenants sur une blockchain à l'aune du RGPD

Le modèle décentralisé de la blockchain ainsi que la pluralité des acteurs intervenants sur cette dernière posent tout

103. www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles.

d'abord la question du rôle de chacun dans un contexte de traitement des données personnelles. En effet, la forme prise par la blockchain, son mode de gouvernance ou l'accès octroyé aux données font varier l'identification des personnes responsables du traitement.

À ce titre, la CNIL estime que le participant doit être qualifié de responsable du traitement dans deux situations :

- Lorsqu'il est une personne physique et que le traitement des données personnelles est une activité professionnelle ou commerciale (a contrario la personne physique ne saurait être qualifiée de responsable du traitement des données lorsque son activité sur la blockchain est strictement personnelle) ;
- Lorsqu'il est une personne morale et qu'il inscrit une donnée à caractère personnel sur la blockchain.

La CNIL estime de plus que les acteurs qui interagissent sur la blockchain ne doivent pas tous être qualifiés de responsables de traitement. Il convient en effet d'effectuer une analyse du rôle joué par l'intervenant dans la détermination des finalités du traitement et des moyens mis en œuvre pour l'exécution des traitements. Ainsi, la simple validation des transactions, effectuée par des mineurs, ne constitue pas un traitement de données.

La détermination des finalités joue un rôle prépondérant dans la qualification de responsable de traitement ou de sous-traitant. Ainsi, les développeurs de smart contracts traitant des données à caractère personnel pour le compte du responsable de traitement tendraient vers une qualification de responsables des données lorsqu'ils participent à la détermination des finalités. À défaut, les développeurs seraient qualifiés de sous-traitants s'ils participent au traitement, mais n'en détermine pas les finalités ou de simples fournisseurs de solution si leur rôle se limite à la conception de l'algorithme.

2. La gouvernance et l'inscription de la donnée : des choix primordiaux

Le choix de la forme de la blockchain (publique, privée ou hybride) n'est pas sans incidence. À ce titre, la CNIL souligne la difficulté dans le cadre des blockchains les plus ouvertes (publiques) de mettre en œuvre des clauses contractuelles types ou contraignantes, dans la mesure où le responsable des traitements peut difficilement exercer un contrôle sur les intervenants, qu'il s'agisse des utilisateurs ou des mineurs.

De plus, les participants peuvent être situés dans un pays en dehors de l'UE, soulevant des interrogations sur les difficultés tant de soumission que d'application aux règles particulières en matière de transfert hors UE. L'orientation de la gouvernance de la blockchain apparait donc comme stratégique pour la conformité au RGPD.

L'un des principaux caractères de la blockchain est son immuabilité. Ainsi, les données inscrites dans les blocs ne peuvent être techniquement modifiées ou supprimées. La CNIL identifie à ce sujet une difficulté quant à la compatibilité entre la blockchain et le principe de minimisation des données qui exigent une collecte pertinente et précise des données pour une durée de conservation déterminée.

À cet égard, la CNIL émet une recommandation sur la technique employée pour l'enregistrement. En effet, l'enregistrement des données sur une blockchain

au travers d'un enregistrement cryptographique[104] ou sous la forme d'une empreinte ou encore a minima d'un chiffré permettrait de garantir, à défaut d'une conservation déterminée, une confidentialité élevée de la donnée.

La CNIL énonce une exception possible à cet enregistrement contraignant des données lorsque (i) la finalité du traitement le justifie et (ii) qu'une analyse d'impact démontrerait que les risques résiduels seraient acceptables.

Ainsi, tant la gouvernance que l'inscription des données constituent des choix essentiels dans la création d'une blockchain, mais ne sauraient être généralisés. Chaque utilisation des données et de la blockchain est à apprécier au cas par cas.

3. L'assurance d'un exercice effectif de ses droits

La transparence de la technologie de la blockchain va dans le sens du droit à l'information des personnes, ainsi que le droit d'accès et le droit à la portabilité. Cependant, si la CNIL constate la compatibilité technique de la blockchain avec les droits énoncés précédemment, elle met également en avant l'impossibilité technique de mise en œuvre du droit à la demande d'effacement, sauf à ce que la donnée inscrite sur la blockchain soit un engagement cryptographique, une empreinte ou un chiffré. Dans ce cas, la donnée peut être rendue quasi inaccessible par le responsable du traitement.

De plus, s'agissant du droit à la demande de rectification, l'absence de possibilité de modification des données inscrites dans le bloc, le responsable de traitement doit procéder à la mise à jour des données par inscription de la donnée dans un nouveau bloc.

Enfin, s'agissant du droit à la limitation et à une intervention humaine, il serait possible d'en trouver une application dans l'utilisation de la blockchain au travers de *smart contracts*. En effet, ces derniers permettraient de prévoir en amont dans le programme une limitation, mais également d'imposer la possibilité d'une intervention humaine pour être exécutés.

Sont identifiées à ce stade comme points critiques suivants :

- La qualification de sous-traitant versus responsable de traitement ;
- La prévisibilité dès la mise en place de la blockchain du mode de gouvernance, des limitations, du mode d'enregistrement des données ainsi que des options des smart contracts le cas échéant, en fonction de la forme de la blockchain publique/privée ;
- Un respect aménagé du RGPD à défaut d'une conformité pleine et entière ;
- La proposition de guidelines dès la création de la blockchain pour une protection des données.

Preuve digitale et responsabilité

1. Preuve

Une des applications les plus prometteuses la technologie blockchain est l'utilisation des registres qu'elle déploie, lesquels sont en théorie immuables et infalsifiables aux fins d'enregistrer et de mettre à disposition des preuves horodatées irréfutables. Les mises en application se multiplient pour la certification de diplômes, la gestion de cadastres, le dé-

104. Un « engagement cryptographique » est un mécanisme qui permet de figer une donnée de telle sorte qu'il soit possible, avec des éléments supplémentaires, de prouver ce qui a été figé, et à la fois impossible de la retrouver ou de la reconnaître à partir de cette seule version « engagée ».

pôt de brevets, etc.
Cependant, il demeure aujourd'hui des incertitudes sur la valeur juridique de ces preuves enregistrées sur des blockchains.

1. Réglementation existante

La réglementation existante permet d'ores et déjà d'aborder la technologie blockchain :

- L'article 1366 du Code civil dispose que *« l'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »*. L'intégrité et l'identification de l'utilisateur sont deux éléments pouvant être attestés par la blockchain, dans ce cas, les éléments enregistrés sur la blockchain pourraient constituer des preuves électroniques au sens du Code civil.
- Les conventions de preuve permettant aux parties signataires de modifier les règles de preuve (charge de la preuve, objet de la preuve, modes de preuves) si ces dernières sont valablement conclues. Cet accord entre les parties n'exclut pas une référence à un protocole électronique comme mode de preuve et pourrait dès lors faire référence à une blockchain comme système attestant par exemple de la réalité de leur engagement ou de la réalisation d'une transaction.
- Les minibons sont des bons de caisse spécialement conçus pour le financement participatif. Au regard des dispositions qui précèdent, la blockchain (« dispositif d'enregistrement électronique ») sert de preuve pour deux finalités différentes :
  - En tant que preuve d'inscription dans un registre, les bons de caisse sont inscrits au nom de leur propriétaire dans une blockchain ;
  - En tant que preuve du transfert de propriété, la simple inscription de la cession dans le dispositif tient lieu de contrat de cession.
- S'agissant des titres financiers, le Code monétaire et financier prévoit depuis l'ordonnance du 8 décembre 2017 que tous les titres financiers non cotés sur Euronext ou Alternext peuvent désormais être représentés ou transmis par la blockchain avec les mêmes effets que l'inscription en compte de titres financiers, bien que la blockchain ne soit pas un compte titre. La France est ainsi le premier pays européen qui encadre par voie législative l'inscription et le transfert de titres non cotés par blockchain, en faisant de cette technologie un support de preuve de l'existence et du transfert de ces derniers.

Ainsi, le législateur a d'ores et déjà intégré la technologie de la blockchain dans sa fonctionnalité de registre partagé.

2. Proposition(s)

La loi PACTE a tenté d'être force de proposition aux fins de conférer à la blockchain davantage de valeur probatoire. En effet, un amendement, malheureusement retiré avant discussion, avait été déposé pour clarifier la valeur juridique des preuves enregistrées sur un dispositif électronique d'enregistrement partagé. Cet amendement visait à reconnaître la valeur de preuve à tout fichier numérique enregistré dans une blockchain, de nature publique ou privée, afin de sécuriser les opérations effectuées par les entreprises utilisant cette technologie.
La France est pionnière dans la reconnaissance de l'inscription sur la blockchain comme une preuve, mais cette consé-

cration demeure circonscrite à une minorité de domaines. Afin de favoriser et de protéger l'expérimentation des entreprises, il conviendrait d'élargir le spectre des domaines de reconnaissance de la blockchain comme mode de preuve.

Recommandation

- La reconnaissance générale de preuve de l'inscription d'éléments dans la blockchain, que ce soit en tant que preuve entre les parties que de preuve judiciaire pouvant être soumise à l'appréciation du juge lors d'un litige.

2. Smart contracts

Il convient de rappeler que les *smart contracts* ne constituent pas des contrats au sens juridique du terme. Un *smart contract* est en effet un logiciel ou un protocole informatique permettant l'exécution automatique d'une action (sans intervention humaine) pouvant être déterminée par un contrat. Dès lors, bien que les *smart contracts* ne constituent pas des engagements contractuels, ils possèdent des implications avec le droit des contrats de deux façons :

- Soit le *smart contract* est le support d'exécution d'un contrat préalablement établi ;
- Soit l'exécution du contrat au travers du *smart contract* implique des questions de responsabilité contractuelle ou de loi applicable par exemple.

Le recours à ces outils pourrait permettre une gestion automatique de certains contrats de financement (crédit, leasing ou location) ou encore l'exécution de polices d'assurance. En effet, à la survenance d'un évènement déterminé, le smart contract pourrait enclencher le remboursement automatique de l'assuré.

À ce titre, il est important de mettre en avant que l'exécution d'un *smart contract*, par son automaticité et son immuabilité sur la blockchain, peut impliquer des conséquences malheureuses en cas de changement dans la situation des parties. Cependant, le smart contract demeurant un programme informatique, ses caractéristiques peuvent évoluer dès lors que celles-ci sont programmées à l'avance. Afin de garantir une exécution du *smart contract* souple et répondant à la volonté des parties, la possibilité d'intégrer dans sa programmation toutes les options possibles, notamment pour faire évoluer l'exécution en fonction de l'évolution de la relation contractuelle, doit être prise en compte au moment de la rédaction du protocole algorithmique.

Recommandations

- Rédiger un guide d'utilisation proposant des recommandations d'actions et des pièges à éviter, permettant d'établir un *smart contract* personnalisé en fonction de chaque application et chaque partie ;
- Structurer une arborescence évolutive des conséquences du *smart contract* avant l'implémentation et en fonction des chemins effectués lors de l'exécution ;
- Établir des clauses types à intégrer dans un *smart contract* au sein d'une banque de clauses afin de compléter le catalogue des recommandations pour garantir une utilisation éclairée de ces protocoles informatiques.

3. Responsabilité

La responsabilité varie nécessairement en fonction de la forme de la blockchain choisie. Dans le cas d'une blockchain privée, les intervenants sont identifiés, voire sélectionnés. À l'inverse, dans une

blockchain publique n'importe quel utilisateur contribue à la construction du réseau. Ainsi, l'identification des membres du réseau et de leurs responsabilités en cas de fraude ou de bug dans l'utilisation de la blockchain serait nécessairement différente en fonction de sa typologie.

Plusieurs questions en matière de responsabilité doivent être soulevées et qui ne comportent à ce jour pas de solutions claires.

Tout d'abord, la sécurité dans l'utilisation de la blockchain repose sur son fonctionnement basé sur le consensus pour la validation des transactions. Par hypothèse, le réseau pourrait accepter une transaction frauduleuse dès lors qu'elle présente toutes les caractéristiques matérielles nécessaires à cette validation. Il peut être soulevé ici la question de la responsabilité du réseau. Or, ce dernier n'ayant pas de personnalité morale, se pose alors une seconde question sur la responsabilité qui pourra être effectivement engagée, et contre quel membre du réseau.

Une autre question de responsabilité est celle qui devra être soulevée en cas de défaut ou dénouement malheureux d'un *smart contract*. En effet, l'exécution automatique de ce dernier entraîne, dans le cas d'une cession par exemple, un transfert direct de l'actif ou du jeton concerné dès que les conditions de son exécution sont réunies. Une solution pour permettre le contrôle de ce transfert est d'ajouter des règles au sein du *smart contract* pour encadrer davantage ce transfert automatique, ou du moins prévoir dans le protocole automatique une faculté de restitution si certaines conditions sont remplies. Enfin, les interrogations en matière de responsabilité se cristallisent autour de l'engagement effectif de celle-ci. En effet, pour engager la responsabilité d'une partie, encore faut-il connaître la juridiction compétente, et qu'une voie de recours soit ouverte. Or, la technologie blockchain étant internationale et transfrontalière à la différence des juridictions et des législations, des points de rattachement à un État et à ses instances juridictionnelles devront être déterminés pour permettre de tels recours.

Recommandation

- L'insertion dans le *smart contract* d'éléments allant dans le sens d'un rattachement à une juridiction ou un droit applicable particulier, à défaut de prise de position par les états ou les instances internationales sur ces points,

Une réglementation

adaptée à l'innovation (« compétitivité »)

Accès au marché et concurrence

Une réglementation adaptée à l'innovation se doit de garantir l'accès au marché et maintenir une concurrence entre les acteurs. Ainsi, alors que certaines blockchains se positionnent comme des concurrents directs au secteur bancaire et financier, les dispositions permettant l'ouverture d'un compte au sein des banques françaises pourraient restreindre la possibilité pour ces néo-acteurs de s'implanter. En effet, il peut être imaginé que par excès de zèle dans l'application de la réglementation, certaines institutions refusent le droit à l'ouverture de compte afin de limiter la concurrence. Il convient à ce titre de mettre en place des garde-fous pour maintenir l'innovation et la diversité des acteurs dans ce domaine.

De plus, l'attractivité et le développement de la France comme un acteur incontournable de l'implantation des structures blockchain impliquent de valoriser les compétences existantes. Ainsi, les entreprises comme Ledger, relocalisant sa production physique de coffres-forts en France du fait de ses compétences en matière de sécurité, doivent être mises en avant et protégées. De la même manière, des structures telles que Lightning, proposant une alternative moins consommatrice d'énergie, fluidifiant les transactions du bitcoin et délivrant une réponse aux questions environnementales de la blockchain, doivent être captées et voir leur développement encouragé.

Recommandations

Elles peuvent être faites au titre de l'accès au marché et de la concurrence et s'articulent autour de l'ambition des initiatives législatives pour faire de la France un pôle attractif de l'innovation. À ce titre, il apparait important d'inciter l'installation en France sous différentes formes telles que la simplification des formalités administratives, l'incitation fiscale, la possibilité de bénéficier d'un crédit d'impôt conditionné par l'innovation ou plus simplement de bénéficier de subventions pour que les communautés blockchain soient domiciliées en France.

Harmonisation législative

L'harmonisation législative au niveau international, et surtout européen, est un enjeu majeur. Il est difficile d'appréhender des relations et des situations d'échanges pour lesquelles les juridictions compétentes et le droit applicable n'existent pas encore, mais dont les implications sont planétaires. Il existe de plus un risque de « forum shopping[105] » en matière de réglementation.

Certains États européens se dotent actuellement de législations attractives pour les membres de la communauté blockchain, pouvant entraîner une fuite de ses acteurs, mais également une augmentation du risque juridique. À titre d'exemple, Malte dispose de trois projets de loi couvrant les trois principaux piliers de la réglementation nécessaire afin de lui

105. Le forum shopping (élection de juridiction) est une pratique de droit international privé qui consiste à saisir la juridiction la plus susceptible de donner raisons à ses propres intérêts (Wikipédia).

permettre de devenir l'eldorado de la technologie blockchain et des crypto-monnaies (régime de registre, place blockchain en collaboration avec l'autorité des marchés financiers maltaise, réglementation des monnaies virtuelles).

Enfin, l'Autorité des services financiers de Malte (MFSA) a publié des documents concernant la mise en place d'un « Test d'instrument financier » pour définir la nature des jetons vendus lors d'une ICO. Bien que ces dispositions soient similaires à celles prévues par le droit français, il peut être constaté la mise en œuvre d'une pluralité de réglementations au sein de l'UE sur le sujet blockchain, pouvant mener à une concurrence entre les États.

Afin d'assurer une meilleure efficacité de la réglementation, il apparait souhaitable de développer une coordination européenne et internationale. Compte tenu du caractère dématérialisé des crypto-actifs et de l'utilisation de technologies liées au monde de l'internet qui facilitent la fourniture de services de façon transfrontalière, l'hétérogénéité des règlementations nationales pourrait empêcher une pleine maîtrise des risques induits.

Ainsi, il apparaît nécessaire aujourd'hui de porter le débat sur la régulation des crypto-actifs au niveau international. Le 7 février 2018, les ministres de l'Économie et des Finances et les banquiers centraux français et allemands ont saisi le G20 à cet effet.

La démarche principale, avant même que ne soit proposée une harmonisation législative au niveau international ou européen, demeure celle de la coopération entre les autorités de régulation et les différentes communautés de l'écosystème des blockchains.

L'adéquation des

règles fiscales et comptables

Fiscalité

La fiscalité des crypto-actifs (aujourd'hui intégrée dans une directive de 2014, partiellement annulée en 2018) et a été revue dans la loi de Finance 2019 (article 41) et ne taxe les gains qu'au moment de la cession et en distinguant les revenus réguliers des revenus occasionnels.

L'analyse qui avait été délivrée par l'administration fiscale s'agissant du bitcoin permettait de penser qu'elle pourrait s'appliquer à l'ensemble des crypto-monnaies. En matière de réalisation de profits, il convient de distinguer si les transferts s'effectuent entre personnes physiques ou personnes morales.

Dans le premier cas, la qualification varie en fonction de l'habitude de la réalisation de telles opérations. Ainsi, la réalisation de profits au travers de ces monnaies serait considérée comme un BIC si l'échange est réalisé à titre habituel ou de BNC si celui-ci est réalisé à titre occasionnel.

Dans le second cas, si les opérations sont réalisées par une personne morale, hypothèse qui pourrait être retenue pour les groupements de mineurs, le régime fiscal serait alors celui de l'IS. Cependant, la revente de crypto-monnaie ne pourrait pas bénéficier du régime des plus-values à long terme. La loi de finance 2019 précise dès lors le régime fiscal :

- Les plus-values réalisées à titre occasionnel par les particuliers lors de la cession d'actifs numériques font l'objet d'une imposition forfaitaire à un taux de 30 % (dont 12,8 % d'impôt sur le revenu) ;
- les cessions n'excédant pas 305 euros par an sont exonérées d'impôt ;
- Les échanges sans soulte entre crypto-monnaies n'entraînent normalement pas d'imposition,

Les gains de « minage » et d'achat-revente à titre habituel ne sont pas directement concernés par cette nouvelle mesure et devraient rester imposés respectivement dans la catégorie des BNC et des BIC.

Les personnes physiques, les associations et les sociétés n'ayant pas la forme commerciale, domiciliées ou établies en France, sont tenues de déclarer, en même temps que leur déclaration de revenus ou de résultats, les références des comptes d'actifs numériques mentionnés à l'article 150 VH bis ouverts, détenus, utilisés ou clos auprès d'entreprises, personnes morales, institutions ou organismes établis à l'étranger. En matière de soumission des opérations sur crypto-monnaies à la TVA, il y a aujourd'hui une absence de position de l'administration fiscale, et cela, quelle que soit la crypto-monnaie. Une hypothèse peut être avancée selon laquelle les opérations au travers de crypto-monnaies pourraient être considérés comme occasionnelles par Bercy, ce qui les exclurait naturellement du champ d'application de la TVA.

La Cour de Justice de l'Union Européenne (CJUE), dans son arrêt du 22 octobre 2015 « David Hedqvist[106] », a apprécié les opérations réalisées par conversion de monnaie nationale en bitcoin comme bénéficiant de l'exonération de TVA dès lors que les

106. https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128fr.pdf.

opérations sur devises non traditionnelles constitueraient des opérations financières. Cette appréciation vaut uniquement pour le bitcoin pour des services consistant en l'échange de devises traditionnelles contre la devise virtuelle bitcoin. Il ne précise pas le traitement TVA des transactions dont le bitcoin est le moyen de paiement.

Recommandation

L'administration fiscale doit établir des règles claires afin que les transactions impliquant des crypto-actifs puissent bénéficier de la même sécurité juridique que les autres transactions.

Comptabilité

L'intégration par la comptabilité de la technologie de la blockchain comme support et outil est au cœur des préoccupations de l'ANC, laquelle a mis en place d'un groupe de réflexion sur la blockchain et la comptabilité par l'ANC : thème des 7e états généraux de la recherche comptable de l'ANC.

Certains constats apparaissent au titre de cette réflexion. Ainsi, il a pu être souligné que la transformation numérique de l'économie, au-delà des opportunités qu'elle génère, fait face à un problème de reconnaissance comptable et de financement de ses activités. Certes, la comptabilité peut répondre en partie sur les aspects « reconnaissance », mais, à ce stade, il semble que des indicateurs extracomptables doivent être également mis en place afin de mieux refléter les opérations liées à l'activité du numérique. Cela pourrait laisser la place à une « normalisation élargie » dont les frontières restent à définir. L'acquisition des données (big data) par les différents acteurs de l'économie du numérique semble au cœur du sujet.

L'ANC vient de publier le règlement N° 2018-07 du 10 décembre 2018[107] modifiant le règlement n° 2014-03 relatif au plan comptable général modifié. Ce règlement se prononce sur le traitement des jetons qu'il définit comme étant « tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits, pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien ». À noter toutefois qu'il reste à préciser le traitement des fourches[108], des airdrops[109] et des jetons mixtes[110].

Recommandation

- Proposer des indicateurs comptables et extracomptables permettant de donner une image fidèle des opérations liées à l'activité du numérique, avec une normalisation qui devrait posséder un caractère international au vu des implications mondiales de la technologie blockchain.

3.8 CONCLUSION

107. Règlement homologué par arrêté du 26 décembre 2018 publié au Journal Officiel du 30 décembre 2018.
108. Une fourche est un événement qui se produit lorsque le code source d'une blockchain existante est modifié, puis scindé en une nouvelle blockchain. La fourche la plus connue est celle de la crypto-monnaie litecoin qui est basée sur la blockchain bitcoin, copiée et modifiée afin que le placement du litecoin puisse être indépendant.
109. Un *airdrop* (largage) est la distribution, généralement gratuite, de jetons d'un cryptoactif afin d'attirer de nouveaux utilisateurs.
110. Forme mixte ou hybride des trois types de jetons existants : les jetons de paiement (cryptomonnaie « pure »), les jetons d'usage/*utility tokens* et les jetons d'investissement/*security tokens*.

Les initiatives se multiplient pour mettre en place un cadre réglementaire, juridique fiscal et comptable adéquat pour les nouveaux usages basés sur les technologies blockchains. Ces initiatives ne se limitent d'ailleurs pas à la France ou à l'Europe et sont partagées mondialement, que ce soit via le rattachement à des réglementations existantes (p. ex. cas des États-Unis), des réglementations ad hoc (France et Malte), la mise en place d'environnements de tests (Suisse) ou bien l'interdiction simple (Chine ou Corée). Cependant, cet effort de réglementation doit être approfondi aux fins de couvrir des thématiques plus larges et de s'inscrire dans une dynamique de stimulation de l'innovation. Certains freins propres aux acteurs demeureront, comme les contraintes de mises à l'échelle, de protection de la vie privée et des données personnelles. Malgré tout, un équilibre doit être trouvé entre protection et incitation.

De plus, cette dynamique d'encadrement de la blockchain ne doit pas être faite au détriment de l'attractivité d'un cadre juridique qui serait trop contraignant. En effet, un décalage peut être constaté entre ces nouvelles règles, visant à ne pas brider l'innovation tout en protégeant les investisseurs, et les recommandations des principaux acteurs et experts. Ces écarts sont accentués par la faible maturité de ces technologies et la vitesse de leurs évolutions qui complexifient d'autant la compréhension et la capacité à légiférer à temps.

L'importance et le potentiel des blockchains doivent en revanche ne jamais être perdus de vue afin que nos entreprises puissent poursuivre leurs activités et expérimentations et maintenir leur compétitivité à l'échelle internationale.

À ce titre, il convient de soulever une dernière interrogation sur l'infrastructure supportant une blockchain. En effet, bien que dématérialisée, la blockchain repose avant tout sur la création d'algorithmes et une technique de minage. Or, pour l'heure, les structures physiques supportant l'émergence et le développement de cette technologie ne se situent pas sur le territoire national, mais à l'étranger. Le développement d'applicatifs sur les technologies ne saurait garantir la souveraineté nationale si l'infrastructure technique peut être à tout moment contrôlée, saisie ou arrêtée par des puissances étrangères, étatiques ou économiques. La France doit disposer au sein de ses territoires de centres de développement algorithmiques, de fermes de minage, de centres de stockage de données et nuage/cloud, etc.

La France possède une opportunité de leadership sur les applications blockchain. Elle peut, grâce aux régimes optionnels mis en place, faciliter l'émergence de plateformes DLT intermédiaires en crypto-actifs et qui soient leaders mondiaux sur les applications métiers. Pour cela, le pragmatisme devra guider ses décisions en matière de fiscalité afin de ne pas freiner une innovation aussi disruptive qu'Internet il y a près de 30 ans. À ce propos, il est bon de noter que ne pas reproduire les erreurs commises à l'époque du Minitel et des débuts d'Internet est en substance la conclusion du rapport de la mission d'information sur la blockchain[111] présenté le 12 décembre 2018. Celui-ci préconise notamment de lancer des expérimentations dans l'administration et de redéployer, à l'occasion de

111. Rapport de la mission d'information commune sur les chaines de blocs (blockchain) présenté par Mme Laure de La Raudière et M. Jean-Michel Mis (décembre 2018).

la loi de finances 2020 si la proposition est retenue par le Gouvernement, 500 millions d'euros dans le secteur sur trois ans pour faire de la France une « blockchain nation ».

Cette question de compétitivité entre les pays se pose d'autant plus que les futures problématiques de la blockchain ne porteront pas sur la sécurité, mais sur l'empreinte énergétique de telles technologies. Or, l'utilisation de fermes de minage étrangères faisant fonctionner des ordinateurs hors d'âge et gourmands en électricité constituera à terme un problème à la fois économique et éthique.

Il existe actuellement des solutions allant dans ce sens, telle que la technologie développée notamment par Lightning permettant de développer une « deuxième couche » qui fonctionne sur une blockchain (le plus souvent bitcoin). Elle permet théoriquement des transactions rapides entre les nœuds participants avec une consommation énergétique moindre. Le développement de telles applications et le maintien de l'attractivité sur le sol français des architectures physiques de la blockchain seront les enjeux de demain pour notre indépendance tant politique qu'énergétique.

Annexes

Annexe 1. Glossaire

Transaction : étape élémentaire de changement d'état dans le cadre d'une procédure.
Bloc : Structure des données regroupées pour un traitement global. Le bloc contient les données et un en-tête.
Chaîne de blocs (blockchain) : registre distribué avec des blocs contrôlés, validés et structurés par seuls ajouts, l'ordonnancement étant assuré par des liens cryptographiques.
Système distribué : système avec des composants portés par un réseau d'équipements informatiques avec des procédures de coordination entre les nœuds du réseau pour assurer un objectif commun.
Registre (ledger) : données stockées de façon définitive et généralement la représentation numérique de transactions.
Registre distribué : système d'enregistrement des données issues de transactions géré par plusieurs nœuds (en écriture/lecture) avec un mécanisme de coordination entre les nœuds assurant la synchronisation des données.
Nœud : élément du réseau de pairs qui portent une chaîne de blocs avec des rôles, des propriétés et des responsabilités définies par la gouvernance de la chaîne de blocs.
Plateforme avec une technologie de registre distribué : ensemble d'équipements et de logiciels assurant les stockages et les traitements associés à une chaîne de blocs.
Consensus : accord entre les nœuds du réseau portant la chaîne de blocs sur la validité d'une transaction et sur l'ordonnancement des blocs ajoutés dans la chaîne.
Mécanisme de consensus : règles et procédures définissant la méthode d'obtention du consensus entre les parties prenantes d'une chaîne de blocs.
Gouvernance : règles implicites ou explicites, pouvant se mettre en œuvre par l'intermédiaire de logiciels exécutés par les nœuds, dirigeant et contrôlant l'usage et les fonctionnalités d'une chaîne de blocs. Elle est le cadre de référence des droits et responsabilités des parties prenantes avec pour objectif d'encourager un comportement souhaitable de ces dernières.
Avec permission/de consortium (*permissioned*) : chaîne de blocs où la participation au mécanisme de consensus est soumise à autorisation.
Ouverte/publique (*permissionless*) : chaîne de blocs où la participation au mécanisme de consensus n'est soumise à aucune autorisation.
Chaîne de blocs privée : chaîne de blocs où les rôles des parties prenantes sont définis et autorisés par une autorité.
Chaîne de blocs publique : chaîne de blocs où les rôles des parties prenantes sont définis par une gouvernance implicite sans autorité ni contrôle a priori.
Minage : activité d'un participant au consensus d'une chaîne de blocs consistant à conserver le contenu de la chaîne et vérifier le contenu d'un nouveau bloc et son ajout à la chaîne en respectant les protocoles définis.
Gratification : distribution d'un jeton associé à la chaîne de bloc accordée lors de la validation d'un bloc ajouté à la chaîne. Elle assure la cohésion des parties prenantes qui garantissent la conformité des données ajoutées et le maintien de la chaîne de blocs.
Actif digital : actif numérique représenté sous forme unique par un jeton pouvant être géré par une chaîne de blocs (création, transferts de propriété, destruction).
Fourche (*fork*) : création de deux chaînes devenant définitivement indépendantes à partir d'une chaîne de bloc initiale.
Immuabilité (*immutable*) : caractéristique d'une chaîne de blocs dont les enregistrements ne peuvent qu'être ajoutés sans possibilité d'annulation ou d'effacement par des moyens usuellement connus.
Hors chaîne (*off-chain*) : opérations (stockage, traitements) réalisées hors des nœuds de

la chaîne.
Dans la chaîne (*on-chain*) : opérations réalisées par les nœuds de la chaîne dans le cadre du mécanisme de consensus.
Oracle : service assurant l'accès à des informations externes pour les nœuds d'une chaîne de blocs.
Smart contract : programme informatique enregistré dans un registre distribué et exécuté sur une chaîne de blocs avec un mécanisme de consensus gérant son exécution et enregistrant ses effets dans la chaîne de blocs.
Jeton (*token*) : représentation d'un actif numérique dont un système assure sa gestion (création, transferts, destruction) ; une chaîne de blocs peut assurer cette gestion de façon distribuée.

Annexe 2. Liens pour approfondir le sujet

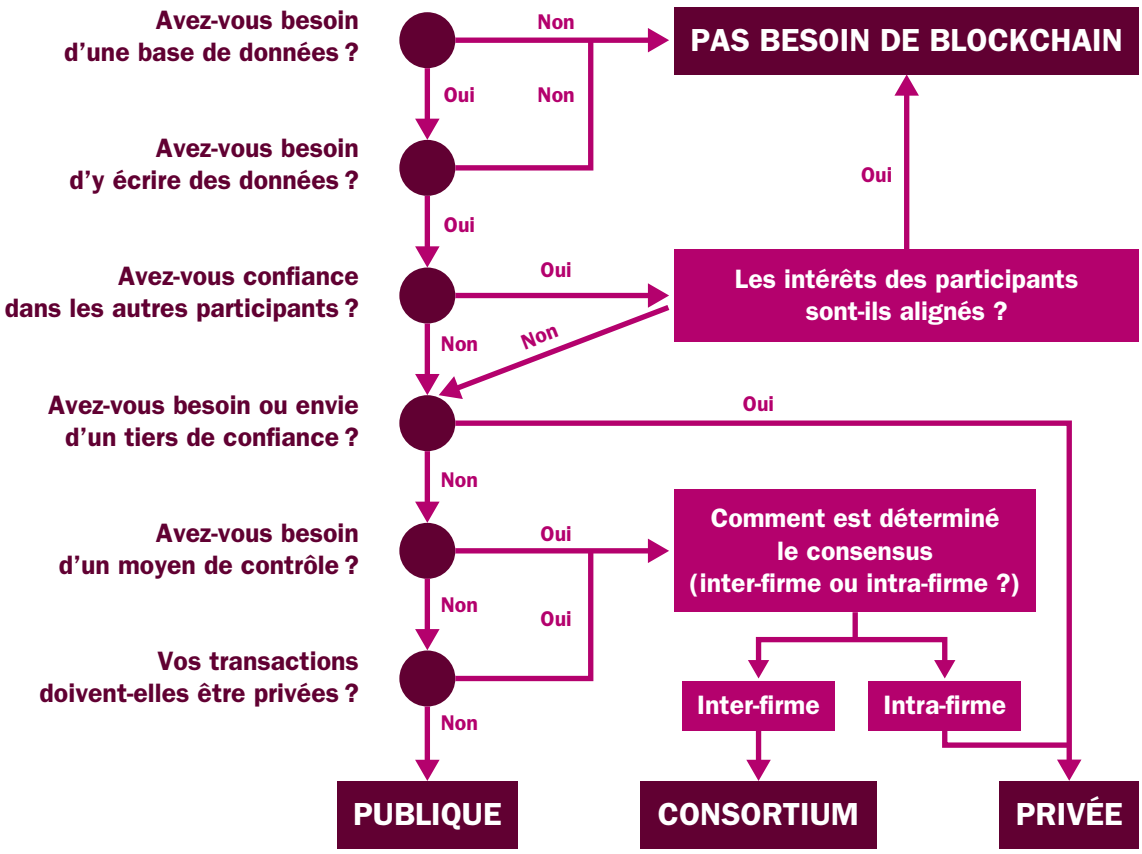
- http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf
- www.gartner.com/smarterwithgartner/the-cios-guide-to-blockchain
- www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
- www.weforum.org/agenda/2015/12/how-blockchain-technology-could-change-the-world
- www.cigref.fr/wp/wp-content/uploads/2017/06/Livre-blanc-Blockchain-pour-entreprises.pdf
- https://systematic-paris-region.org/wp-content/uploads/2017/07/Systematic-LB-Blockchain-HD.pdf
- www.louisbachelier.org/lecteur-pdf/?pid=52647
- www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf
- www.institutsapiens.fr/wp-content/uploads/2018/02/Note-Bitcoin-07-f%C3%A9vrier.pdf
- www.thedigitalnewdeal.org/wp-content/uploads/2017/06/the_digital_new_deal-org-JEANNEAU-Clement-LAge-DuWebDecentralise.pdf
- https://hbr.org/2017/01/the-truth-about-blockchain
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2977811
- www.annales.org/ri/2017/ri_aout_2017.html
- www.telecom-paristech.org/article/revue-telecom-183-drones-jusqu-ou-nous-emmenent-ils-blockchain-la-nouvelle-revolution-numerique/22/12/2016/2307
- www.thedigitalnewdeal.org/wp-content/uploads/2017/06/the_digital_new_deal-org-JEANNEAU-Clement-LAge-DuWebDecentralise.pdf
- www.anc.gouv.fr/files/live/sites/anc/files/contributed/ANC/1.%20Normes%20françaises/Reglements/2018/Reglt_2018_07/2018-07_%20recueil_ICO_.pdf

Annexe 3. Benchmark des solutions blockchain

Les grandes différences intrinsèques entre blockchain doivent être fortement monitorées pour répondre aux besoins. Une blockchain publique permettra d'utiliser les réseaux existants, mais soulèvera des problèmes de confidentialité, d'utilisation utilisateur par les clients et de protection des clés privées contre les attaques.

Les blockchains privées et de consortium ont l'avantage d'offrir un contrôle plus strict, mais présentent un niveau de sécurité généralement inférieur, un coût de maintenance plus élevé et peuvent être compliquées à déployer avec des entreprises parfois concurrentes et aux agendas et stratégies divergents.

Annexe 4. Benchmark de quelques solutions blockchain



	Bitcoin	Ethereum	Ripple	Consortium R3 Corda	Hyperledger Fabric	Hyperledger Sawtooth
Publique	Oui	Oui	Oui	Non	Non	Non
Open Source	Oui	Oui	Seulement en partie	Oui	Oui	Oui
Asset	Oui BTC	Oui ETH	Oui XRP	Non	Non	Non
Consensus	PoW	PoW/PoS	Ripple Protocol Tolérance aux fautes Byzantines en pratique (PBFT)	Pluggable uniqueness service	Tolérance aux fautes Byzantines en pratique (PBFT)	Proof of elapsed Time
Smart Contract	Non	Oui (EVM)	Non	Oui	Oui (chaincode)	Oui (transaction families)
Version entreprise	N/A	N/A Quorum	Oui	Oui	Oui	Prévue
Ownership	Crown-founded	Crown-founded	Fondateurs et venture capitalistes	Consortium de banques	Communautaire, Open Source	Communautaire, Open Source

Annexe 5. Textes « Enjeux réglementaires »

Amendement n° 2492, article 26 de la loi PACTE (adopté en première lecture par l'Assemblée nationale)

Pour l'application du présent chapitre, les actifs numériques comprennent :

1° Les jetons mentionnés à l'article L. 552-2 du présent code, à l'exclusion de ceux remplissant les caractéristiques des instruments financiers visés à l'article L. 211-1, et des bons de caisse visés à l'article L. 223-1 ;

2° Toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement.

Art. L. 549-26. – Les services sur actifs numériques comprennent les services suivants :

1° Le service de conservation pour le compte de tiers d'actifs numériques ou de clés cryptographiques privées, en vue de détenir, stocker et transférer des actifs numériques ;

2° Le service d'achat ou de vente d'actifs numériques en monnaie ayant cours légal ;

3° Le service d'échange d'actifs numériques contre d'autres actifs numériques ;

4° L'exploitation d'une plateforme de négociation d'actifs numériques ;

5° Les services suivants :

a) La réception et la transmission d'ordres sur actifs numériques pour le compte de tiers ;

b) La gestion de portefeuille d'actifs numériques pour le compte de tiers ;

c) Le conseil aux souscripteurs d'actifs numériques ;

d) La prise ferme d'actifs numériques ;

e) Le placement garanti d'actifs numériques ;

f) Le placement non garanti d'actifs numériques.

Un décret précise la définition des services mentionnés au présent article.

Présentation de l'article 26 de la loi PACTE

Dans l'attente de règles européennes et internationales, nécessaires sur ces sujets par nature transnationaux, il apparaît souhaitable, pour mieux protéger les acquéreurs de jetons et les porteurs de projets « légitimes », de permettre à l'AMF de délivrer un visa aux acteurs qui souhaiteraient émettre des jetons destinés notamment au marché français pour le financement d'un projet ou d'une activité, sous réserve qu'ils respectent certaines règles de nature à éviter des abus manifestes et à informer et protéger l'investisseur. L'AMF se verrait ainsi confier le soin d'examiner les documents élaborés par les émetteurs de jetons en amont de leur offre (« white paper »). Elle pourrait en outre exiger que les émetteurs se dotent d'un statut de personne morale établie ou immatriculée en France, mettent en place un mécanisme de séquestre des fonds recueillis, ou tout outil d'effet équivalent et un dispositif d'identification et de connaissance du client.

Amendement n° 1914, article 26 de la loi PACTE (adopté en première lecture par l'Assemblée nationale)

13° Après le premier alinéa de l'article L. 312-23, est inséré un alinéa ainsi rédigé :

« Les établissements de crédit mettent en place des règles objectives, non discriminatoires et proportionnées pour régir l'accès des émetteurs de jetons ayant obtenu le visa mentionné à l'article L. 552-4 du présent code aux services de comptes de dépôt et de paiement qu'ils tiennent. Cet accès est suffisamment étendu pour permettre à ces personnes de recourir à ces services de manière efficace et sans entraves. »

Position 2014-p-01, le 29 janvier 2014 sur les opérations sur bitcoins en France

Dans le cadre d'une opération d'achat/vente de bitcoins contre une monnaie ayant cours légal, l'activité d'intermédiation consistant à recevoir des fonds de l'acheteur de bitcoins pour les transférer au vendeur de bitcoins relève de la fourniture de services de paiement. Exercer cette activité à titre habituel en France implique de disposer d'un agrément de prestataire de services de paiement (établissement de crédit, établissement de monnaie électronique ou établissement de paiement) délivré par l'ACPR.

La délivrance de cet agrément impose le respect de conditions relatives notamment aux apporteurs de capitaux, à la gouvernance, à la structure financière et au niveau de fonds propres. Elle impose également que les entreprises agréées mettent en place (i) un dispositif de contrôle interne et (ii) des mesures de vigilance en matière de lutte contre le blanchiment et le financement du terrorisme, adaptés à l'activité exercée et aux risques encourus.

Code monétaire et financier, sur les minibons

Art. L. 223-12 : Sans préjudice des dispositions de l'article L. 223-4, l'émission et la cession de minibons peuvent également être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations, dans des conditions, notamment de sécurité, définies par décret en Conseil d'État.

Art. L. 223-13 : Le transfert de propriété de minibons résulte de l'inscription de la cession dans le dispositif d'enregistrement électronique mentionné à l'article L. 223-12, qui tient lieu de contrat écrit pour l'application des articles 1321 et 1322 du Code civil.

Amendement retiré, article 26 loi pacte

Après l'article 40, insérer l'article suivant :

Après l'unique alinéa de l'article 1358 du Code civil, insérer un alinéa ainsi rédigé :

« À cet effet, tout fichier numérique enregistré dans un dispositif électronique d'enregistrement partagé (DEEP) de nature publique ou privée vaut preuve de son existence et de sa date, jusqu'à preuve contraire, dès lors que ledit DEEP répond à des conditions définies par décret ».

Centre des Professions Financières
www.professionsfinancieres.com

COMPRENDRE ET FAIRE COMPRENDRE LES PROFESSIONS FINANCIÈRES

Crée en 1957, **le Centre des Professions Financières** présidé par Michel Pébereau rassemble l'ensemble des professions financières : banque, assurance, gestion d'actifs, marchés financiers, émetteurs de cautions, intermédiaires ainsi que leur écosystème, fonctions financières des entreprises et des collectivités publiques, conseils et auditeurs, enseignement, recherche... Le Centre a pour objectif de promouvoir et de faire connaître les métiers de la finance.

1 000 membres

7 publications

50 manifestations

5 groupes de travail

9 clubs

1 concours des mémoires

Le Centre travaille sur des sujets d'actualités tels que : **l'Investissement de Long Terme, la Finance verte, l'éducation financière** ou encore **l'Intelligence Artificielle, dans un contexte européen.** Par exemple, en 2018-2019 :

- Un séminaire « Blockchain & ICO »
- « Intelligence Artificielle et métiers de la finance » dans le Magazine n°16 des Professions Financières avec des articles de chercheurs, des autorités financières, des acteurs impactés...
- La Convention annuelle sur le thème : « La Relation Client 2.0 : quel rôle pour l'IA ? »
- Le Centre répond à la consulation de place organisé par l'ACPR sur l'IA

Et aussi :

- Parution prochaine d'un cahier consacré au Blockchain et ICO
- Big data et data protection, objet d'une conférence en décembre 2016 et thème d'une prochaine manifestation sur les ICO et les crypto actifs en juin 2019
- Le Centre soutient Paris Fintech Forum



@Centre_Prof_Fin

Centre des Professions Financières

Centre des Professions Financières

CONTACTS

www.professionsfinancieres.com
contact@professionsfinancieres.com



Les technologies quantiques au service de l'industrie financière

4. Les technologies quantiques au service de l'industrie financière

4.1 INTRODUCTION

Au début du XXe siècle est apparu la physique quantique décrivant le comportement des atomes et des particules, ce que la physique classique, notamment la mécanique newtonienne et la théorie électromagnétique de Maxwell, n'avait pu expliquer. Permettant de comprendre certaines propriétés du rayonnement électromagnétique qui restaient incompréhensibles pour la physique classique, elle est aujourd'hui un élément incontournable pour tous ceux qui veulent découvrir la physique contemporaine.

La physique quantique est à l'origine d'une révolution conceptuelle qui a eu des répercussions jusqu'en philosophie (remise en cause du déterminisme) et en littérature (science-fiction). Elle a permis nombre d'applications technologiques : énergie nucléaire, imagerie médicale par résonance magnétique nucléaire, diode, transistor, circuit intégré, microscope électronique et laser. Un siècle après sa conception, elle est abondamment utilisée dans la recherche en chimie théorique (chimie quantique), en physique (mécanique quantique, physique statistique quantique, astrophysique, gravité quantique), en mathématiques (formalisation de la théorie des champs) et, récemment, en informatique (ordinateur quantique, cryptographie quantique). Elle est considérée avec la relativité générale d'Einstein comme l'une des deux théories majeures du XXe siècle.

Parmi ses applications prometteuses qui commencent à se concrétiser est l'informatique quantique qui permet d'envisager la conception d'ordinateurs, d'algorithmes et de systèmes de communication dont les performances en termes de puissance de calcul et de sécurité sont inatteignables avec les technologies actuelles. Elle permettra de résoudre des problèmes complexes, non ou mal résolus aujourd'hui, et ce dans un délai raisonnable.

Les systèmes informatiques et de communication occupent une telle place dans notre société que le développement et la sécurité de ces nouvelles technologies vont devenir un enjeu stratégique à l'échelle des États. Les risques de souveraineté associés seront comparables à ceux de la défense des nations. En témoignent les investissements colossaux à travers le monde engagés par des pays comme les États-Unis ou la Chine, mais également par des sociétés comme IBM, Google, Microsoft, à l'instar de ceux réalisés pour développer les supercalculateurs.

L'Union Européenne a ainsi lancé un programme de recherche à grande échelle et à long terme, le « Quantum Technologies Flagship », qui rassemble des instituts de recherche, des entreprises et des bailleurs de fonds publics, consolidant et développant le leadership scientifique européen et l'excellence dans ce domaine. En mettant à disposition les résultats de la recherche quantique sous forme d'applications commerciales et de technologies perturbatrices, le programme, d'une durée de dix ans et doté d'un budget d'un milliard d'euros, favorisera le développement

d'une industrie quantique compétitive en Europe. Au cours de sa phase de démarrage (octobre 2018 à septembre 2021), il fournira un financement de 132 millions d'euros pour 20 projets relevant de quatre domaines d'application (communication quantique, simulation quantique, informatique quantique et métrologie quantique et détection) et financera également des recherches sur les bases scientifiques des technologies quantiques.La vision à long terme du Flagship est de développer en Europe un réseau quantique où ordinateurs, simulateurs et capteurs quantiques seront interconnectés via des réseaux de communication quantiques[112].

Il est toutefois difficile de préciser aujourd'hui quand les applications des technologies quantiques se concrétiseront au niveau commercial. Les challenges scientifiques, technologiques et industriels sont nombreux et l'ordinateur quantique universel reste un objectif futuriste. Au vu du nombre et de la qualité des équipes qui travaillent sur le sujet dans le monde entier, on peut néanmoins penser que les progrès seront significatifs à court terme et que des percées majeures sont vraisemblables à plus long terme. Par ailleurs, comme le montre l'expérience passée, il n'est pas nécessaire qu'une technologie soit complètement au point et satisfaisante à tous égards pour s'imposer si elle apporte déjà un avantage compétitif décisif.

Les pages qui suivent vont présenter cette nouvelle aventure qui commence dès maintenant en six thématiques :

- Thématique « Informatique quantique » ;
- Thématique « Sécurité des communications à l'ère de l'ordinateur quantique » ;
- Thématique « Communications sécurisées quantiques » ;
- Thématique « Hardware » ;
- Thématique « Ingénierie logicielle et outils de développement » ;
- Thématique « Conduite du changement, nouveaux métiers, formation, éducation et enjeux réglementaires, juridiques et éthiques ».

112. https://ec.europa.eu/digital-single-market/en/quantum-technologies.

4.2 THÉMATIQUE « INFORMATIQUE QUANTIQUE »

En 1982, le prix Nobel de physique Richard Feynman est le premier à imaginer les possibilités faramineuses d'un ordinateur capable de tirer parti des lois quantiques : on parle alors de la seconde révolution quantique. Dès les années 1990, plusieurs théoriciens démontrent que certains calculs verraient leur résolution accélérée dans des proportions inouïes s'il était possible de les implémenter sur des qubits plutôt que sur des bits classiques. À condition, bien sûr, de disposer d'un processeur quantique pour les utiliser, processeur dont personne ne sait à l'époque à quoi il pourrait ressembler[113].

Un **calculateur quantique** (en anglais *quantum computer* parfois traduit **ordinateur quantique** ou **système informatique quantique**) utilise les propriétés quantiques de la matière, telle que la **superposition** et **l'intrication** pour effectuer des opérations sur des données.

La superposition quantique

Pour une particule (photon, électron, etc.), on appelle état quantique la valeur d'une propriété physique de cette particule. Ces états sont discontinus, c'est-à-dire qu'ils ne peuvent prendre que certaines valeurs bien définies. Par exemple :

- Le sens de magnétisation du spin d'électron est orienté vers le haut ou vers le bas ;
- La polarisation linéaire des photons est horizontale ou verticale, après passage au travers de filtres polarisants ;
- La fréquence ou l'énergie d'un courant oscillant dans un qubit supraconducteur.

Contrairement aux principes classiques, une particule quantique peut être dans différents états simultanément.
Appliqué à l'informatique :

- un bit classique est soit dans l'état 0, soit dans l'état 1 ;
- un bit quantique (qubit) est à la fois dans les états 0 et 1.

Il s'agit du **principe de superposition**[114] **:** la particule est simultanément dans plusieurs des états de la base qui la caractérise. Son état est indéfini et indéterminé avant toute mesure, c'est sa mesure qui place la particule dans tel ou tel état.

Le principe de superposition quantique est extrêmement puissant et est au cœur des communications et de l'informatique quantique en cours de développement. Mais il est aussi fragile, à la merci d'interactions non désirées qui précipiteraient un retour au monde classique, dans lequel l'état du système est bien défini. La destruction de la superposition quantique est appelée la décohérence. C'est cela qui permet aux calculateurs quantiques de paralléliser les calculs à un niveau inégalé comparativement aux meilleurs supercalculateurs classiques.

113. www.cea.fr.
114. Mathématiquement, la *superposition* correspond à une combinaison pondérée de ces états, comme le serait une distribution probabiliste. En revanche, ces poids peuvent être négatifs, et même être des nombres complexes. Les carrés de leurs modules valent 1. Si la particule est observée ou mesurée, cette *superposition* est réduite à l'état correspondant de la particule au moment de son observation. La particule est alors dans l'état mesurée et ne peut alors plus se trouver dans les autres états. La possibilité de trouver la particule dans l'état observé lors de la mesure est donnée par une probabilité fournie par le carré (du module) de son poids dans la *superposition* d'états quantiques.

L'intrication quantique

Le caractère surprenant des états intriqués a été pour la première fois souligné par Einstein, Podolsky et Rosen (E.P.R) dans un article de 1935 qui tentait de montrer que la mécanique quantique était incomplète. Dans cet article, les auteurs décrivent une expérience de pensée qui restera connue comme le paradoxe EPR[115].

En mécanique quantique, l'intrication correspond à la situation de deux ou plusieurs particules ayant préalablement interagi entre elles[116] et dont les états quantiques dépendent instantanément les uns des autres, quelles que soient les distances qui les séparent. Cette dépendance spatiale est aussi appelée principe de non-localité.

Ces particules ont un destin commun qui est formulé dans le paradoxe d'EPR. Ainsi, avec une paire de particules intriquées, l'action sur l'une des deux particules a un impact instantané sur l'autre particule, par exemple, une mesure effectuée sur un quantum aura instantanément un effet sur l'autre quantum, sans attendre un délai de transmission d'informations à la vitesse de la lumière entre les deux quantums, comme l'a démontré le physicien français Alain Aspect dans sa fameuse expérience réalisée en 1982[117].

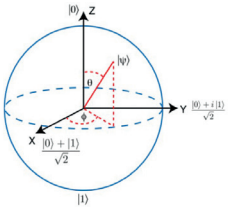
Bit quantique ou qubit

Dans un ordinateur classique, l'information est stockée dans un ensemble (registre) de cases mémoires, les bits, dont la valeur est soit 0, soit 1. Un bit quantique (qubit) a, quant à lui, deux états quantiques |0> (ket 0) et |1> (ket 1), séparés par une différence d'énergie définissant sa fréquence, et peut être à la fois dans ces deux états.

Un qubit[118] est la plus petite unité d'information binaire représentant un état quantique d'une particule ou un système profitant de ses propriétés de superposition d'états. Les possibilités de :

- mettre un qubit dans une superposition d'états ;
- d'intriquer deux objets quantiques dans une superposition d'états devraient permettre des calculs d'un type nouveau, « quantiquement parallélisés ».

Au cours d'un algorithme (succession d'opérations dites « portes logiques »), le registre de qubits se trouve dans une superposition quantique de tous ses états possibles (|00… 0>, |10… 0>, |11… 1>, |10… 1>),

115. fr.wikipedia.org/wiki/Paradoxe_EPR.
116. Par exemple, deux photons intriqués sont le résultat du passage d'un seul photon dans un miroir dichroïque qui les sépare en deux photons de polarisations orthogonales.
117. L'expérience d'Alain Aspect fait la preuve de l'intrication qui met à défaut le principe de non-localité par la violation des inégalités de Bell.
118. 

La valeur d'un qubit est une superposition linéaire de deux états de base |0> (Ket 0) et |1> (Ket 1) : | ψ > = α |0> + b |1> avec a, b ϵ C² et |α|2 + |b|2 = 1. Mathématiquement, l'état d'un qubit peut être représenté sur la sphère de Bloch (ou de Poincaré). En l'absence de décohérence, un qubit évolue donc sur la surface de la sphère de Bloch qui est une représentation géométrique en coordonnées sphériques des états quantiques possibles suivant la relation : |ψ> = cos (θ/2) |0> + $e^{iθ}$ sin (θ/2) |1>. Lors de sa mesure, entrainant la décohérence (perte de l'état quantique), le qubit peut valoir :
- |0> et le qubit se trouvent alors dans cet état après sa mesure ;
- |1> et le qubit se trouvent dans cet état après sa mesure.

permettant un calcul massivement parallèle[119]. En effet, **l'ordinateur quantique peut doubler sa puissance de calcul à chaque qubit ajouté**, d'où un gain exponentiel de sa puissance, impossible à réaliser en informatique traditionnelle. Pour 250 qubits en interaction, il faudrait environ 10*80 bits classiques pour stocker l'équivalent d'informations ! C'est plus d'atomes qu'il n'y en a dans l'univers visible…

Ainsi, dans un ordinateur classique, une série de N bits égaux à 0 ou 1 permet d'encoder un unique nombre parmi les 2^N possibles (un parmi 4096 pour N = 12). En revanche, un registre quantique dont les 12 qubits seraient en parallèle, plongés dans les deux états de base |0> ou |1>, se trouverait dans une superposition des 4096 états de base du registre. Toute opération quantique qui lui serait appliquée s'effectuerait en parallèle sur ces 4096 états de base en même temps. Ceci ne réaliserait pas pour autant du calcul parallèle, car la lecture ne donnera qu'un seul résultat. L'art de l'algorithmique quantique consiste alors à exploiter le parallélisme tout en concentrant, par chaque étape de mesure, l'état du registre quantique sur la ou les solutions du problème étudié.

L'enjeu de la puissance de calcul d'un ordinateur quantique consiste à assembler le plus de qubits possibles (intriqués en état de superposition).

Interaction des qubits avec l'environnement : mesure, manipulation et décohérence quantique

L'état du qubit est indéfini tant qu'il n'a pas été mesuré. La mesure consiste à lire la valeur du qubit après le calcul, qui perd alors son état quantique. La perte de l'état quantique s'appelle la décohérence. Pour effectuer un autre calcul quantique, il faut réinitialiser les qubits en les remettant en état quantique, via l'application de *codes de correction d'erreur.*

Ce qui limite aujourd'hui les performances de l'ordinateur quantique est le fait que les qubits interagissent avec leur environnement et perdent leur information quantique (phénomène de décohérence : plus les qubits sont nombreux et intriqués, plus ils sont sensibles au monde extérieur, ce qui génère un nombre non négligeable d'erreurs) avant que le calcul quantique n'ait eu le temps d'être réalisé. L'interaction avec l'environnement est cependant nécessaire, car c'est ce qui permet la manipulation des qubits ainsi que leur lecture. La vitesse des opérations quantiques est un paramètre majeur pour construire un ordinateur quantique ayant un impact. Il apparait donc nécessaire de trouver un compromis entre immunité à l'environnement (qui permet de grands temps de cohérence) et interaction pour accélérer les opérations. Les meilleurs compromis sont encore en train d'être étudiés.

Afin de prendre en compte la décohérence, la communauté de la physique a deux stratégies : construire des qubits dans lequel l'information quantique est protégée (stratégie de Microsoft avec un très bas TRL, l'existence de ces qubits n'a pas encore été prouvée) ou prendre en compte la décohérence à travers les codes correcteurs d'erreur quantiques qui permettent de construire des qubits

119. www.cea.fr/multimedia/Documents/infographies/defis-du-cea-infographie-processeur-quantique-elementaire214.pdf.

logiques dont le temps de cohérence est plus grand que les qubits physiques. Là encore, la communauté de la recherche est dans la phase de démonstration de la possibilité de réaliser un calcul quantique tolérant aux fautes.

Une approche de compromis est en train d'émerger avec le NISQ/*noisy intermediate scale quantum computing*. Le NISQ vise à étudier s'il est possible de réaliser des calculs combinant les effets quantiques et classiques pour résoudre des problèmes spécifiques mieux que ne saurait le faire un ordinateur quantique.

L'ordinateur quantique sera composé de parties constituées de technologies et d'architectures classiques qui permettront de piloter et contrôler des parties exploitant des phénomènes quantiques pour ces calculs : on parle alors de co-processeur quantique.

Pour mieux saisir la différence entre deux ordinateurs, l'un classique et l'autre quantique, nous avons relevé les différents éléments (voir le tableau ci-dessous).

Bien que 10 à 15 ans soient probablement encore nécessaires à la construction d'un calculateur intégrant la correction d'erreur[120] et susceptible de battre un ordinateur classique, c'est-à-dire d'atteindre la « suprématie quantique[121] », l'immense saut de performance calculatoire attendu en fait dès aujourd'hui un espace de recherche et d'innovation de rupture majeur. L'informatique quantique est potentiellement la technologie de traitement de

Informatique classique	Informatique quantique
L'élément le plus fondamental pour stocker et traiter l'information se fait sur la base du bit qui prend les valeurs 0 ou 1 selon que le courant circule ou non.	**L'unité élémentaire de stockage et de traitement de l'information est le qubit (quantum bit), en état quantique (de superposition : 0 et 1 en même temps et intriqué : corrélé avec d'autres qubits). La mesure au final permet de le lire comme un 0 ou un 1 et lui fait perdre son état quantique.**
Quatre portes logiques : AND, OR, NOT, XOR à la base de la logique booléenne qui impose un traitement séquentiel.	**Les portes logiques quantiques sont différentes des portes classiques, et plus nombreuses : Hadamard, Toffoli, Pauli, Cnot, Swap, etc., sont conçues pour manipuler l'état des qubits se traduisant par leurs déplacements sur la sphère de Bloch.**
Toute opération ou tout calcul est in fine réalisé sur la seule base logique d'une itération séquentielle de ces quatre portes.	**Au cours d'un calcul quantique (algorithme : succession d'opérations dites « portes logiques »), le registre de qubits se trouve dans une superposition quantique de tous ses états possibles (|00… 0>, |10… 0>, |11… 1>, |10… 1>), permettant un calcul massivement parallèle. Seule la mesure permet de lire le résultat final.**
Ce type de traitement est déterministe : répéter le calcul conduit toujours au même résultat.	**Le résultat d'un qubit est aléatoire et obéit à une loi de distribution probabiliste entre les 2 valeurs logiques 0 et 1. Contrairement au calcul classique, le calcul quantique n'est pas déterministe : répéter plusieurs fois le calcul conduit à des résultats différents jusqu'à constater une convergence comme la solution optimale du calcul.**

120. Un problème important est la perte de la cohérence quantique des qubits physiques qui introduit des erreurs. Pour les corriger, on peut utiliser plusieurs qubits physiques imparfaits couplés pour créer un qubit logique « parfait ». Plus le taux d'erreur est important, plus le nombre de qubits physiques nécessaire est grand.
121. On estime qu'elle pourra être atteinte à partir de 50 qubits logiques, pour des applications de simulation de systèmes quantiques. Cette estimation dépend néanmoins de la classe de problèmes à résoudre. Pour la factorisation de très grands nombres pour la cryptographie, le « seuil d'utilité » est estimé à ~1M de qubits logiques, soit > 1 milliard de qubits physiques.

l'information de demain[122] post-exascale et post-loi de Moore. Alors que dans un ordinateur classique, la croissance de la puissance est linéaire en nombre de bits et de transistors, en informatique quantique, l'ajout d'un bit quantique double la puissance théorique possible.

Il faut réinventer toute la chaîne de valeur du traitement automatique de l'information : architecture matérielle, système d'exploitation, outils de développement, langages de programmation, algorithmes…

122. Pour certaines classes de problèmes dont l'étendue est encore mouvante, mais en rapide évolution.

Les applications de l'informatique quantique

CCependant, une fois un tel ordinateur construit, encore faudra-t-il le programmer… Un acteur économique qui aura développé des algorithmes métiers et acquis un processeur quantique capable de les exécuter efficacement retirera un avantage concurrentiel majeur de la possibilité de, notamment :

- Résoudre des problèmes inaccessibles à la puissance de calcul classique : découverte de nouvelles molécules…
- Calculer dans un temps décisif : pricings complexes…
- Porter atteinte à la propriété intellectuelle de la concurrence : reverse engineering, crypto-analyse…

Quelques exemples par industrie :

- Banque et assurance : trading et prévisions de marché, sécurisation des échanges bancaires, analyse de risques, gestion de portefeuilles, actuariats ;
- Santé : conception de molécules, simulations d'épidémie, recherche pharmaceutique et génétique ;
- Industrie (énergie, exploration pétrolière, simulations…) : trouver une solution optimale dans un système complexe multiparamètres, p. ex. la tournée la plus rapide d'un camion de livraison ou ajuster l'offre à la demande sur un réseau électrique très décentralisé ;
- Intelligence artificielle : au cours de la phase d'apprentissage d'un système d'IA, tel que la reconnaissance d'images, les informations pourront être simultanément reconnues et non de façon séquentielle comme c'est le cas avec des processeurs classiques (examiner une situation, puis une autre, etc.) ;
- Tous secteurs : planification, gestion des ressources, ordonnancement, optimisation multicritère.

À ce jour, quatre principales catégories d'algorithmes quantiques sont disponibles :

1. **Les algorithmes de recherches** basés sur ceux de Deutsch-Jozsa, Simon et Grover. L'algorithme quantique de Grover permet un gain quadratique en temps de tout algorithme exécutant une recherche exhaustive ou heuristique. Les applications sont multiples, dont principalement la recherche d'informations précises dans une base de données ou la crypto-analyse ;

2. **Les algorithmes basés sur les transformées de Fourier quantiques (QFT)**, comme celui de Shor qui sert à la factorisation des grands nombres entiers et n'est pas adressable en des temps raisonnables par l'informatique classique. L'une des premières mises en œuvre de l'algorithme de Shor a eu lieu en 2001 chez IBM avec un ordinateur quantique expérimental de 7 qubits, pour factoriser le nombre 15. L'algorithme de Shor permet en théorie de casser les clés publiques de la cryptographie RSA couramment utilisée dans la sécurité sur Internet. Avec lui, il deviendra possible de casser les clés de chiffrement RSA et d'autres algorithmes cryptographiques asymétriques qui garantissent aujourd'hui le bon fonctionnement d'Internet (dans la banque, on utilise l'algorithme de chiffrement RSA-2048 ; en 2010, il a fallu 2 ans pour trouver le RSA-768). Cette menace potentielle

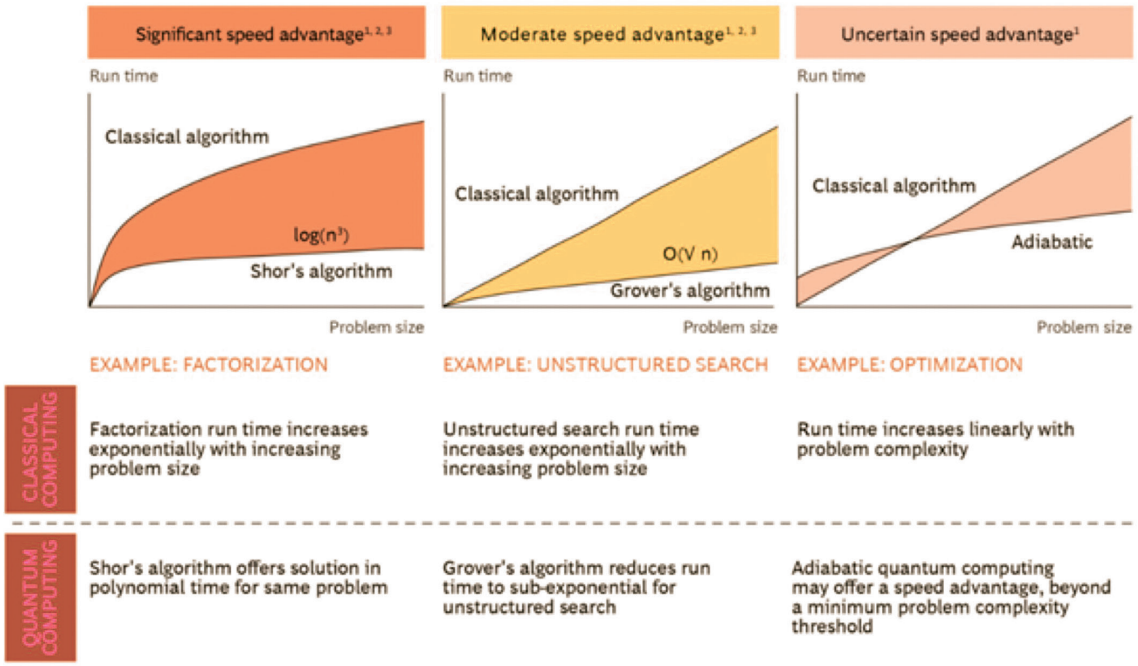
a donné naissance au champ de recherche de la cryptographie post-quantique (voir la thématique suivante sur la sécurité des communications à l'ère de l'ordinateur quantique) ;

3. **Les algorithmes qui cherchent un point d'équilibre d'un système complexe (minimisation de fonctions notamment d'énergie)** comme dans l'entraînement de réseaux de neurones, la recherche de chemin optimal dans des réseaux ou l'optimisation de processus. Certains de ces algorithmes peuvent d'ores et déjà être implémentés sur des machines à recuit quantique telles que la machine de DWave ;

4. **Les algorithmes de simulation quantique** qui servent notamment à simuler les interactions entre atomes dans des structures moléculaires diverses, inorganiques et organiques. Il s'agit à la base de l'idée originelle d'ordinateur quantique de Richard Feynman (1981). Pour cela, deux critères sont nécessaires :
   - Le problème doit être formulé sous forme dite « hamiltonienne ». C'est le cas « natif » pour des problèmes venant de la physique ou de la chimie quantiques.
   - L'hamiltonien doit être implémentable par le simulateur quantique. Les simulateurs quantiques connus actuellement (ions piégés, atomes froids, atomes de Rydbergs…) n'implémentent que certaines classes d'hamiltoniens. Il faut donc s'assurer que le problème recherché peut être approché avec suffisamment de précision par un hamiltonien connu.

Les algorithmes de simulation quantique ne doivent pas être confondus avec la simulation d'algorithmes quantiques effectuée sur un hardware classique, p. ex. la Quantum Learning Machine (QLM) d'Atos, aujourd'hui seule entreprise au monde à

EXHIBIT 1 | Quantum Computing Offers a Big Speed Advantage for Solving Some Problems



Source : BCG analysis

commercialiser un simulateur quantique opérationnel. La QLM est utilisée pour tester les programmes, créer de nouveaux algorithmes et découvrir le champ de la programmation quantique. La promesse d'Atos est que toutes les applications créées et tournant sur le simulateur seront fonctionnelles sur un calculateur quantique lorsque celui-ci sera disponible. Atos entend être le premier constructeur (et vraisemblablement le seul) européen à livrer un simulateur quantique[123].

123. www.atos.net/fr/vision-et-innovation/atos-quantum.

Les principaux algorithmes utilisés en informatique quantique et applications correspondantes en finance

Les principaux algorithmes quantiques déjà existants aujourd'hui sont présentés ci-dessous :

Algorithme de Shor

Il permet de calculer les périodes de fonctions algébriques. Parmi les applications, on dénote la factorisation, le calcul du logarithme discret et la plupart des communications chiffrées par des clés générées par de la cryptographie asymétrique.

Algorithme de Grover

Il permet un gain quadratique en temps par rapport à tout algorithme exécutant une recherche exhaustive ou heuristique. Les applications sont multiples, dont principalement la recherche d'informations précises dans une base de données ou la crypto-analyse.

	Algorithme de Schor	Algorithme de HHL	Programmation linéaire, semi-définie	Monte Carlo Quantique	Quantum Machine Learning	Simulation Quantique	Recuit Quantique
Déchiffrer la plupart des communications chiffrées par des clés générées par de la cryptographie asymétrique avec les technologies actuelles	•						
Analyse statistique en grande dimension		•	•				
Techniques de data sciences et de machine learning (analyse factorielle, décomposition en valeurs singulières, régressions, réseaux de neurones,...)		•	•				
Optimisations		•	•			•	•
Allocation de ressources		•	•				
Résolution d'équations différentielles linéaires		•	•				
Parcours de graphes		•	•				
Trading analytics				•	•		
Résolution du problème de la trajectoire de trading optimale					•		
Modélisation des risques				•	•		
Gestion de portefeuilles				•			
Prédiction					•		
Simulation de processus aléatoires					•		
Apprentissage automatique (*deep learning*, en particulier)						•	•
Science des matériaux						•	
Résolution de systèmes d'équations aux dérivées partielles						•	

Algorithme de HHL (Harrow-Hassidim-Lloyd)

Sous certaines conditions, cet algorithme quantique permet de résoudre un système d'équations linéaires Ax=b de taille n x n en temps log (n), alors que le meilleur algorithme classique connu a une complexité entre n^2 et n^3. La particularité de cet algorithme est de convertir une superposition quantique encodant b vers une superposition quantique encodant la solution x. Ainsi, seuls log (n) qubits sont nécessaires. À proprement parler, la solution x n'est donc pas connue, mais elle est disponible en superposition.

Monte-Carlo quantique

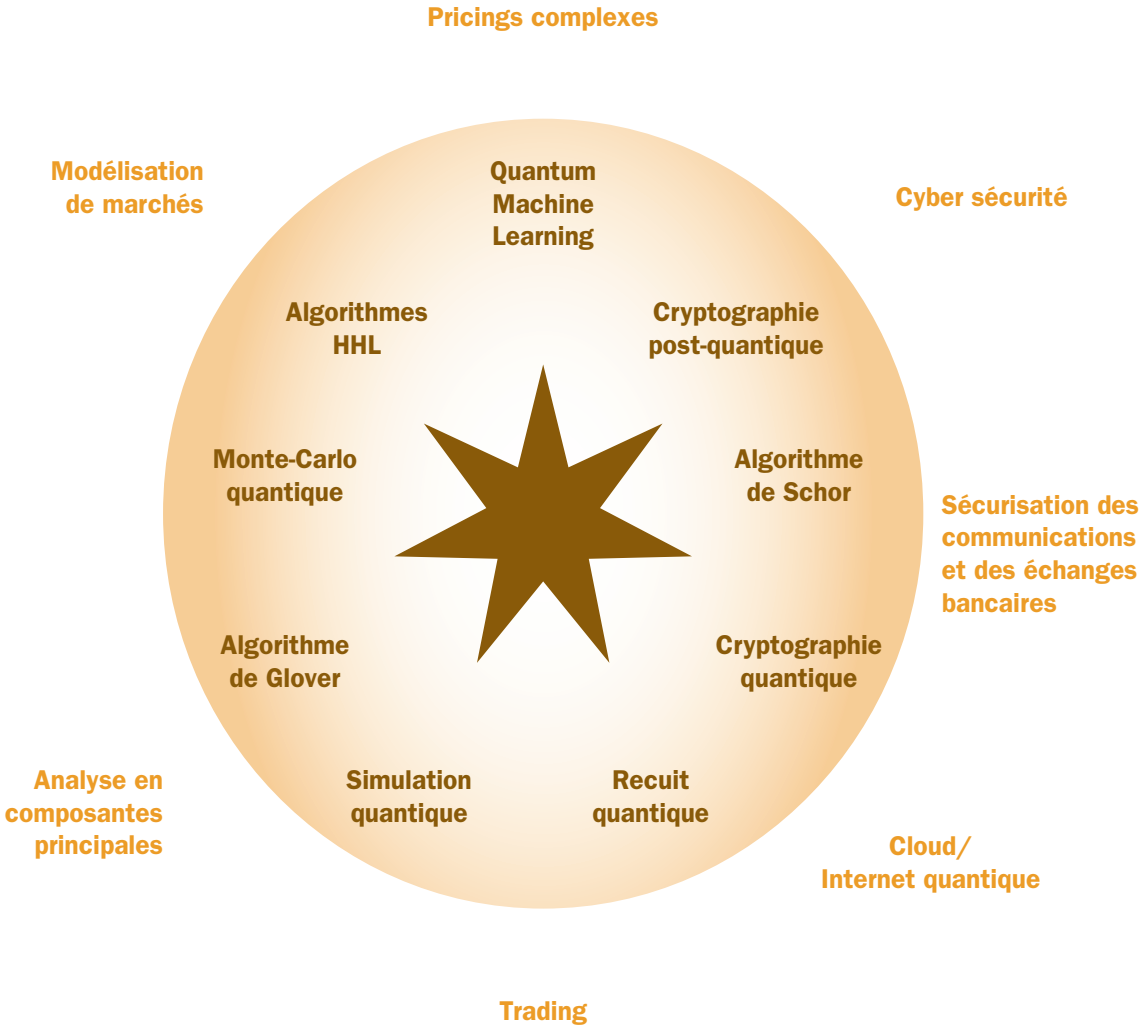
Les méthodes d'échantillonnage de Monte-Carlo peuvent être accélérées de façon quadratique à l'aide d'outils quantiques telles que les marches quantiques. L'échantillonnage de Gibbs est l'une des applications de la méthode précédente pour les processus de Markov (prise en compte de la dimension temporelle) et qui a été récemment améliorée de façon exponentielle.

Programmation linéaire, semi-définie

L'algorithme utilise une version quantique de la méthode MMWU (*matrix multiplicative weight update*) avec un échantillonnage quantique de Gibbs exponentiellement plus rapide.

Quantum machine learning

L'apprentissage quantique consiste à utiliser des échantillons présentés en super-



position afin de réduire l'espace mémoire nécessaire pour les stocker. Ce codage super-dense permet néanmoins d'effectuer la plupart des techniques algébriques utilisées en *machine learning* classique jusqu'aux techniques de descentes de gradient.

D'un point de vue purement théorique, le nombre d'échantillons nécessaire à l'apprentissage quantique est exactement le même qu'en classique pour une distribution quelconque. En revanche, pour certaines distributions, le gain peut être exponentiel. D'un point de vue pratique, les gains en mémoire et temps, y compris pour les heuristiques, peuvent être eux exponentiels, à nombre d'échantillons quantiques fixés.

Simulation quantique

Les simulateurs quantiques vont permettre d'expérimenter et de développer de nouveaux algorithmes pour de nouveaux cas d'application. La simulation quantique consiste à exploiter les propriétés et résultats issus des opérations réalisées avec les qubits pour résoudre des problèmes relevant de la mécanique quantique.Son principe consiste à obtenir la solution d'un problème de manière « analogique », en le répliquant sur un système quantique contrôlable et observable (appelé le simulateur quantique), dont l'évolution convergera vers la solution recherchée.

Dans tous les cas, un travail important est nécessaire au niveau de la reformulation des problèmes, ce qui exclut a priori des résultats généraux avec une approche universelle systématique.

Quantum annealing (recuit simulé) et calcul adiabatique

En attendant, des calculateurs adaptés et optimisés pour certaines tâches déterminées (*adiabatic quantum computer*) sont envisagés à plus court terme.

Le recuit quantique est un modèle théorique d'optimisation, pouvant être vu comme une amélioration de la méthode du recuit simulé grâce à l'effet tunnel. Il est souvent confondu avec le terme « calcul adiabatique » qui est la voie la plus explorée pour les réalisations. Alors que le recuit « classique[124] » peut perdre du temps à explorer des extrema locaux, le recuit « quantique » pourra éviter ces extrema en les traversant par effet tunnel.

La société canadienne D-wave a été la première à revendiquer l'implémentation pratique du recuit quantique. Cependant, la communauté scientifique a majoritairement réfuté cette affirmation après les conclusions d'une commission indépendante. Le recuit quantique est unanimement regardé comme très prometteur et fait l'objet de nombreuses recherches. Les pistes d'implémentation se concentrent sur la simulation quantique.

Le recuit quantique présente le grand avantage d'offrir une formulation très générale, adaptée à un très grand nombre de problèmes d'optimisation. Il faut toutefois bien noter que si un problème est formulable sous forme de recuit quantique, la possibilité d'une accélération par rapport à un algorithme non quantique n'est pas acquise.

Il existe en effet des cas d'école pour lesquels l'impossibilité d'avance quantique, voire une « décélération » quantique, a été prouvée théoriquement. Il n'en demeure

124. fr.wikipedia.org/wiki/Recuit_simulé.

pas moins un potentiel technologique considérable. Parmi les applications les plus étudiées :

- l'optimisation numérique ;
- l'optimisation combinatoire, notamment de type qubo ;
- le Deep Learning, via les deux précédentes.

Le forum dédié www.quantumforquants.org dresse un inventaire des applications en finances.

Enjeux

- Manque de compétences multidisciplinaires : la jeunesse de l'informatique quantique et sa complexité inhérente font qu'un acteur, qui souhaite maîtriser cette nouvelle technologie et identifier de nouvelles opportunités métiers, a besoin d'un grand nombre de compétences (physique théorique, algorithmique théorique, architecture informatique, logiciels, mathématiques). Une bonne analogie est celle du premier ordinateur électronique ENIAC dont la programmation nécessitait mathématiciens, électroniciens, développeurs…
- Verrou de la technologie par des acteurs leaders (notamment dans le domaine des processeurs quantiques), peu d'acteurs de poids, risque de comportement hégémonique des leaders (p. ex. Google qui ne souhaite commercialiser sa technologie que sous forme cloud) ;
- En attendant que l'ordinateur quantique universel soit mis au point, l'enjeu des années à venir est l'hybridation, c.-à-d. l'ajout aux ordinateurs classiques de calculateurs quantiques spécialisés sur des problématiques bien déterminées ;
- Les problèmes associés au domaine de la finance nécessiteront des ordinateurs quantiques plus performants que les ordinateurs classiques actuels et donc probablement avec une correction d'erreur intégrée. Il est important pour le domaine de la finance de suivre les développements matériels qui permettent d'intégrer un grand nombre de qubits au plus tôt, car il est envisagé que le type de problèmes à résoudre ait un impact sur l'architecture.

Recommandations

La communauté scientifique nationale, bien structurée, réactive et dotée de compétences de tout premier plan, et de grands groupes industriels (Atos, Thales ou Total) ont pris conscience des enjeux.

Cependant, les moyens disponibles ne sont pas au niveau des efforts consentis par certains de nos concurrents et devraient être renforcés et diversifiés. Il faut donc favoriser les synergies à l'échelle européenne et les partenariats stratégiques avec l'Allemagne voire avec le Japon et favoriser échanges et transferts entre la recherche fondamentale et l'industrie.

Un effort doit également être réalisé pour élargir le périmètre des recherches à la fois dans la conception de prototypes, le renouvellement de l'algorithmique et la mise au point de systèmes d'exploitation permettant le couplage.

4.3 THÉMATIQUE « SÉCURITÉ DES COMMUNICATIONS À L'ÈRE DE L'ORDINATEUR QUANTIQUE »

La cryptographie classique constitue la brique fondamentale de la sécurité des données et des échanges numériques. Elle est présente dans toutes les activités de la vie quotidienne : communications (téléphonie, internet), cartes à puce, documents d'identité, systèmes embarqués dans l'aéronautique, transports et objets connectés (« Internet-of-Things »).

La confidentialité, l'intégrité, la disponibilité et la traçabilité des données financières et assurantielles réclament une utilisation intensive de ces méthodes cryptographiques. L'avènement d'un ordinateur quantique, reposant sur des principes physiques différents, menace néanmoins la plupart de ces applications. Plus précisément, de telles technologies quantiques constitueraient une menace majeure pour tout un pan de la cryptographie classique dite asymétrique dont la sécurité ne nécessite pas l'échange préalable d'un secret entre les différentes parties.

En effet, la sécurité de ces crypto-systèmes repose sur la complexité computationnelle de certains problèmes mathématiques, comme la factorisation des grands nombres ou le problème dit du logarithme discret. L'ordinateur quantique apparaît ainsi comme une épée de Damoclès menaçant le chiffrement RSA ou l'algorithme de signature digitale sur courbe elliptique ECDSA, tous deux massivement déployés dans nos systèmes d'information.

Dès lors, un changement technique majeur devra être opéré dans les prochaines années de manière à garantir dans tous ces domaines un niveau de sécurité satisfaisant et durable, faute de quoi la confidentialité des échanges numériques, la sécurité et la vie privée des utilisateurs seront menacées.

La transition vers les schémas de cryptographie dits post-quantiques et résistants à l'ordinateur quantique est une migration sensible qu'il convient d'aborder avec le souci constant d'assurer constamment un niveau de sécurité minimum sans introduire de fossé sécuritaire.

Cryptographie post-quantique : standardisation et développements industriels

Le processus de standardisation de la cryptographie post-quantique a débuté il y a plusieurs années déjà, en particulier sous l'impulsion de l'agence américaine NIST qui a lancé début 2017 un appel à contributions. Un des premiers jalons de ce travail de normalisation a eu lieu le 30 novembre 2017, date butoir de soumission des candidats aux standards. Soixante-neuf candidatures ont été validées formellement par le NIST et font actuellement l'objet d'analyses avancées par le NIST et l'ensemble de la communauté internationale en sécurité.

La France a bien pris la mesure de ces enjeux en lançant début 2017 un Programme d'Investissements d'Avenir (PIA) dans la catégorie des Grandes Défis du Numériques : le projet RISQ (Rassemblement de l'Industrie française pour la Sécurité post-Quantique). L'écosystème académique et industriel français en sécurité s'est ainsi fédéré pour répondre à ce défi dans le cadre d'un projet national, instruit par la Direction Générale des Entreprises et financé par Bpifrance, qui a pour objectif de positionner la France comme un acteur international majeur de la « transition post-quantique ». RISQ va ainsi renforcer la présence de la filière française de la sécurité numérique au sein des organismes de standardisation en rassemblant les acteurs nationaux (grands groupes industriels, PME/ETI, services étatiques, laboratoires académiques) – dont les compétences sont reconnues internationalement – afin de concerter leurs actions de propositions de standards et d'évaluation des candidatures.

En interaction avec ce processus, le projet définit une feuille de route pour la commercialisation de gammes de produits de sécurité « post-quantique » – librairies de calculs cryptographiques logicielles et matérielles, serveurs d'archivage, d'horodatage – allant de la conception des briques théoriques par les laboratoires partenaires au développement de démonstrateurs et leur validation. La présence de grands groupes au sein du consortium est garante de l'adaptabilité des solutions



La composition du consortium

développées aux systèmes déployés à l'heure actuelle.
À l'issue du projet à l'horizon 2020, les partenaires disposeront de la propriété intellectuelle et des offres en avance de phase nécessaires pour gagner une visibilité précoce sur les marchés qui seront issus des nouveaux standards dont les premiers sont attendus pour 2019/2020.

Enjeux

Si la feuille de route du NIST laisse présager l'émergence de standards post-quantiques à l'horizon 2020, il n'en demeure pas moins que ces standards devront être éprouvés de nombreuses années avant de gagner la confiance nécessaire à une adoption effective. La cryptographie est une science aux constantes de temps longues, mais le travail de cryptanalyse des candidatures post-quantiques a commencé et devrait écarter au cours du temps les schémas les plus fragiles.

L'implémentation sécurisée de ces algorithmes demeure une question centrale et devra prendre en compte les spécificités des différents domaines applicatifs et segments de marchés. Dans le domaine bancaire, les exigences en termes de performances sont fort diverses et il convient donc de définir précisément les besoins en termes de performances et sécurité.

Aucun schéma de chiffrement ou de signature n'étant pour le moment standardisé, l'enjeu est principalement de trouver des implémentations sécurisées par hybridation de solutions pré-quantiques (classiques) et post-quantiques, telles des méthodes de surchiffrement ou de concaténation de clés. Ces solutions sont multipliées, mais doivent être pensées sous contraintes. À l'heure actuelle, les algorithmes post-quantiques sont moins performants que les algorithmes classiques. Il convient de réaliser que cette transition douce permettra de parer à des failles sécuritaires importantes qui pourraient apparaître en cas de saut brutal dans le monde post-quantique.

Finalement, il faut être conscient que la cryptographie post-quantique n'apporte que peu de nouvelles « fonctionnalités », résout peu ou prou les mêmes problèmes que la cryptographie classique et constitue donc un pur mouvement de destruction créatrice (Schumpeter) qui doit être vu comme un levier potentiel d'innovation tout autant qu'un outil de souveraineté renouvelée.

Ces vingt dernières années ayant été riches en enseignement quant à l'implémentation sécurisée de schémas cryptographiques, la cryptographie post-quantique est une opportunité de rebâtir des modèles ayant pris acte de ces nouvelles connaissances et qui sont garants de cette sécurité.

Recommandations

À l'issue d'une revue des opérations actuellement chiffrées et authentifiées dans le domaine bancaire, il conviendrait d'établir un cahier des charges en termes de performances couplé à une analyse du risque afin de concevoir des solutions cryptographiques hybrides minimisant le risque résiduel face à des attaques classiques et quantiques et répondant aux besoins opérationnels du monde de la finance.

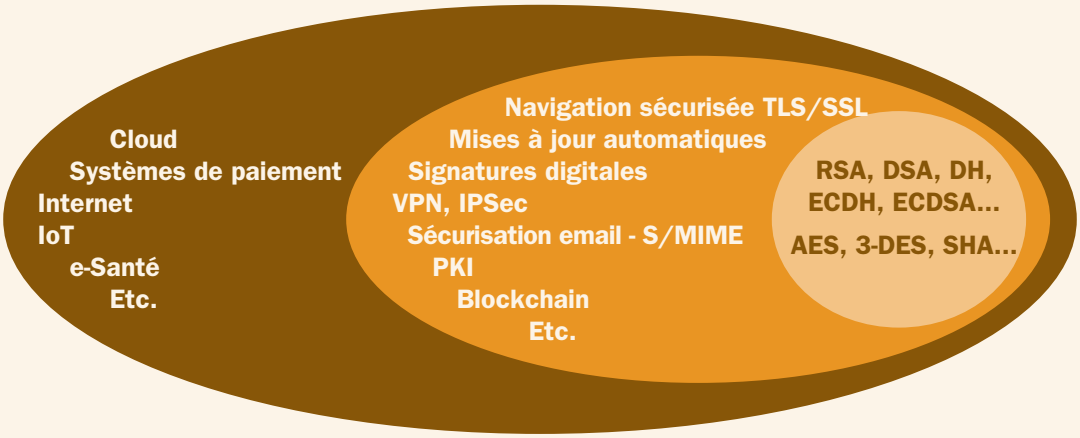
Focus
Le point de vue de Michele Mosca

Comme l'explique Michele Mosca[125] [1], il faut prendre en compte trois paramètres décrits comme tels dans le tableau ci-dessous.

Dans l'hypothèse d'un x + y > z, cela signifierait qu'à la fin des y prochaines années, l'information protégée par des outils vulnérables à l'ordinateur quantique pourrait être déchiffrée par des ordinateurs quantiques en moins de x années [1].

Paramètre	Définition	Exemple
X	Durée pendant laquelle il faut sécuriser l'information	En Allemagne, les informations de santé doivent être protégées au-delà de la vie d'un patient et dans ce cas x = 100
Y	Durée de migration vers des solutions résistantes à l'ordinateur quantique.	La migration des smart cards RSA vers les algorithmes Elliptical Curve Cryptography (ECC) pourrait durer jusqu'à 2030 et dans ce cas y = 12.
Z	Durée avant que les solutions de cryptographie asymétriques classiques ne soient cassées par des ordinateurs quantiques ou d'autres méthodes.	En prenant l'hypothèse d'une loi de Moore qui s'appliquerait aux technologies quantiques, Michele Mosca estime à un sur 7 la probabilité que le code RSA-2048 soit cassé d'ici 2026 et à un sur deux d'ici 2031, soit respectivement z = 8 et z = 11.

Qu'est-ce qui sera impacté ?



evolution

UNIVERSITY OF WATERLOO

IQC Institute for Quantum Computing

125. Michele Mosca est co-fondateur et directeur adjoint de l'Institut d'informatique quantique de l'Université de Waterloo.

Focus
Le cas Bitcoin

La sécurité de la blockchain bitcoin est assurée par des technologies de cryptographie asymétrique. Concrètement, les bitcoins sont « rattachés » à une adresse, dérivée d'un couple clé privée/clé publique. Tout détenteur de la clé privée peut dépenser et utiliser les bitcoins. (Par analogie, les euros sont déposés sur des comptes et toute personne utilisant le numéro de carte bancaire et le code associé peut les dépenser à sa guise.

La robustesse des systèmes à clé privée/clé publique repose sur le postulat que les technologies informatiques actuelles ne permettent pas de deviner la clé privée à partir de la clé publique en un temps raisonnable. Tant qu'un utilisateur ne divulgue pas sa clé privée, les bitcoins qu'il a en sa possession, rattachés à cette clef, ne peuvent pas lui être dérobés.

Les ordinateurs quantiques devraient permettre à terme de calculer une clé privée à partir de sa clé publique en un temps raisonnable, rendant vulnérable l'ensemble du système. Il existe aujourd'hui des barrières qui protègent le bitcoin contre ce type d'attaque.

Pour recevoir des bitcoins, il suffit de communiquer son adresse bitcoin qui est un hash de la clé publique, c'est-à-dire tant que vous n'avez pas dépensé les bitcoins d'une adresse, la clé publique reste masquée et personne ne peut retrouver ni la clé privée ni la clé publique. La pratique veut que lors d'une transaction, le compte soit entièrement soldé et qu'une nouvelle adresse soit créée pour recevoir la différence entre le solde du compte et le montant de la dépense.

Le risque est donc relativement limité et les experts estiment que les ordinateurs quantiques ne représenteront pas une menace avant 10 ans[126]. D'ici là, de nouveaux algorithmes et protocoles pourront être déployés pour protéger le réseau, d'autant que l'ensemble des méthodes cryptographiques utilisées (banque, finance, sécurité nationale…) sera menacé et que le bitcoin ne devrait pas être le principal sujet d'inquiétude.

Enjeux

Ils résident dans la conception d'une preuve de travail alternative pour protéger le bitcoin, les crypto-monnaies et toutes les blockchains face au risque quantique. L'article de référence est ici celui de Miklos Santha et al[127] : *« Les principaux protocoles cryptographiques utilisés pour sécuriser Internet et les transactions financières aujourd'hui sont tous susceptibles d'être attaqués par le développement d'un ordinateur quantique suffisamment puissant. Les crypto-monnaies constituent un domaine particulièrement menacé avec un marché évalué actuellement à plus de 150 milliards US $. Nous étudions le risque du bitcoin et d'autres crypto-monnaies face aux attaques d'ordinateurs quantiques. Nous pensons que la "proof-of-work" du bitcoin est relativement résistante à une accélé-*

126. www.technologyreview.com/s/609408/quantum-computers-pose-imminent-threat-to-bitcoin-security.
127. www.technologyreview.com/s/609408/quantum-computers-pose-imminent-threat-to-bitcoin-security et www.arxiv.org/abs/1710.10377.

ration substantielle des ordinateurs quantiques au cours des 10 prochaines années, principalement parce que les mineurs ASIC spécialisés sont extrêmement rapides par rapport aux fréquences estimées des ordinateurs quantiques à court terme. D'un autre côté, le schéma de signature de la courbe elliptique utilisé par le bitcoin est beaucoup plus à risque et pourrait être cassé par un ordinateur quantique dès 2027, selon les estimations les plus optimistes. Nous analysons une autre "proof-of-work" appelée Momentum, basée sur la découverte de collisions dans une fonction de hachage cryptographique qui est encore plus résistante à l'accélération d'un ordinateur quantique. Nous passons également en revue les schémas de signature post-quantique disponibles pour déterminer lequel répond le mieux aux exigences de sécurité et d'efficacité des applications blockchain.»

Recommandations

Le concept de non-clonage permet de concevoir de l'argent quantique infalsifiable et, contrairement au chiffrement quantique, il s'agit d'un investissement à long terme. Les premières expérimentations[128] ont commencé.

128. www.fortune.com/2018/01/06/breaking-bitcoin-cybersaturday et https://www.nature.com/articles/s41534-018-0058-2.epdf.

4.4 THÉMATIQUE « COMMUNICATIONS SÉCURISÉES QUANTIQUES »

Les technologies quantiques permettent de développer de nouveaux protocoles de communication dont la sécurité est garantie et résistant aux attaques d'un ordinateur quantique. Les applications concerneront dans un premier temps l'échange d'information sécurisé entre deux points, souvent à l'aide de clés cryptographiques, le déploiement d'un internet quantique avec une sécurité reposant sur l'exploitation de l'intrication puis, à terme, la possibilité de réaliser des calculs à distance dans le « cloud quantique » de façon totalement sûre.

La distribution quantique de clés (Quantum Key Distribution – QKD)

Quelques définitions :

- **Distribution quantique de clés/*Quantum Key distribution* (QKD) :** ce système de communication exploite les propriétés de superposition cohérente d'états (et parfois d'intrication quantique dans certaines implémentations) pour permettre à deux parties de produire une clé secrète aléatoire partagée connue seulement d'eux. Les deux parties peuvent ensuite utiliser cette clé pour chiffrer et déchiffrer des messages en chiffrement symétrique.
- **Authentification d'identité :** il s'agit de s'assurer que c'est bien Alice qui cherche à communiquer avec Bob et non pas un usurpateur et que son accès est légitime.
- **Cryptographie quantique au-delà de la QKD :** la communication quantique peut être utilisée pour effectuer plusieurs protocoles cryptographiques au-delà de la distribution de clés. Quelques exemples sont la délégation de calcul sécurisée entre un client et un serveur, le tirage à pile ou face quantique, l'argent quantique, la transmission anonyme, etc.

Enjeux

La distribution de clé cryptographique (QKD) est le protocole phare du domaine de la cryptographie quantique et promet, en principe, une sécurité inconditionnelle des communications reposant unique-

ment sur les lois de la physique. En effet, la QKD est la seule méthode d'établissement de clés cryptographiques offrant une sécurité absolue dans le sens de la théorie de l'information et a l'avantage d'être sûre face aux attaques futures : il n'est pas possible pour un espion de conserver une copie des signaux quantiques envoyés dans un processus de QKD, en raison du théorème de non-clonage quantique.

Les applications potentielles de la cryptographie quantique incluent la garantie de sécurité dans des infrastructures critiques, les institutions financières et la défense nationale. Du fait de son potentiel stratégique, ce domaine joue un rôle central dans le contexte plus large des technologies quantiques et a été au centre d'un très grand effort scientifique et d'ingénierie ces dernières années.

Les systèmes QKD exploitent le codage de l'information quantique dans certaines propriétés des signaux photoniques. Les deux parties qui communiquent, Alice et Bob, échangent un grand nombre de signaux par un canal physique (fibre optique ou espace libre) et des informations supplémentaires envoyées sur un canal classique public, mais authentifié. Ils suivent ainsi un protocole qui aboutit à la génération d'une chaîne de bits secrète – la clé – avec un niveau de sécurité voulu au prix d'une réduction de la taille de chaîne initiale.

Les protocoles QKD peuvent être distingués essentiellement par la technique de détection utilisée pour extraire les informations sur la clé encodées dans les propriétés de la lumière. Des techniques de détection de photons uniques sont nécessaires pour des protocoles à variables discrètes (DV), comme le protocole BB84, développé en 1984 par Charles Bennett (IBM) et Gilles Brassard et sa version à états leurres. D'autre part, dans des protocoles QKD à variables continues (CV), l'information de la clé est codée dans les quadratures du champ électromagnétique quantifié, comme ceux des états cohérents et des techniques de détection cohérente sont utilisées dans ce cas. À tous ces protocoles de type préparation-et-mesure s'ajoutent les protocoles à base d'intrication où les deux parties reçoivent les photons d'un état intriqué et exécutent des mesures appropriées.

On remarque aussi que, bien que la sécurité d'un protocole QKD puisse être prouvée rigoureusement, sa mise en œuvre réelle contient souvent des imperfections qui peuvent ne pas être prises en compte dans la preuve de sécurité correspondante. En réponse à cette menace de « hacking » quantique, il a été nécessaire de développer des contre-mesures correspondantes. Une approche plus fondamentale afin de regagner la sécurité dans la mise en œuvre pratique de la QKD est la conception de nouveaux protocoles, notamment les protocoles de type (M) DI (en anglais *[measurement] device independent*). Même si la mise en œuvre de tels protocoles reste encore difficile, elle permettra d'établir la sécurité sans connaître les détails de l'implémentation.

Recommandations

- Il est important de comprendre que les solutions futures seront hybrides, combinant des solutions classiques et quantiques et offrant une sécurité à long terme. Ces solutions doivent être définies et mises en place en pratique ;
- Il est aussi important de comprendre

que la cryptographie porte aujourd'hui le qualificatif « quantique », car l'établissement de la clé secrète est fait à partir des lois de la physique quantique. Cependant, l'action de chiffrer et déchiffrer est parfaitement classique et non quantique ;

- Il est nécessaire d'avancer vers la certification et la standardisation de la QKD, ce qui permettra leur utilisation pour la sécurisation des transactions dans la vie courante ;
- La QKD est l'application-phare du domaine, mais tous les progrès dans ce domaine s'étendent sur une riche gamme d'applications au-delà de la distribution de clés (argent quantique, délégation de calcul sécurisé, transmission anonyme, identification, etc., voir section B pour quelques exemples), permettant d'utiliser l'avantage obtenu en exploitant des ressources quantiques pour des tâches complexes et variées ;
- Soutenir le développement du hardware permettra à la France et l'Europe de se positionner de façon stratégique sur ce marché porteur des communications quantiques (sources de lumières quantiques, générateurs de nombres aléatoires, détecteurs de photons uniques, systèmes de cryptographie) dans un contexte de forte poussée technologique internationale.

Les réseaux quantiques sécurisés

Enjeux

Au-delà des échanges de clés cryptographiques pour les communications sécurisées entre deux points, les technologies quantiques travaillent au déploiement de véritables réseaux de communications sécurisés par réseau fibré ou via communication par satellite. Ce réseau permettra de connecter différents ordinateurs quantiques entre eux en préservant la sécurité de l'information. Ces réseaux ne peuvent se satisfaire de lasers atténués, comme c'est encore possible pour la distribution de clés cryptographiques, mais reposent sur l'utilisation des propriétés éminemment quantique de la lumière, comme l'intrication, pour garantir la distribution sécurisée d'information. Dans ce domaine, la Chine a récemment réalisé des avancées remarquables avec la démonstration de téléportation quantique entre terre et satellite.

Plusieurs architectures sont envisagées pour cet internet quantique :

- une architecture basée sur des sources de photons uniques et des mémoires quantiques localisées sur les nœuds du réseau de communication ;
- une architecture basée sur l'utilisation d'états intriqués à grand nombre de photons. Cette architecture repose sur des sources de lumière très performantes et réduit les besoins en hardware local,

Ces deux architectures sont en cours de développement et requièrent différentes

ressources en termes de hardware. Un exemple de chemin de développement d'une architecture à base de mémoire quantique est donné en annexe.

Enfin, notons qu'au-delà de l'infrastructure nécessaire au développement de ces réseaux de communication quantique, de nouveaux protocoles sont développés pour mettre en réseau la puissance des ordinateurs quantiques. Étant donnée la sensibilité des informations traitées sur ces calculateurs, de nouveaux protocoles sont également développés pour permettre l'utilisation de « clouds » de serveurs de calculs quantiques garantissant la confidentialité des calculs de l'utilisateur.
L'internet quantique se trouve aujourd'hui dans une situation similaire à celle des réseaux de communication au milieu des années 60, lorsque furent développées les techniques fondamentales permettant le déploiement et l'interconnexion de réseaux de communication classiques.

L'un des challenges majeurs est également de découvrir de nouvelles applications non anticipées de l'internet quantique. En se basant sur l'évolution d'internet depuis 1969, on peut supposer que lorsque chacune des étapes de déploiement de ces réseaux sera franchie, et seulement alors, on découvrira quelles sont les applications importantes de ces nouvelles technologies. Ainsi, la motivation principale pour le développement de l'internet quantique n'est pas le nombre déjà important d'applications connues, mais plutôt de se donner ainsi les moyens d'en découvrir de nouvelles.
Un effort substantiel doit être entrepris du côté du développement du hardware afin de permettre le déploiement de cet internet quantique. Contrairement à la distribution de clés cryptographiques point à point qui a aujourd'hui atteint des niveaux de TRL[129] élevés, le développement de l'internet quantique possède un niveau de maturité technologique comparable à celui l'ordinateur quantique. Le choix de la meilleure architecture n'est pas encore finalisé, même si l'utilisation d'états quantiques à grand nombre de photons intriqués permettra à terme un débit de communication beaucoup plus élevé.

Recommandations

- Le déploiement d'un réseau de communication quantique multipoints sécurisé, permettant la mise en réseau de calculateurs quantiques et la communication sécurisée à grande distance et entre de multiples utilisateurs, est une ressource stratégique pour tous les secteurs d'activités où la sécurité de l'information est essentielle. Il existe beaucoup de développements technologiques (hardware, software, protocoles) au meilleur niveau mondial en France et en Europe et qu'il est aujourd'hui essentiel de soutenir pour permettre de mener en tête la course au déploiement de l'internet quantique ;
- Dans les démonstrations actuelles, les répéteurs quantiques – les nœuds du réseau – sont supposés fiables. Un enjeu important est le développement de protocoles et de hardware permettant le maintien de la sécurité, sans l'hypothèse de la fiabilité des nœuds intermédiaires.

129. TRL : *Technology Readiness Level*/Niveau de maturité technologique.

4.5 THÉMATIQUE « HARDWARE »

Les applications des technologies quantiques identifiées dans ce groupe de travail concernent le calcul quantique (ordinateur quantique) et la sécurité des communications.

Des révolutions technologiques sont en cours dans ces deux domaines qui ouvrent la voie à la résolution de problèmes insolvables avec les calculateurs classiques actuels et aux réseaux de communication de sécurité inviolables.

Le développement du hardware nécessaire au développement de ces deux larges domaines d'applications est l'objet d'une très forte activité de recherche et d'ingénierie scientifique au niveau international.

Hardware de l'ordinateur quantique

Côté calcul quantique, de nombreuses plateformes sont explorées, allant des ions piégés et des bits quantiques supraconducteurs aux qubits basés sur le spin ou la lumière. Chaque plateforme présente des forces et des faiblesses qui prennent plus ou moins d'importance quand on passe des systèmes de recherche aux systèmes faisant appel à un grand nombre de qubits.

On rappelle que pour surpasser les supercalculateurs classiques, l'ordinateur quantique devrait comporter environ 100 qubits capables de réaliser des millions d'opérations quantiques sans erreurs. Cela est aujourd'hui hors de portée de tous les systèmes physiques et c'est pourquoi les codes correcteurs quantiques, qui reposent sur la redondance d'information (comme en classique) et sur l'intrication, sont requis. Ils introduisent la notion de qubit logique qui est un qubit « parfait » composé de plusieurs centaines voire milliers de qubits physiques arrangés dans un réseau bidimensionnel.

Cela conduit le hardware à se projeter aujourd'hui vers des nombres de qubits de l'ordre ou supérieur au millier de qubits. Dans ce contexte, les figures de mérite prépondérantes pour la montée en complexité, au niveau du qubit unique, sont :

- **sa fidélité :** c'est le terme consacré en ingénierie quantique pour décrire l'inverse du taux d'erreur. On veut que la fidélité soit la plus proche possible de

100 % pour permettre d'implémenter des codes correcteurs d'erreur avec le moins *d'overhead* possible ;

- **sa vitesse de manipulation et de lecture** qui assurera des temps de calcul raisonnables. À titre d'exemple, un ensemble de portes quantiques fonctionnant à la µs conduira à des temps de calcul de l'heure pour des milliards d'opérations quantiques ;
- **sa taille** qui permettra de conserver des tailles de circuits quantiques que l'on sait gérer (particulièrement important pour les qubits fonctionnant à basse température).

Les différentes plateformes physiques explorées pour l'ordinateur quantique

L'ordinateur ou l'accélérateur quantique sera constitué d'un cœur quantique à base de qubits (pour rappel, les qubits sont l'analogue de bits classiques ; ces systèmes à deux états peuvent être simultanément dans les deux états). Les principales approches de qubits pour le calcul à grande échelle sont présentées ci-dessous :

- **Les qubits à base de silicium :** en ce qui concerne l'intégration à large échelle, c'est le seul système physique qui remplit potentiellement tous les critères requis (vitesse de manipulation, fidélité des qubits, taille de la cellule élémentaire). Il s'appuie sur des technologies de la micro-électronique qui devraient faciliter la fabrication de qubits identiques et la réalisation de l'électronique de contrôle nécessaire pour piloter le cœur quantique. En revanche, la maturité de cette plateforme est faible : l'état de l'art aujourd'hui n'est encore que de deux qubits. Ceci s'explique par le fait qu'il faut un certain degré de maturité technologique que les laboratoires académiques ne peuvent atteindre. L'arrivée dans la compétition de grands acteurs de la micro-électronique, tant au niveau de la R&D que des industriels, pourrait accélérer la feuille de route ;
- **Les qubits à base de supraconducteurs :** ces systèmes sont les plus avancés en termes de nombres de qubits (Google annonce avoir fabriqué 72 qubits). L'avantage de la technologie est l'intégration aisée à partir de moyens de fabrication académiques. En revanche, la définition des deux niveaux du qubit se heurte à des limites physiques fondamentales qui ralentissent actuellement le passage à un grand nombre de qubits.

Ces deux premières approches requièrent un refroidissement des systèmes à des températures proches du zéro absolu. La cryogénie est toutefois devenue un outil standard et les spins qubits opèrent vers 1-10K quand les qubits supraconducteurs opèrent vers 50 mK. Pour les applications envisagées à l'heure actuelle, c'est-à-dire le calcul à haute performance, ces besoins cryogéniques ne sont néanmoins pas un frein au déploiement technologique (ils sont à mettre en regard des infrastructures aujourd'hui mises en place pour refroidir les serveurs de calcul).

- **Les qubits à base d'ions piégés :** cette approche s'appuie sur plusieurs décades de techniques permettant de piéger des ions dans des réseaux optiques. Ce système est sans conteste le plus avancé en termes de qualité des qubits. Ces systèmes présentent l'avantage de permettre un couplage à la lumière pour mise en réseau. L'enjeu est la miniaturisation et la faible vitesse des opérations ;
- **Les qubits à base de photons uniques :** l'information est codée sur un grain élémentaire de lumière et de nombreux degrés de liberté sont exploités pour augmenter l'espace de calculs (cou-

leurs des photons, polarisation, mode spatial, mode temporel, etc.). Se propageant à la vitesse de la lumière sur des puces optiques, cette technologie permet en principe une vitesse de calcul inégalée. Par ailleurs, elle est la seule technologie offrant une interface naturelle pour la mise en réseau des calculateurs quantiques et le calcul distribué. Ces technologies ont jusqu'à présent souffert de la faible efficacité des composants élémentaires, mais d'importants progrès ont vu le jour ces dernières années.

Enfin, mentionnons que d'autres approches sont explorées, mais non discutées ici, car à un stade de développement trop préliminaire. Certains de ces systèmes sont toutefois prometteurs, comme les qubits topologiques. Ces qubits auraient une immunité aux erreurs qui permettraient de s'affranchir des codes correcteurs, mais n'ont pas encore été démontrés expérimentalement de manière fiable.

Le tableau ci-dessous présente l'état de l'art des démonstrations expérimentales.

Pour aller à grande échelle, en plus des performances individuelles des qubits, la dispersion sur les propriétés individuelles et l'aptitude à contrôler un grand nombre de qubits de manière simultanée vont être prépondérantes dans les performances globales du système.

Ces questions sont aujourd'hui des questions de recherche ouvertes. Les moyens investis par les grandes compagnies et les levées de fonds de startups (allant de 20 M$ pour des entreprises récentes à plus de 200 M$ pour DWave) permettent néanmoins des avancées rapides.

	Superconductors	Silicon	Trapped ions	Photon
Size	$(100\ \mu m)^2$	$(100\ nm)^2$	$(1\ mm)^2$	1 mm2
Fidelity	~99.9%	>98%	99.9%	50% (measurement and generation) 98% (one and two-qubit gate)
Speed	200 ns	5 µs	100 µs	1 ms
Number of entangled qubits	17 (claimed 72)	2	20	18
Companies	IBM, Google, Intel, Dwave, Rigetti, QCI...	Intel, HRL, Silicon Quantum Computing	IonQ	Xanadu, Candela, HP, Tundra Systems
leading academic teams	UCSB, Yale, IBL Zurich, CEA, Berkeley, TU Delft, MIT	UNSW, CEA-CNRS Grenoble, Tokyo University, TU Delft, Princeton, Sandia, Uwisconsin, NTT	innsbruck, Oxford, NIST, UMaryland, Sussex, MIT	Oxford University

Nombre de qubits et taux d'erreur

Quelle que soit la plateforme explorée, le nombre de qubits n'est pas, loin s'en faut, le seul critère pour obtenir un calculateur quantique plus performant qu'un calculateur classique (suprématie ou avantage quantique). Xavier Vasques, directeur technique chez IBM France, indique : *« Le qubit n'est pas le seul paramètre, car il faut s'atteler à la gestion et la correction d'erreurs qui sont des opérations complexes »*. À ce jour, au-delà de la course au nombre de qubits, d'autres métriques apparaissent, notamment avec la possibilité de paralléliser des groupes de qubits. IBM définit le Quantum Volume qui illustre que la puissance d'un ordinateur quantique dépend du nombre de qubits et aussi du taux d'erreur. Cette seconde métrique place par exemple à 15 le nombre de qubit par groupe parallélisables[130].

Les performances de l'ordinateur quantique sont également algo-dépendantes et nécessitent une évaluation au cas par cas. En effet, les algorithmes classiques doivent être repensés pour avoir une version quantique et nécessitent une évaluation spécifique.

Recommandations

Après les preuves de concept de faisabilité de portes à un ou deux qubits, la question de la mise à l'échelle soulève de nombreux problèmes d'ingénierie et de science (ex. : les liaisons à grande distance pour les systèmes solides). La France possède à la fois des connaissances fortes en information quantique, de solides compétences technologiques et une recherche d'excellence en mathématiques et informatique appliquée. Avec un soutien industriel idoine, elle pourrait prendre un rôle majeur dans la fabrication du premier ordinateur quantique à grande échelle.

Efficacité énergétique du calcul quantique

C'est en partie aux problématiques énergétiques (liées notamment à la miniaturisation des composants et au refroidissement des serveurs nécessaires au stockage d'un nombre de plus en plus grand de données) que l'on doit l'explosion des technologies quantiques. En effet, le déroulement d'un calcul quantique est en principe réversible et, d'autre part, il comporte *a priori* moins d'étapes que son équivalent clas-

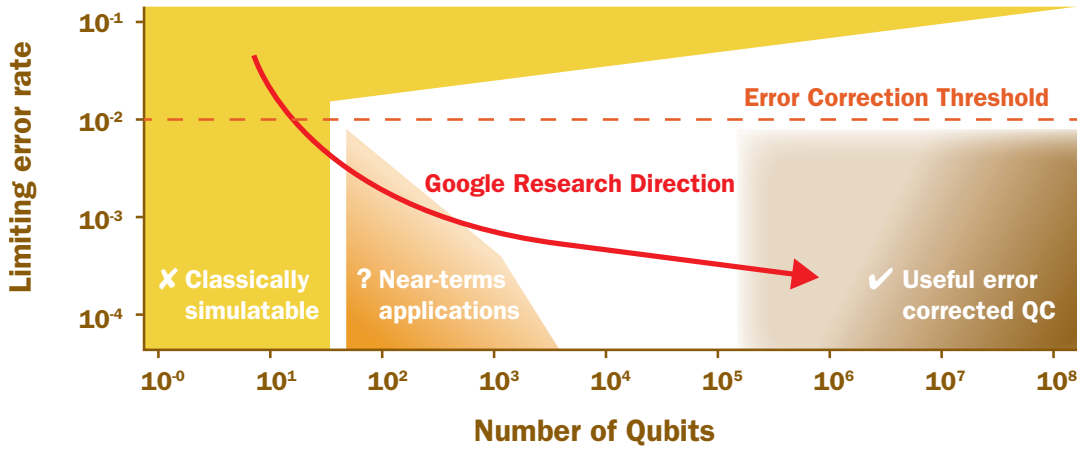


Figure 9 : la version de Google, proposant sur un graphique le lien taux d'erreurs/nombre de qubits[131]

130. www.research.ibm.com/ibm-q/resources/quantum-volume.pdf.

sique : deux raisons fondamentales pour lesquelles les coûts énergétiques liés au traitement de l'information quantique devraient être moins élevés.

Cependant, ce raisonnement ne tient pas compte de la nécessaire lutte contre la décohérence et le bruit d'origine quantique. La mise en œuvre de codes correcteurs d'erreur et le développement d'architectures de calcul « *fault tolerant* » requièrent l'utilisation de grands nombres de qubits additionnels dont le contrôle pourrait conduire à d'importants surcoûts énergétiques. L'analyse détaillée de ces surcoûts pourrait déboucher sur une classification des architectures de qubits en fonction de leur consommation énergétique.

Recommandations

La question de l'énergétique du calcul joue un rôle fondamental dans le développement et l'optimisation des architectures de calcul classique. La question est en passe de devenir stratégique dans la perspective de développer des calculateurs à l'échelle, mais est actuellement largement sous-représentée dans les *roadmaps* autour des technologies quantiques de l'information. Un dialogue entre recherche fondamentale et R&D devrait s'établir autour de ces questions.

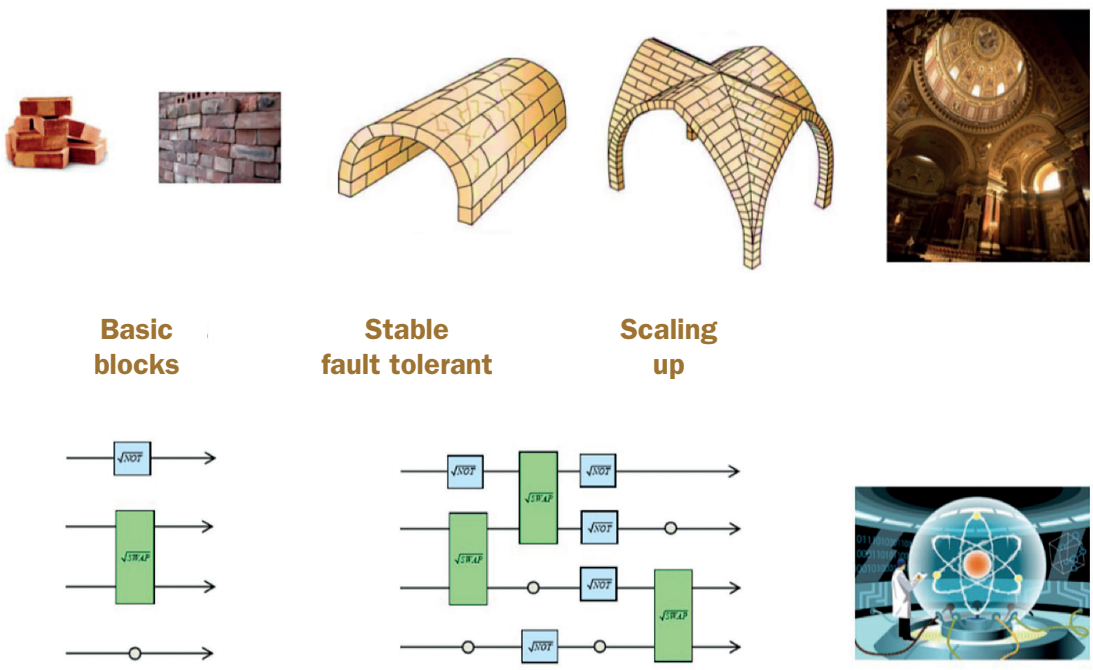


Figure 10 : construire des ordinateurs quantiques (source : la présentation d'Artur Ekert – « Is the age of computation yet to begin? »)

Hardware des communications quantiques

Du côté des **communications sécurisées** par les lois de la mécanique quantique, les hardwares développés sont mieux identifiés et dépendent des applications envisagées. Une première application des technologies quantiques est la **distribution de clés cryptographiques** entre deux points géographiques. Dans ce cas, le niveau de TRL du développement du hardware est élevé avec une commercialisation maintenant internationale de système clé en main de cryptographie (ID Quantique…) et le début du déploiement à grande échelle (voir le récent communiqué de presse de la société suisse ID Quantique, financé à hauteur de 65 M€ par l'équipementier Coréen SK Telecom).

Une autre application des communications quantiques concerne le développement d'un véritable réseau, type « internet quantique », dont la sécurité sera également garantie par les lois de la mécanique quantique. Ce type de réseau est le complément indispensable au développement des ordinateurs quantiques, permettant de préserver la sécurité des liens entre ordinateurs quantiques et permettant l'utilisation de calculateurs en réseau pour décupler les puissances de calculs. Pour développer ces réseaux quantiques, plusieurs architectures sont envisagées, reposant sur différents hardwares. Ces derniers comprennent par exemple des détecteurs et sources de lumières quantiques qui ont atteint le marché de l'instrumentation ces dernières années (voir par exemple les sociétés SingleQuantum, QuantumOpus, Quandela, SparrowQuantum, PhotonSpot…). Nous dressons ci-après un rapide panorama du hardware développé pour le calcul et les communications sécurisées ainsi que le coût énergétique des technologies quantiques.

En ce qui concerne les démonstrations pratiques, la performance des liaisons point à point est évaluée par la distance à laquelle les clés secrètes peuvent être distribuées et par le taux de génération de la clé secrète pour un niveau de sécurité donné.

On remarque deux limitations inhérentes pour de tels systèmes :

- **La distance maximale de communication qui peut être atteinte sur des canaux de fibre optique :** L'atténuation de la lumière à la longueur d'onde des télécommunications (1550 nm) étant de l'ordre de 0,2 dB/km, les pertes engendrées par la propagation dans le canal limitent la portée des liens QKD point à point à quelques centaines de kilomètres : au-delà, générer un seul bit de clé secrète nécessiterait plusieurs années, même en utilisant des sources et des détecteurs de lumière parfaits, ce qui présente peu d'intérêt pratique. L'extension de la portée des systèmes QKD est un défi majeur pour les applications du domaine. Pour les systèmes basés sur la détection de photon unique, le facteur-clé est la possibilité d'utiliser de vraies sources de photons uniques efficaces et le bruit de ces détecteurs. Des sources de photons uniques efficaces sont en cours de développement et commencent à être commercialisées (Quandela, Sparrow Quantum). Un enjeu est de transférer ces technologies aujourd'hui fonctionnant à 900 nm vers

les longueurs d'onde télécom. Les détecteurs basés sur des nano fils supraconducteurs (SNSPD – *superconducting nanowire single photon detectors*) sont des dispositifs extrêmement prometteurs pour les communications quantiques grâce à leur efficacité élevée et leurs faibles temps morts, taux de coups d'obscurité et incertitude temporelle, et sont commercialement disponibles. Pour les systèmes à variables continues, le facteur crucial est l'excès de bruit – le bruit excédant le bruit de photon fondamental des états cohérents – qui doit être le plus bas possible. Afin de franchir les distances à l'échelle mondiale, il est nécessaire de recourir à deux approches : des structures réseaux (voir Section C) et des liens satellitaires.

- **Le taux maximal de génération de clé secrète possible en utilisant des canaux de communication pratiques, et donc bruités, ce qui est sujet à des limitations théoriques récemment déterminées :** En pratique, les clés de chiffrement produites par la QKD peuvent être utilisées dans un schéma de chiffrement symétrique comme le protocole AES (*Advanced Encryption Standard*) qui est résistant à une attaque par ordinateur quantique ou encore être combinées avec la méthode de masque jetable afin d'obtenir une sécurité absolue. Dans les deux cas, le taux de clé obtenu par la couche QKD sous-jacente pour un scénario d'application typique est crucial. Des taux plus élevés permettent une mise à jour plus fréquente de clés de chiffrement dans le cas du chiffrement symétrique et une augmentation proportionnelle de la bande passante de communication dans le cas du chiffrement à masque jetable. Actuellement, il existe encore une forte disparité entre les débits de communications optiques classiques et la QKD. Des taux de plusieurs centaines de gigabits par seconde et par canal de longueur d'onde sont atteints aujourd'hui par des méthodes classiques, tandis que des taux de l'ordre du mégabit par seconde sur quelques dizaines de kilomètres sont réalisés par des systèmes QKD. Ces derniers sont suffisants par exemple pour la transmission vidéo ; cependant, pour chiffrer de grands volumes de trafic de réseau classique en utilisant la cryptographie à masque jetable, il sera nécessaire d'augmenter de façon significative le taux de clés secrètes produites par la QKD. Comme pour le défi de la portée, les performances des détecteurs sont cruciales pour tous les types de protocoles. Il est aussi possible d'utiliser le multiplexage en longueur d'onde ou en mode spatial qui est une technologie utilisée couramment en communications optiques.

En plus des limitations de performance analysées ci-dessus, un défi important pour les prochaines années sera le développement des systèmes permettant de réduire la complexité, les coûts et la consommation de puissance. L'intégration photonique offre un niveau de miniaturisation élevé, ouvrant la voie à des modules compacts qui peuvent être produits en masse à bas coût. Le déploiement des systèmes répondant aux exigences des applications pratiques sera aussi grandement facilité par la coexistence dans la même fibre des signaux quantiques avec le trafic des données usuelles, éliminant le besoin pour des fibres dédiées.

4.6 THÉMATIQUE « INGÉNIERIE LOGICIELLE ET OUTILS DE DÉVELOPPEMENT »

L'informatique classique d'aujourd'hui repose sur une architecture de type Von Neumann composée d'une unité de calcul (processeur) manipulant des bits, d'une mémoire vive (RAM), d'unités de stockage et de composants de gestions de périphériques et d'entrées/sorties. La gestion de ces ressources matérielles est assurée par le système d'exploitation (Windows, Mac, Linux…) mettant à disposition les ressources matérielles nécessaires à l'exécution des algorithmes pour répondre à un besoin applicatif spécifique.

Aujourd'hui, les développeurs utilisent généralement des langages de programmation évolués (Python, C++, Java, …) qui, intégrés dans des outils de développement, traduisent et compilent les programmes des développeurs en langage machine directement exécutables par le processeur.

Comme nous l'avons vu dans les précédentes thématiques, les processeurs quantiques et leur programmation sont bien différents des processeurs actuels. L'exploitation des superpositions d'états des qubits remet en cause les architectures matérielles et logicielles, ainsi que le principe du tiers exclus sur lequel repose la logique des prédicats.

Outil de développement	Éditeur	Description/Liens
Plateforme de simulation quantique	Atos	Plateforme basée sur du hardware classique qui permet aux chercheurs de tester dès maintenant des algorithmes et des logiciels pour les futurs calculateurs quantiques.
aQasm	Atos	Langage de programmation universel.
Google's Quantum Computing Playground	Google	Kit de développement.
QISKit (Quantum Information Software Kit)	IBM	Kit de développement QISKit. Lien : www.qiskit.org.
Composer IBM Q	IBM	Environnement en ligne de simulation et d'exécution sur processeurs quantiques. Lien : quantumexperience.ng.bluemix.net/qx/editor.
XACC (EXtreme scale ACCelerator)		Interfaces avec le simulateur Rigetti et les systèmes D-Wave en production.
QuTiP (Quantum Toolbox in Python)	Open source	Simulateur open source utilisé sur un grand nombre de plateformes hardware (logos de Alibaba, Amazon, Google, Honeywell, IBM, Intel, Microsoft, Northrup Grumman, Rigetti, et RIKEN visibles sur leur site).
OpenFermion	Google et Rigetti	Package logiciel pour compiler et analyser des problèmes de chimie quantique.
Microsoft Language-Integrated Quantum Operations: LIQUi|>	Microsoft Research	Architecture logicielle et suite d'outils pour convertir un algorithme quantique codé dans un langage de haut niveau dans les instructions de bas niveau requises pour un ordinateur quantique.
Microsoft Quantum Development Kit	Microsoft	Fournit le support pour programmer des algorithmes quantiques dans le langage Q#.
Q# (« Q-sharp »)	Microsoft	Langage de programmation pour ordinateur quantique. Microsoft, lors de la conférence Ignite fin septembre 2018 à Orlando, a annoncé la mise à disposition prochaine d'un nouveau langage de programmation pour l'informatique quantique. Ce langage est intégré dans Visual Studio et comprend un simulateur d'ordinateur quantique qui fonctionne sur un poste de travail, mais aussi sur le Cloud Azure en supportant jusqu'à 40 qubits. Ce nouveau langage contient toutes les fonctionnalités nécessaires pour un développeur dans un environnement quantique, notamment le traitement du cas de l'utilisation de qubits, de bits, la notion de «mesure» et les conditions de la mesure ainsi qu'un langage entièrement nouveau qui génère du code C#.

Cela nécessite une refonte totale des systèmes d'exploitation, des outils de développements, des langages de programmation et la démarche de spécification et de développement logiciel.

Outils de développement

À ce jour, il existe essentiellement des plateformes de simulation d'algorithmes quantiques basées sur du hardware classique, des environnements de développement (IDE) et des langages de programmation de type assembleur pour les ordinateurs quantiques à portes logiques. Des programmes de recherche visent à mettre au point des environnements de développement avec des langages de plus haut niveau.

Le tableau page précédente liste les principaux outils de développement existants actuellement.

4.7 THÉMATIQUE « CONDUITE DU CHANGEMENT, NOUVEAUX MÉTIERS, FORMATION, ÉDUCATION, ET ENJEUX RÉGLEMENTAIRES, JURIDIQUES ET ÉTHIQUES »

Comme évoqué dans les thématiques précédentes, l'informatique quantique va transformer radicalement dans les années à venir les architectures matérielles et logicielles des systèmes d'information et apportera de très nombreuses opportunités de développements de nouvelles applications ou cas d'usages.

La nouvelle ère engendrée par cette nouvelle informatique nécessite une conduite du changement, car la technologie quantique sera déployée, utilisée et valorisée progressivement par tous les acteurs de l'entreprise. Pour répondre aux nouvelles règles du jeu, la question des relations entre innovations technologiques, décisions stratégiques et reconfigurations organisationnelles doit être posée.

La réussite de cette nouvelle ère quantique dépend des acteurs de l'entreprise, car il n'y aura pas d'avancée majeure sans leur implication. Les entreprises doivent considérer que leurs développements dépendent de la motivation, de la mobilisation et de l'implication de l'ensemble de leurs collaborateurs.

Le changement organisationnel doit être accompagné par la conduite du changement, c.-à-d. l'ensemble des activités qui amènent une organisation d'un état actuel vers un état futur souhaitable dans le cadre de la stratégie définie par sa direction.

Ce changement est un acte indispensable pour accompagner la transformation générée par les nouvelles solutions possibles (qu'elles soient hybrides ou exclusivement quantiques). La réussite de cette transformation apportée par cette nouvelle technologie passe par l'acceptation et l'adaptation de nouveaux outils, usages et habitudes. La conduite du changement doit être mise en place rapidement, car le quantique passera par une phase de transition relativement longue du fait de l'hybridation et de l'interaction pendant de nombreuses années entre le monde quantique et le monde traditionnel. De plus, l'éducation, la communication et les formations sont essentielles.

Formation initiale et continue

La formation initiale, à peine existante en France aujourd'hui, doit permettre de former les prochains utilisateurs, promoteurs et experts ingénieurs/scientifiques. En effet, en plus des nouveaux spécialistes indispensables au développement de cette nouvelle informatique, une nouvelle industrie et de nouveaux usages vont apparaitre, entraînant des formations initiales auprès des futurs commerciaux et utilisateurs. Par ailleurs, de très nombreux sujets de recherche fondamentale et appliquée existent déjà et vont sensiblement croître. Des formations pour de futurs chercheurs dans ce domaine devraient se développer.

L'arrivée de l'informatique quantique entrainera l'évolution de certains métiers existants comme l'architecte matériel et logiciel ou l'architecte intégrateur de technologie et l'apparition de nouveaux métiers :

- mathématicien spécialisé en modélisation et simulation quantique ;
- ingénieur en cryptographie quantique et post-quantique ;
- architecte spécialisé en architecture hybride classique et quantique ;
- informaticien spécialisé en informatique quantique théorique ;
- informaticien spécialiste en développement d'outils de développement et de langage de programmation.

Quant aux entreprises, elles devront se doter de programmes de formation continue pour accompagner les salariés éligibles à l'accès aux nouveaux métiers listés ci-dessus.

Enjeux réglementaires, éthiques et juridiques

La puissance de calcul théorique des prochains calculateurs quantiques apportera aux détenteurs (entreprises, états…) de cette nouvelle technologie une suprématie assurée. Cela nécessitera, à l'instar des solutions mettant en œuvre des techniques d'intelligence artificielle ou des techniques de machine learning, des réglementations assurant la réglementation des usages, la transparence, le contrôle de loyauté et la traçabilité des algorithmes développés. Des problèmes d'éthique semblent se dessiner, évoqués dans « *The potential impact of quantum computers on society* », Wolf (2017)[131].

Un enjeu particulier : la sécurité des données personnelles (RGPD)

La prise en compte du risque quantique doit être intégrée dans les exigences de protection des données personnelles, en particulier la RGPD. L'effervescence médiatique et technique autour de la suprématie quantique est également contemporaine de l'arrivée du cadre réglementaire européen sur la protection des données personnelles (RGPD). À ce titre, le niveau

131. www.arxiv.org/abs/1712.05380.

de protection des droits des citoyens européens devrait être équivalent dans tous les États membres, tel que le précise le considérant 10 du RGPD. Mais alors, quel sera l'impact de l'ordinateur quantique sur cette fédération européenne en matière de sécurité de la donnée ?

Et la loi dans tout ça ?

L'idée de la suprématie quantique est une vision technique qu'il est nécessaire d'appréhender dans le cadre légal. Le règlement européen est ainsi composé en grande partie de renvois aux lois des pays membres. Leur objectif est, entre autres, de responsabiliser les entreprises qui traitent de données personnelles et de renforcer la protection de celles des citoyens européens en invitant lesdites entreprises à gagner la confiance des utilisateurs. Du côté pénal français, les articles 323 du Code pénal français sont clairs en termes de sanctions et la CNIL a d'ailleurs fait savoir qu'elle n'hésitera pas à les appliquer en cas de manquement à l'entrée en vigueur du RGPD.

Oui, mais en pratique…

Les menaces informatiques concernent fréquemment les données personnelles. On pensera aux trois milliards de comptes Yahoo piratés en 2013 alors que les auteurs de l'attaque ne sont toujours pas identifiés. À ce jour, les hackers s'attaquent avec des techniques non quantiques aux failles sécuritaires et l'opération « Hack The Pentagon » en 2016 a révélé que le plus sophistiqué des systèmes d'information au monde contient toujours des vulnérabilités exploitables. La question de la sécurité des systèmes d'information reste toujours posée et, dans ce contexte, disposer d'un ordinateur quantique permettrait, s'il se trouve entre de mauvaises mains, des attaques bien plus efficaces et dangereuses.

En conclusion

La question de la RGPD face au quantique se rapproche ainsi de celle de l'éthique dans l'utilisation des nouvelles technologies. Le paradoxe est que les futurs propriétaires des ordinateurs quantiques seront les géants de l'information, c'est-à-dire des multinationales dont la puissance défie les états.

Annexes

Annexe 1. Pour aller plus loin

Pour une introduction en anglais aux concepts du « Quantum Computing », voir : A quantumcomputingprimer–Intel:newsroom.intel.com/newsroom/wp-content/uploads/sites/11/Quantum_Computing.png.

- Frequently Asked Questions General questions about quantum information science : quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=full-user-guide&page=000-FAQ~2F000-Frequently_Asked_Questions.
- Quantum computers could crack bitcoin, but fixes are available now : www.theregister.co.uk/2017/11/09/quantum_computers_could_crack_bitcoin.

Pour une version en français, le lecteur peut se référer au site du CEA : L'essentiel sur… la mécanique quantique : www.cea.fr/comprendre/Pages/physique-chimie/essentiel-sur-mecanique-quantique.aspx.

Annexe 2. Les acteurs en cryptographie

Catégorie	Sous-catégorie	Technologie	Acteur	Lien
Solutions quantiques de cryptographie	Chiffrement et communication	QKD	ID-Quantique	www.idquantique.com
			De nombreuses équipes académiques pour divers protocoles : en France LIP6, Sorbonne Université ; en Europe, Université de Genève, Max Planck à Erlangen, University of Vienna, ICFO Barcelona, University of Bristol, University of Padova, Lancaster University	www.quantuminfolip6.fr www.lancaster.ac.uk/physics/about-us/people
			Toshiba	www.toshiba.co.jp/about/press/2017_09/pr1501.htm
			Huawei Munich	www.huawei.com/de
		Algorithmes de cryptographie quantique	ATOS	atos.net/fr/vision-et-innovation/atos-quantum
	Autres primitives quantiques dont authentification, identité, argent et méthodologies	Q-ID	QuantumBase	www.quantumbase.com
		Quantum Risk Assessment	Evolution Q	www.evolutionq.com
		Theoretical Quantum Cryptography, QKD, Cryptography beyond QKD	Paris Centre for Quantum Computing	www.pcqc.fr
		Réseau quantique	VeriQloud	www.veriqloud.com/
	Internet quantique, satellite quantique	Secure, unhackable net	Quantum Internet Alliance	www.quantum-internet.team
			UCL-led-team of scientists	www.ucl.ac.uk/quantum
		QKD + satellite	Quantum Experiments at Space Scale (QUESS)	fr.wikipedia.org/wiki/QUESS
			Space-QUEST consortium	Arxiv paper
Cryptographie post-quantique	Chiffrement	Crypto post-quantique	RISQ, Regroupement de l'Industrie française pour la Sécurité Post – Quantique	www.risq.fr/?page_id=8&lang=fr
			IBM	www.zurich.ibm.com/securityprivacy/quantumsafecryptography.html
			CNRS	www.cnrs.fr/inp/spip.php?article1675
			Secure-IC	www.secure-ic.com

Annexe 3. Les grandes étapes du développement d'un internet quantique

Un grand nombre d'équipes au niveau international travaillent au déploiement de cet internet quantique. Un consortium européen baptisé « Quantum Internet Alliance » a proposé six grandes étapes technologiques au développement d'un tel réseau de communication à base de mémoires quantiques. De plus, chaque étape de ce développement permet de déployer de nouvelles applications qui ne sont possibles qu'avec les réseaux quantiques.

La **première étape** est celle que nous connaissons aujourd'hui. Dans les réseaux quantiques actuels, chaque nœud peut émettre des qubits, les envoyer à son ou ses voisins qui mesurent immédiatement l'information reçue. Un tel réseau permet de mettre en œuvre la QKD (*Quantum Key Distribution*) entre deux points arbitraires du réseau, à condition que les points intermédiaires ne soient pas contrôlés par un éventuel espion.

Dans la **seconde étape**, des répéteurs quantiques installés sur le réseau permettent d'augmenter considérablement la distance de transmission des qubits. Ainsi, un qubit peut voyager d'un nœud à un autre, sans être mesuré par les nœuds intermédiaires. Les utilisateurs du réseau peuvent s'échanger des qubits pour garantir leurs positions géographiques de manière infalsifiable. La communication quantique peut être utilisée pour améliorer la sécurité de tâches cryptographiques, comme le vote électronique.

Dans la **troisième étape**, les qubits envoyés peuvent être intriqués avec les uns avec les autres. La cryptographie change de visage et devient *device-independent*. Ceci permet, pour des tâches comme l'échange de clés de chiffrement, de garantir la sécurité même si le matériel utilisé a été altéré par un adversaire qui cherche à en prendre connaissance.

Dans la **quatrième étape**, les nœuds sont équipés de mémoires quantiques, autorisant des protocoles de communication plus complexes. Un utilisateur du réseau peut déléguer un calcul à un nœud distant *à l'aveugle,* c'est-à-dire que le nœud exécute son calcul sur des données chiffrées sans en comprendre la signification. Les communications anonymes deviennent possibles et les télescopes peuvent être reliés entre eux via un réseau quantique afin d'améliorer la résolution des images obtenues. Les systèmes de calcul distribué tirent parti de ressources quantiques pour, par exemple, améliorer la détection d'erreur lorsque des données sont répliquées sur plusieurs serveurs.

Dans la **cinquième étape**, le calcul tolérant aux fautes devient possible à chaque nœud sur un petit nombre de qubits, étendant ainsi le temps de stockage de l'information. Grâce à cela, la précision de la synchronisation des horloges connectées au réseau quantique s'améliore considérablement.

Enfin, dans la **dernière étape**, l'ensemble des améliorations technologiques est *scalable*. Chaque nœud contient un grand nombre de qubits, l'intrication est maîtrisée et stable et la correction d'erreur est parfaite. Tous les protocoles de communication quantique connus peuvent alors être implémentés. Ceci permet, dans certains cas, de réduire exponentiellement le coût des communications. Les systèmes de calcul répartis deviennent encore plus efficaces.

Chaque étape de ce développement repose sur des modifications profondes du hardware utilisé. Ces modifications dépendent à leur tour d'avancées scientifiques conséquentes. Toutefois, la variété des protocoles présentés ici montre bien le bénéfice que l'on pourrait tirer de telles avancées.

Annexe 4. Hardware

Qubits à base d'ions piégés

Historiquement, les premiers qubits ont été démontrés en physique atomique. La raison principale est la protection relative du degré de liberté interne des systèmes atomiques en raison de leur échelle microscopique. À ce jour, le meilleur système en physique des systèmes atomiques est le piège à ions où l'information est stockée dans les états hyperfins d'ions comme Ca +, Be +...

Les ions sont en lévitation sous vide et capturés dans un piège (Pauli trap) par des moyens électriques. La manipulation ainsi que la détection des états qubit sont effectuées à l'aide d'une excitation laser avec une échelle de temps de quelques dizaines de microsecondes. Les ions sont, d'un ordre de grandeur, le système le plus cohérent démontré jusqu'à présent avec un taux d'erreur pour la manipulation de qubit et des portes de l'ordre de 10-4 compatibles avec la plupart des protocoles de correction d'erreurs quantiques.

Même si les contraintes de manipulation cohérente dans les pièges à ions et la grande taille effective du qubit avec toutes les fonctionnalités quantiques semblent difficilement compatibles avec une architecture à très grande échelle, des processeurs ont été démontrés dans ces systèmes et une perspective de quelques dizaines de qubits dans un futur proche est très plausible.

En ce qui concerne la question cruciale de l'intégration à grande échelle, la gamme des choix possibles devient beaucoup plus étroite. À cet égard, les qubits à l'état solide et les photons sont en principe bien positionnés en raison de la possibilité naturelle de réaliser des architectures intégrées rassemblant toutes les fonctionnalités quantiques et de leur compatibilité avec la technologie de nano-fabrication.

Qubits supraconduteurs

Parmi les approches à l'état solide, les qubits basés sur des éléments supraconducteurs ont atteint le niveau de développement le plus avancé. Historiquement, les manipulations cohérentes dans les qubits supraconducteurs ont été démontrées beaucoup plus tard que dans la physique des systèmes atomiques ou à ions en raison du fort couplage à l'environnement de l'état solide.

Contrairement à l'ion piégé, les qubits supraconducteurs sont des systèmes macroscopiques et les états quantiques sont des états quantiques collectifs résultant du mouvement de milliards d'électrons dans des matériaux supraconducteurs et contrôlés par l'incorporation de jonctions Josephson. Ils sont conçus de façon déterministe sur une puce à l'aide de techniques de nano-fabrication relativement bon marché. Après une longue étude de leur couplage à l'état solide, les qubits supraconducteurs atteignent maintenant une haute-fidélité pour la manipulation des qubits et des portes avec des taux d'erreur de deux qubits de l'ordre de 10-2 compatibles avec les procédures de correction d'erreurs topologiques seulement.

Leur sensibilité relative permet une conduite rapide du qubit supraconducteur et une échelle de temps typique de quelques dizaines de nanosecondes, trois ordres de grandeur plus rapides que les systèmes de pièges à ions. La fabrication de processeurs composés de quelques dizaines de qubits a été récemment réalisée avec un contrôle cohérent démontré très récemment sur des processeurs de 18 bits. Les perspectives d'intégration dense, compacte et au-delà de la 2D sont encore une question ouverte en raison de la taille relativement grande des bits pour intégrer toutes les fonctionnalités quantiques (100 µm par qubit). Néanmoins en 2018, Google a déjà annoncé un processeur à base de supraconducteurs Bristlecone à 72 qubits au March Meeting de San Francisco et IBM propose en ligne une offre de service IBMQ pour accéder à ses processeurs supraconducteurs à 16 qubits.

Qubits dans le silicium

Par rapport aux plateformes physiques les plus avancées mentionnées ci-dessus (qubits supraconducteurs [Dev13] et pièges à ions [Mon13]), les qubits de silicium ont un historique de développement plus récent. Ici, le bit élémentaire de l'information quantique est codé dans un degré de liberté de spin, tel que le moment magnétique d'un électron [Los98] ou celui d'un noyau [Kan98]. Les qubits de spin partagent donc avec les systèmes atomiques la protection relative à l'environnement en raison de leur taille microscopique.

Par le déclenchement local, on peut changer la charge contenue dans le point et réussir à piéger les électrons individuels. De plus, en appliquant un champ magnétique, la dégénérescence entre les états spin up et spin down est levée et le degré de liberté de spin peut être étudié. Dans

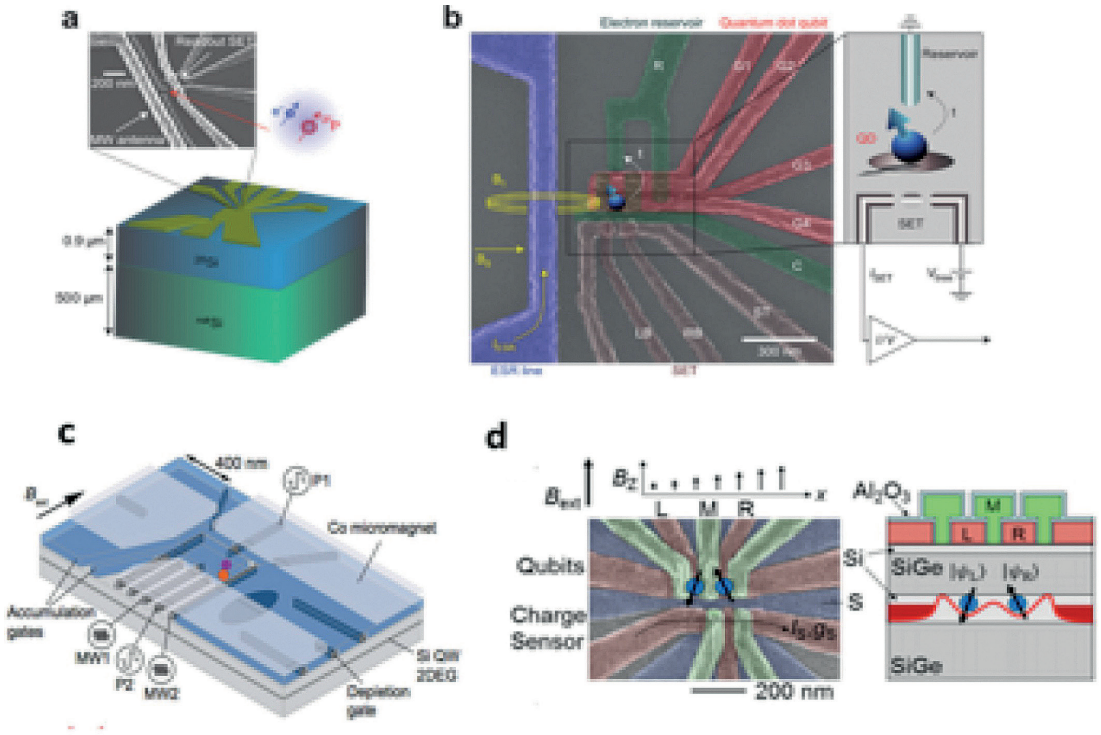


Figure 11 : exemple de réalisation de systèmes à qubits de spin. Rangée du haut : qubits de spin UNSW Si fabriqués sur 28Si purifié isotopiquement

ce domaine, la possibilité de mesurer [Elz04] et de contrôler de façon cohérente [Kop06] un spin d'un seul électron est maintenant bien établie.

Les premiers qubits uniques reposant sur des spins d'électrons confinés dans le silicium n'ont été réalisés qu'en 2012. Depuis lors, leur développement en termes de réalisation de porte a été relativement rapide, également grâce à l'introduction de 28Si purifié de manière isotopique, conduisant à une grande amélioration de la cohérence de spin. Suivant différentes approches, plusieurs groupes de recherche ont réalisé des portes quantiques à un ou deux qubits avec des fidélités déjà élevées et en amélioration. Très récemment, des fidélités à un seul seuil > 99,9 % et des portes à deux queues avec des fidélités supérieures à 90 % ont été rapportées.

En fait, le paramètre de performance pertinent pour quantifier la qualité d'un bit quantique est le nombre d'opérations quantiques effectuées dans le temps de cohérence. Les expériences mentionnées ci-dessus indiquent que les qubits de spin électronique de Si ont progressé rapidement et déjà obtenu des performances comparables aux meilleurs qubits supraconducteurs [Dev13].

En plus de longs temps de cohérence et de faibles erreurs de porte quantique, les qubits de spin de silicium ont d'autres avantages potentiels qui les rendent aptes à une intégration à grande échelle, avec une perspective encore plus grande que les qubits supraconducteurs. Le premier avantage réside dans la compatibilité inhérente à la technologie du silicium. Le contrôle et la reproductibilité exceptionnels sur les processus de fabrication des dispositifs en silicium et l'accès au développement le plus avancé dans l'intégration 3D compacte sont certainement un atout pour l'intégration de qubits à grande échelle.

Plus précisément, il permettra de tirer parti du qubit de spin avec toutes les fonctionnalités quantiques dont la taille est inférieure à un micron carré et donc potentiellement d'atteindre un million de bits dans une cellule inférieure à un mm^2. De plus, les qubits peuvent être directement couplés à une électronique intégrée sur puce. En raison des propriétés mentionnées ci-dessus, les qubits de spin de silicium fournissent l'une des voies les plus prometteuses pour les ordinateurs quantiques évolutifs, mais en sont encore au niveau des portes uniques.

Les processeurs à base de photons

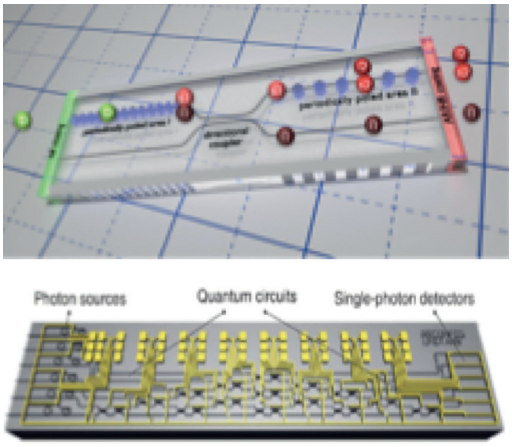


Figure 12 : exemple de réalisation de calculateurs optiques, à base de Niobate de Lithium (haut, Paderborn) et silicium (bas, Bristol, UK)

Les processeurs optiques sont développés depuis une dizaine d'années. Le nombre de qubits manipulés est typiquement de l'ordre de 12, record détenu par le groupe de J.W. Pan à Hefei en Chine.

Des calculs quantiques ont été implémentés avec code de correction d'erreur et de nombreuses plateformes intégrées sont développées pour générer les photons uniques et réaliser les calculs sur puce : silicium, niobate de lithium, etc. Des calculateurs de plus en plus complexes sont réalisés, utilisant des méthodes de fonderies traditionnelles pour réaliser les puces optiques.

Les calculateurs optiques reposent sur trois ingrédients : des sources de lumière quantique (photons uniques), des puces optiques programmables pour réaliser le calcul et des détecteurs de photons. Hormis les sources et détecteurs qui peuvent requérir un refroidissement cryogénique simple (10K), le calculateur lui-même est opéré à température ambiante, permettant de changer le processus de façon très versatile. Enfin, le calculateur optique, basé sur les photons uniques est la seule architecture qui permet naturellement d'implémenter des calculs quantiques distribués et d'intégrer les calculateurs quantiques dans des réseaux. Ils peuvent par ailleurs opérer à très grande vitesse et ne souffrent pas de décohérence, hormis les pertes optiques.

Depuis 2012, des détecteurs à bases de nano-fils supraconducteurs très efficaces ont vu le jour et sont maintenant commercialisés (SingleQuantum, PhotonSpot, QuantumOpus). Cependant, le développement de ces calculateurs optiques a récemment été freiné par l'absence de solution technologique viable pour la génération efficace de photons uniques à grande échelle. Les méthodes utilisées ont longtemps consisté à utiliser des sources de photons annoncés : une paire de photons est créée de façon aléatoire et la détection d'un photon de la paire annonce la présence de l'autre. Ces sources ont des efficacités intrinsèques limitées aux 1 %, limitant fortement le nombre de qubits générés par seconde. Par ailleurs, cette faible efficacité a longtemps conduit à un compromis entre la qualité des calculs et leur vitesse.

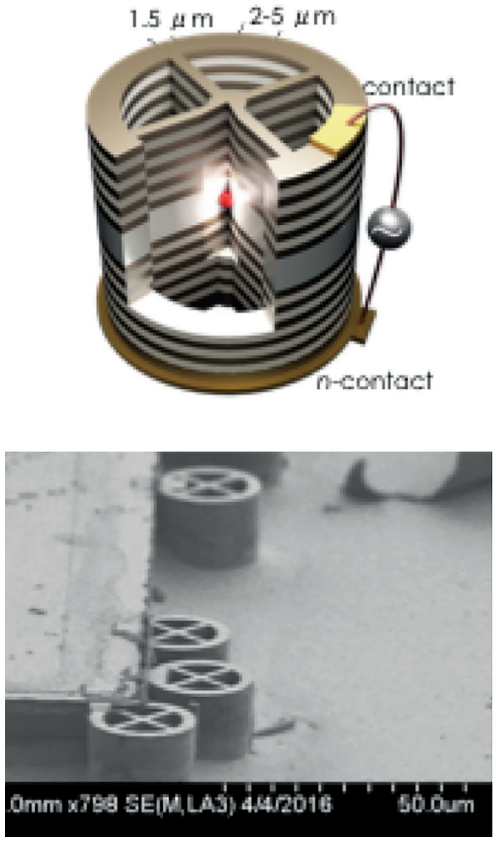


Figure 13 : illustration d'une source de photon unique de haute efficacité à base de boîtes quantiques semi-conductrices commercialisée depuis 2017 par Quandela, spin-off issue du CNRS

Ces dernières années ont vu l'émergence de sources de photons uniques véritables, à base de boites quantiques semi-conductrices, offrant des efficacités de 30 à 80 %. Développées en 2016, ces sources ont d'ores et déjà permis de manipuler 7 photons en gagnant 7 ordres de grandeur en vitesse par rapport aux sources annoncées.

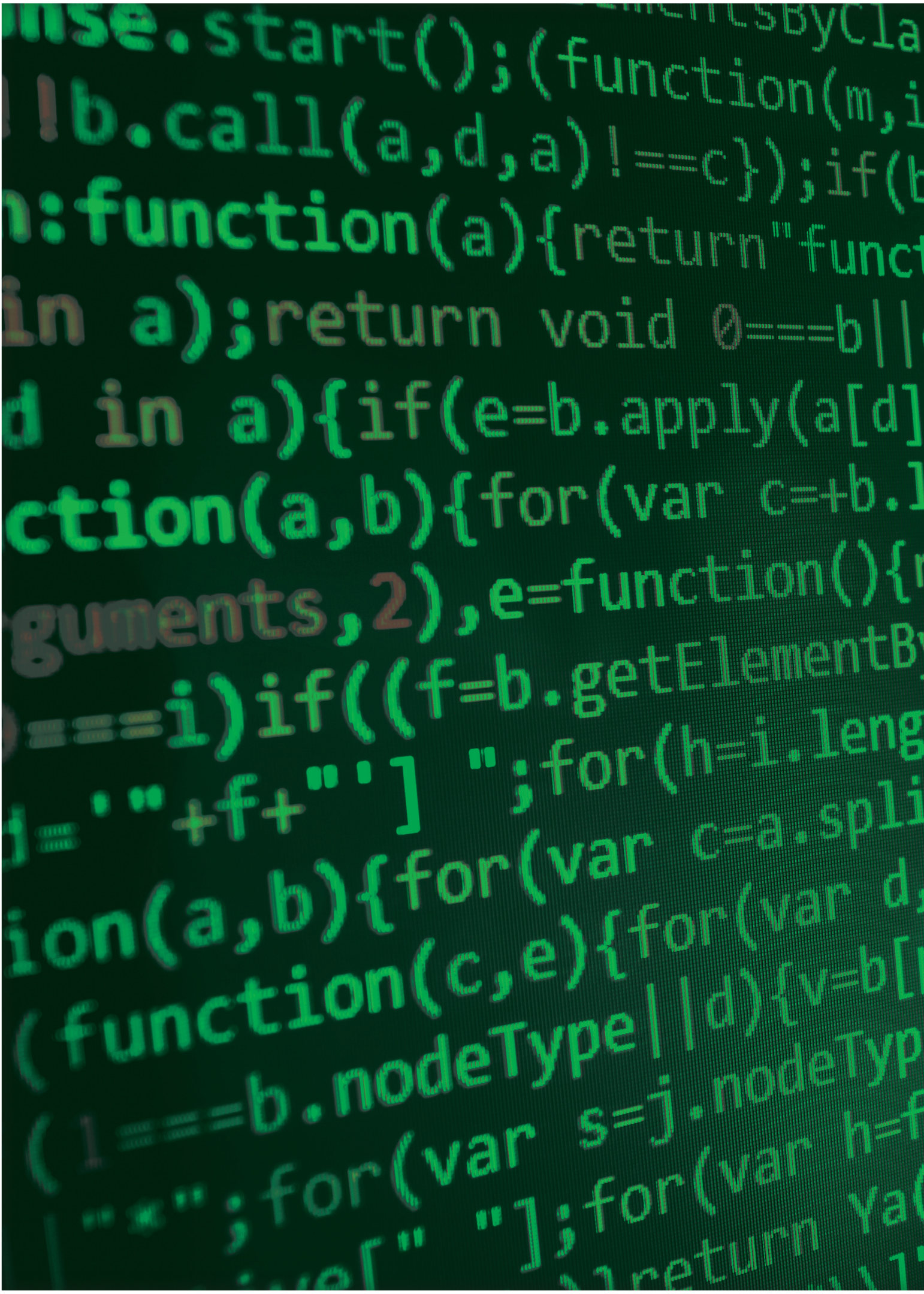
Par ailleurs, ces nouvelles sources présentent une grande pureté quantique, indépendamment de leur efficacité, de sorte que leur utilisation laisse prévoir une très forte baisse des erreurs dans les calculs également.

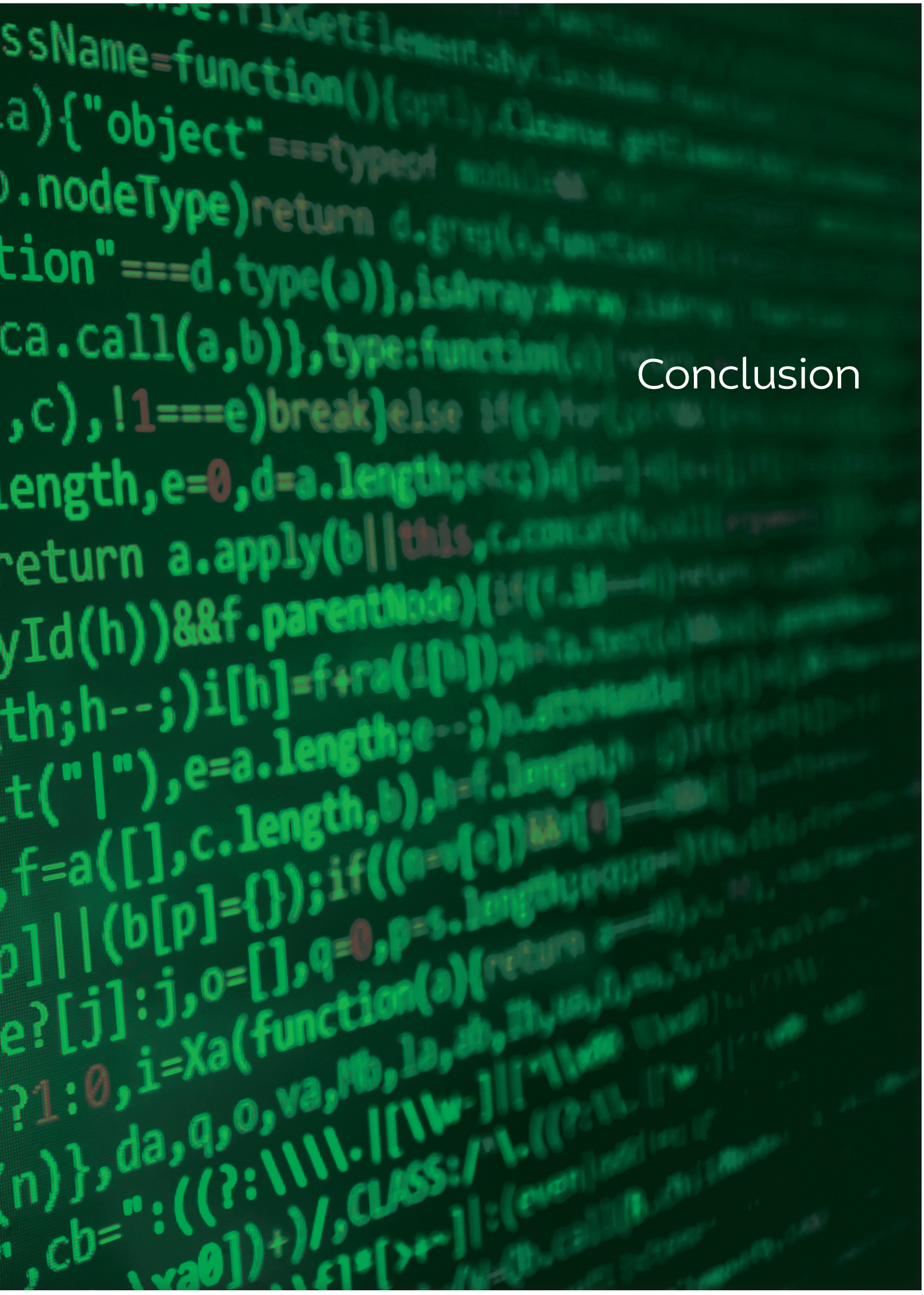
Efficacité énergétique du calcul quantique

On distingue deux types de coût énergétique liés au traitement de l'information classique : pratique et fondamental. Le coût pratique est essentiellement causé par la dissipation des circuits. À l'échelle du supercalculateur, il est typiquement de 1pJ/bit et comprend le traitement de l'information et son transfert. À l'échelle du processeur, ce coût se réduit à 1 fJ/bit. D'autre part, le coût énergétique fondamental d'un calcul est lié à la nature même du traitement de l'information, en particulier à son irréversibilité logique : la perte d'un bit d'information au cours de l'initialisation d'une mémoire ou d'une opération NAND contribue à la dissipation de l'énergie kTlog(2), qui est de l'ordre d'1 zJ/bit.

Les coûts pratiques peuvent être factorisés en travaillant sur le software et l'architecture des calculateurs et minimisés en améliorant les performances du hardware. Réduire les coûts fondamentaux revient à développer du calcul réversible. Toutes ces solutions pointent vers le développement des technologies quantiques de l'information.

Le coût énergétique d'un processeur quantique présente également des causes pratiques et des causes fondamentales. Les coûts pratiques impliquent essentiellement le refroidissement et des processeurs ainsi que leur adressage (travail en cryostat). Les coûts fondamentaux sont dus aux bruits quantiques, tels que la décohérence, qui sont sources d'irréversibilité thermodynamique. L'échelle d'énergie typique pour corriger les erreurs dues au bruit quantique est h€, où €est la fréquence de transition du qubit (de l'ordre de 10-24J pour des qubits Silicium). Ces coûts scalent comme le nombre de qubits physiques utilisés dans un processeur quantique, ce qui peut rapidement devenir non négligeable dans le cadre du Fault Tolerant Quantum Computing qui emploie des millions de qubits.





Conclusion

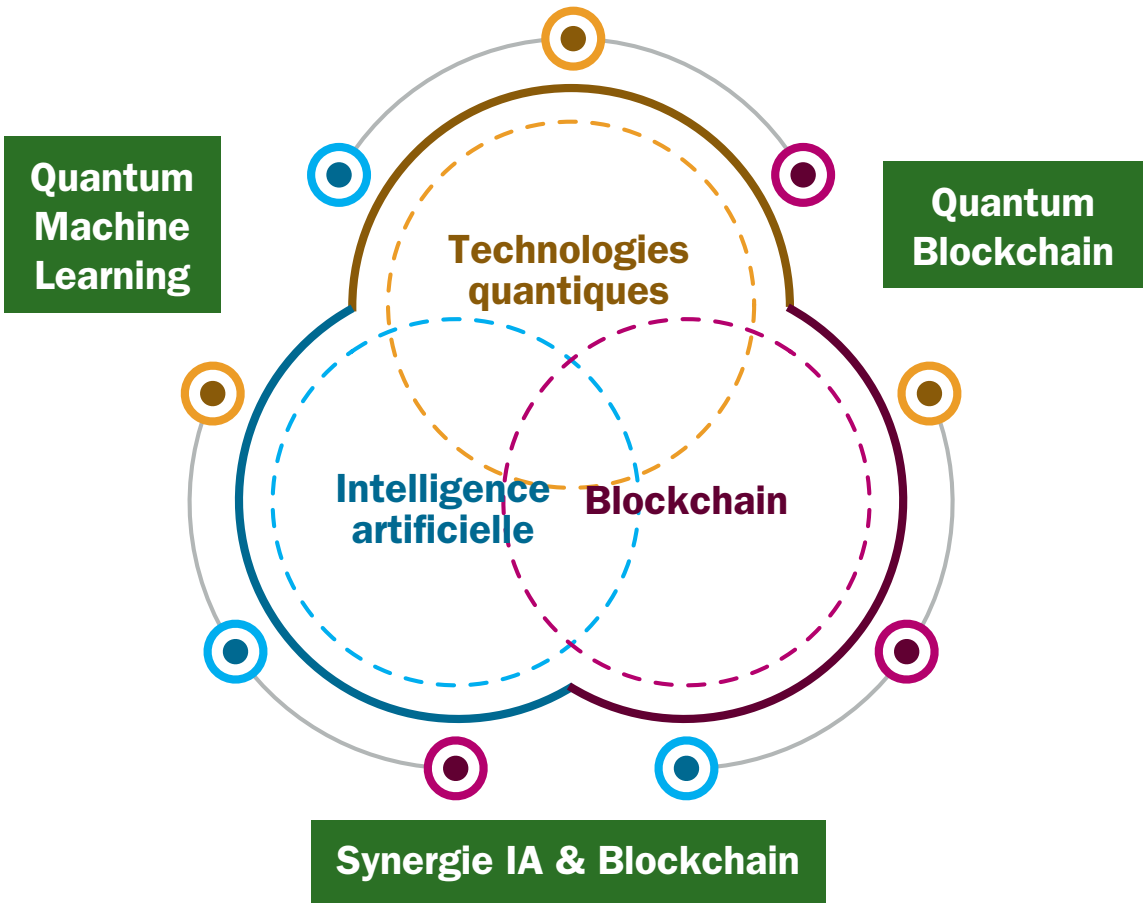
Synergies entre les trois technologies et perspectives

1. SYNERGIE INTELLIGENCE ARTIFICIELLE ET BLOCKCHAIN

Les algorithmes d'apprentissage tels que le *deep learning* ont besoin de se nourrir de gros volumes de données dont la collecte reste un vrai défi, car les entreprises et usagers n'ont pas nécessairement de raisons ni de désirs de les partager. Or, avec l'arrivée de *data marketplaces* basées sur la blockchain, cette technologie permettra d'accéder facilement à des masses de données et, *in fine*, de développer des services basés sur l'IA.

En effet, en tant que registre sécurisé, incorruptible, transparent et chronologique où seuls des ajouts sont possibles (« *append-only* »), la blockchain peut enregistrer les autorisations de partage de données requises, par exemple dans le cadre de « contrats intelligents » (*smart contracts*) et permettre des échanges de données à une échelle encore plus large (en utilisant par exemple des objets connectés).

Ainsi, l'usager comme l'entreprise pourront stocker leurs données de manière sécurisée pour mieux en gérer l'accès et la vente. Les données seront alors monétisées en toute sécurité et leurs propriétaires en garderont le contrôle.



2. SYNERGIE INTELLIGENCE ARTIFICIELLE ET TECHNOLOGIES QUANTIQUES

Ces dernières années, des circuits intégrés destinés à des applications spécifiques comme les puces neuromorphiques[132] et les unités de calcul ont offert de nouveaux composants physiques à l'IA. Les ordinateurs quantiques feront partie de cette évolution. En effet, le *quantum machine learning* et le recuit quantique seront ces prochaines années une des applications du calcul quantique.

« Unsupervised learning had a catalytic effect in reviving interest in deep learning but has since been overshadowed by the successes of purely supervised learning. [...] we expect unsupervised learning to become far more important in the longer term. Human and animal learning is largely unsupervised: we discover the structure of the world by observing it, not by being told the name of every object. »

Yann LeCun, Yoshua Bengio & Geoffrey Hinton, «Deep Learning», Nature, Vol. 521, 28th May, 2015

Ces approches utiliseront le phénomène de physique quantique pour, par exemple, remplacer les chaînes de Markov dans les méthodes de Monte-Carlo avec des applications dans l'évaluation des actifs financiers et l'évaluation du prix des options ou encore pour optimiser le rendement d'un portefeuille d'actifs financiers. L'ordinateur quantique pourrait aussi faire progresser l'apprentissage non supervisé[133]. Citons l'équipe de Rigetti Computing[134] qui a utilisé un algorithme hybride quantique/classique pour la classification non supervisée[135] (*clustering*). IBM, Google, Intel et Microsoft, ainsi que quelques startups, se sont lancées dans le développement de machines quantiques qui promettent une nouvelle ère dans le domaine de l'informatique.

3. SYNERGIE BLOCKCHAIN ET TECHNOLOGIES QUANTIQUES

L'arrivée de l'informatique quantique pose un réel défi en matière de cybersécurité. Certains pessimistes prévoient même « la mort de la blockchain et du bitcoin ». En effet, les mécanismes cryptographiques, et en particulier les protocoles de chiffrement asymétriques, permettent aujourd'hui de

132. Julie Grollier, Directrice de recherche à l'Unité mixte de physique CNRS-Thales de Palaiseau, a développé avec ses collaborateurs le premier nanoneurone artificiel capable de reconnaître 9 chiffres prononcés par différents locuteurs. Dans les prochaines années, ces nanoneurones magnétiques pourront être interconnectés grâce à des synapses artificielles, pour mettre au point des machines de calcul de type neuromorphique.
133. Contrairement à l'apprentissage automatique supervisé, où le résultat d'un algorithme est basé sur des données d'apprentissage « étiquetées », l'apprentissage automatique non supervisé offre la possibilité de résoudre des problèmes complexes en utilisant uniquement des données d'entrée sans le passage par un jeu de données d'apprentissage (commentaire : on pourrait plutôt dire que le jeu de données d'apprentissage est aussi le jeu de données de test).
134. Fondée en 2013 par Chad Rigetti (ex-employé d'IBM dans le domaine de l'informatique quantique), la startup a levé 70 millions de dollars avec en figure de proue Andreessen Horowitz comme investisseur.
135. Le clustering, aussi appelé classification non supervisée, est le processus qui permet d'identifier des groupes homogènes au sein d'un ensemble de données multidimensionnelles. Il est calculé de telle manière que les données appartenant au même groupe soient les plus similaires possibles les uns des autres, au sens d'un certain critère de similarité et que les données appartenant à des groupes différents soient les plus dissimilaires possible. Les algorithmes classiques de clustering sont connus pour leur convergence rapide vers des optimums locaux. Pour pallier ce problème, le clustering a été reformulé comme un problème d'optimisation et plusieurs métaheuristiques lui ont été appliquées, tels que les algorithmes génétiques (GA) [2], l'algorithme de colonies de Fourmis (ACO) [3,4] et l'algorithme d'optimisation par essaim de particules (PSO).

sécuriser les communications sécurisées, les systèmes de paiements, les transactions financières et les monnaies virtuelles telles que le bitcoin. Ces approches étant fortement combinatoires, il faut un temps certain pour casser un code par la «force brute». Pour un ordinateur quantique, ce décryptage devient réalisable en très peu de temps, ce qui compromettrait le e-commerce et les offres de service de banque en ligne. Les documents signés électroniquement pourront être falsifiés… De plus, certaines cyberattaques telles que les dénis de service pourraient devenir facilement exécutables avec les technologies quantiques et auraient un effet démultiplié. Cependant, avec la cryptographie quantique, il devient possible d'ajouter une couche quantique au protocole standard de la blockchain ou de concevoir une blockchain entièrement quantique (Quantum Blockchain).

Un groupe de chercheurs australiens dans les technologies quantiques et cryptographiques, en collaboration avec une équipe singapourienne, a expliqué[136] que l'algorithme «*Elliptic Curve Digital Signature Algorithm*» utilisé pour le bitcoin pourrait devenir vulnérable et les cryptages RSA pourraient être «crackés» via l'algorithme de Shor d'ici à dix ans.

« Les protocoles cryptographiques utilisés actuellement afin de sécuriser l'internet et les transactions financières sont susceptibles de faire l'objet d'une attaque, en cas de développement d'un ordinateur quantique suffisamment puissant ».

Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2017)

Les attaques par déni de service (DDoS ou *Brute force attack*) auraient un effet démultiplié par l'utilisation d'ordinateurs quantiques.

Le phénomène physique au cœur de cette dernière approche s'appelle un enchevêtrement. L'idée est de créer une blockchain utilisant des particules quantiques enchevêtrées dans le temps et donc partageant la même existence. Cela se produit lorsqu'elles interagissent au même moment dans l'espace et dans le temps : la mesure de l'une influence immédiatement l'autre, quelle que soit la distance qui les sépare.

L'enchevêtrement garantit la sécurité, car ce phénomène physique est extrêmement fragile : une mesure sur une paire de particules enchevêtrées détruit immédiatement le lien. Donc, si un utilisateur malveillant tente d'interférer avec l'une des paires, cela est immédiatement évident pour l'autre. Tout comme les particules peuvent s'enchevêtrer dans l'espace, elles peuvent aussi s'enchevêtrer dans le temps. Ainsi, une particule existant dans le présent peut être enchevêtrée avec une autre qui existait dans le passé. Et la mesure sur celle-ci influence immédiatement sa prédécesseure. La chaîne est alors sécurisée, car toute personne tentant de la manipuler l'invalide immédiatement : c'est l'avantage de l'intrication quantique.

Il est donc fondamental de rester dans le peloton de tête de la compétition internationale de cette technologie en développant et en renforçant la recherche et l'industrialisation ainsi que la formation des compétences spécifiques qui permettront demain de concevoir et développer de nouveaux algorithmes et imaginer de nouvelles applications.

136. Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2017). Quantum attacks on Bitcoin, and how to protect against them. arXiv preprint arXiv:1710.10377.

Conclusion

S'intéressant à l'ensemble des métiers de la finance, de l'assurance à la gestion d'actifs en passant par les banques de réseau et les fintechs, FINANCE INNOVATION est un Pôle de compétitivité d'envergure internationale dont la mission est de favoriser l'innovation, la recherche et les projets collaboratifs pour la compétitivité de l'industrie financière en France et la création d'emplois. Toujours en quête d'une forte valeur ajoutée dans son secteur de prédilection, le Pôle est lanceur de projets novateurs et structurants en France et à l'international. Pour atteindre ses objectifs, il publie de manière régulière des livres blancs identifiant des Domaines d'Innovation Prioritaires, qui font l'objet d'appels à projets partout sur le territoire, ainsi que les tendances porteuses du secteur financier pour encourager l'innovation.

Ce livre blanc a identifié 28 domaines prioritaires d'innovation qui sont, déjà aujourd'hui et encore plus demain, les leviers majeurs de la compétitivité de l'industrie financière. Les trois technologies de l'intelligence artificielle (IA), de la blockchain et de l'informatique quantique, à la fois complémentaires et synergiques, revêtent chacune un caractère prioritaire à des horizons temporels différents (aujourd'hui pour l'IA et la blockchain, plus tard pour le quantique) du fait de leur importance stratégique pour le développement de l'écosystème technologique de manière générale et celui de la finance en particulier.

Un changement global de paradigme avec une IA omniprésente

L'IA impacte déjà aujourd'hui tous les métiers de la finance de manière transversale. Un futur proche montrera l'IA comme une composante principale de la majorité des solutions fournies, passant d'un modèle où l'IA est une addition à la conception initiale à un modèle *IA by design*. Il est nécessaire de se préparer à cette transformation grâce à la recherche et la formation et en créant la confiance nécessaire à son utilisation à grande échelle.

La blockchain introduit de nouveaux modèles économiques

Les blockchains sont considérées comme des technologies facilitant la transformation des modèles de partage entre acteurs économiques indépendants et permettant l'apparition de nouveaux *business models*. La première utilisation de la blockchain est la simplification des process en réduisant le nombre d'intermédiaires et le temps de traitement des opérations/transactions. Il est donc primordial de poursuivre la stratégie d'investissement et de développement de cette technologie de manière à maintenir et accentuer le leadership dans les secteurs de la finance au sens large (banque – assurance – gestion d'actifs – immobilier – directions financières – économie sociale et solidaire) : la France dispose là d'une véritable opportunité avec les applications blockchain.

Les pouvoirs publics l'ont bien compris en lui donnant dans la loi PACTE le cadre législatif permettant son essor. Il facilitera l'émergence de plateformes intermédiaires en crypto-actifs et qui seront leaders mondiaux sur les applications métiers.

Pour cela, le pragmatisme guidera certainement les décisions en matière de fisca-

lité afin de ne pas freiner une innovation qui semble aussi disruptive qu'Internet il y a près de 30 ans.

Demain, les technologies quantiques...

Il est difficile de préciser aujourd'hui quand les applications se concrétiseront au niveau commercial. Les challenges scientifiques, technologiques et industriels sont nombreux et l'ordinateur quantique universel reste un objectif futuriste. Au vu du nombre et de la qualité des équipes qui travaillent sur le sujet dans le monde entier, on peut néanmoins penser que les progrès seront significatifs à court ou moyen terme et que des percées majeures sont vraisemblables à plus long terme. Par ailleurs, comme le montre l'expérience passée, il n'est pas nécessaire qu'une technologie soit complètement au point et satisfaisante à tous égards pour s'imposer si elle apporte déjà un avantage compétitif décisif.

Les systèmes informatiques et de communication occupent une telle place dans notre société que le développement et la sécurité de ces nouvelles technologies vont devenir un enjeu stratégique à l'échelle des États. Les risques de souveraineté associés seront comparables à ceux de la défense des Nations. En témoignent les investissements colossaux à travers le monde engagés par des pays comme les États-Unis ou la Chine, mais également par des sociétés comme IBM, Google, Microsoft, à l'instar de ceux réalisés pour développer les supercalculateurs. Ces technologies sont perçues comme fondamentales, car elles permettent, à défaut de fabriquer l'ordinateur quantique universel à l'échelle industrielle, de développer des technologies dérivées et complémentaires avec des applications industrielles immédiates et de se positionner comme leader potentiel des technologies informatiques, de sécurité et de communication qui ont le potentiel de devenir la norme dans les deux prochaines décennies.

L'IA, la blockchain et l'informatique quantique ne sont pas seulement individuellement des technologies majeures. Elles sont aussi complémentaires, le quantique permettant potentiellement de faire évoluer les modèles de calculs de haute performance, la blockchain de transformer les architectures métiers et l'IA de valoriser les modèles de données pour un grand nombre d'applications en Finance. Ce sont les synergies entre ces différentes technologies qui, mises en place sur différents horizons de temps, vont accentuer l'évolution des modèles de la finance, probablement progressive, mais possiblement très disruptive dans des cas spécifiques.

Les 28 DIP identifiés et analysés sont rédigés de façon à tracer une feuille de route relative à l'évolution des projets et des investissements pour le développement de ces technologies fondamentales à la compétitivité de la finance. L'opportunité pour la France de figurer parmi les leaders en matière d'innovation en finance est avérée et notre recommandation est de redoubler d'efforts dans ce sens. C'est le but principal défendu dans ce premier livre blanc dédié aux nouvelles technologies : il fera l'objet de travaux complémentaires en 2019-2020 avec des focus sur des métiers et secteurs spécifiques de la finance, un benchmark avec d'autres industries (smart city, santé/prévention, mobilité, aérospatiale) et des passerelles avec les autres centres stratégiques d'innovation dans le monde.





Répertoire des entreprises

570 Asset Management 248
Accrma 248
Addventa 249
Advestis 249
Aevatar 250
Agreement Avocat 250
Ailancy 251
Aston ITF 251
Bird & Bird 252
Blockchain Partner 252
Blue DME 253
Bolden 253
Cabinet Michelle Abraham 254
Cadre de Vie 254
CDLK Services 255
Chappuis Halder & Co. 255
Cowork.io 256
Devenez Proprio 256
Dreamquark 257
Drivequant 257
Elcimaï Financial Software 258
Estimeo 258
Expensya 259
Fanvoice 259
Fieldfisher France 260
Finances & Création 260
Formee 261
Fortia Financial Solutions 261
Garantme 262
Granada 262
Homelinks 263
Immo Factory 263
Icare technologies SAS 264
Incube 264
Institut de Recherche Biomédicale des Armées 265
Invivoo 265
Ixtel 266
Iznes 266
Kernix 267
Kriptown 267
Laboratoire Informatique Grenoble (CNRS-UGA-GINP-INRIA) 268
Le partenaire 268
Lexing Alain Bensoussan Avocats 269
Lingua Custodia 269
Margo 270
Mieuxplacer.com 270
Monemprunt.com 271
Monuma 271
Mydataball 272
Napoleon Index 272
Nephelai 273
Netheos 273
OneWealthPlace 274
Oze Energies 274
Paylead 275
+Simple.fr 275
Quard 276
Quantcube Technology 276
Quantic Technologies 277
Real Quality Rating 277
Secure-IC 278
Serendptech 278
Shift Technology 279
SIS 279
Stratumn 280
Tacotax 280
Testamento 281
The Independant Calculation Agent 281
Tiime 282
Treezor 282
Uniris 283
Unkle 283
Utocat 284
Variabl 284
Vialink 285
Wizi-Tyrell SAS 285
Xbrain 286
Yesaccount 286
Youse 287
Zelros 287

570 ASSET MANAGEMENT

Anass PATEL - Président
06 84 48 91 86 – anass.patel@groupe570.com

Spécialisée dans le développement et la distribution de produits financiers conformes à l'éthique musulmane et en lien avec les valeurs de la finance responsable.

44, rue Poliveau, 75005 Paris
www.570easi.com
www.linkedin.com/company/groupe-570

Chiffres-clés

Date de création : 2011
Effectif en 2018 : 14
CA en 2018 : > 1 M€
Statut juridique : SAS
Projet(s) labellisé(s) : Home Easi et Peace
Pays d'implantation : France, Luxembourg, Belgique

Mission et offres

Marchés cibles : épargne et crédit éthiques pour les personnes physiques et morales. Plateformes Fintech labellisées de structuration et d'origination de produits de financement et placement en faveur de l'accession à la propriété (570easi) et de l'épargne responsable (fair invest).

Expertise et savoir-faire

Structuration financière, gestion d'actifs, technologie de plateforme fintech.

Marchés visés

Accédants à la propriété, épargnants et toutes entités en recherche d'une alternative de produits financiers durables, adossés à des actifs réels, loin de toute spéculation. À la convergence de la finance participative et de l'investissement socialement responsable sur les marchés francophones.

Solutions/produits innovants

Crédit immobilier sous forme de crédit-vendeur, épargne sous forme de SCPI ISR, services financiers sous forme d'application mobile (coach digital) et de solutions d'enregistrement distribué (blockchain).

ACCRMA

Olivier BLANDIN – Président
+ 33 6 17 72 07 07 – o.blandin@accrma.fr

Assurance courtage conseil risk management – Assureur de niche en risques d'entreprises.

1, rue Ménard, 78000 Versailles
www.accrma.fr
www.linkedin.com/in/olivierblandin

Chiffres-clés

Date de création : mai 2013
Effectif en 2018 : 1
Statut juridique : SASU
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B
Description du produit/service : Accompagnement des TPE/Startup/PME sur les risques d'entreprise avec un zoom particulier sur les lignes financières de type responsabilité civile professionnelle, mais aussi l'assurance des cyber risques ou l'assurance homme clé.

Expertise et savoir-faire

Diagnostic et proposition de solutions (packages ou contrat stand alone), approche de groupes Affinitaires partageant même activités, appartenance ou centres d'intérêt : Alumni Grandes Écoles, Start-Up, Clients Entreprises de Portage salarial, Sociétés membres d'une Franchise, Espaces de coworking…
Objectifs : Créer des programmes d'assurance sur mesure d'accompagnement de la promesse client.

Marchés visés

Marché des TPE (2,7 M), Startup, PME.

Solutions/produits innovants

Offres packagées (sur mesure) bâties avec Assureurs de premier rang (Français et/ou Internationaux), en Dommages (exemple assurances Franchiseurs) ou en Assurances de personnes (Homme clé – Garanties croisées).

ADDVENTA

Serge BAUDIN – Président
+33 1 82 83 33 99 – serge.baudin@addventa.com

Solutions d'intelligence artificielle pour les métiers de la finance et les administrations.

74, rue de la Tour, 75116 Paris
www.addventa.com
www.linkedin.com/company/addventa

Chiffres-clés

Date de création : 2014
Effectif en 2018 : 28
CA en 2018 : 2,5 M€
Statut juridique : SAS
Projet(s) labellisé(s) : SCRIBE.AM
Pays d'implantation : France. Clients en France, Allemagne, Luxembourg, Suisse.

Mission et offres

Marchés cibles : Sociétés financières et administrations.
Description du produit/service : Addventa réalise pour de grands acteurs du secteur financier des solutions métier tirant profit des innovations en intelligence artificielle (traitement automatique du langage naturel, machine learning, agents cognitifs).

Expertise et savoir-faire

Expertise fonctionnelle et technique pour réaliser des solutions opérationnelles qui s'inscrivent dans des projets de transformation à fort enjeux économique ou réglementaire :

- augmentation des revenus ;
- amélioration de la productivité ;
- réduction des coûts ;
- conformité.

Marchés visés

La banque de détail, la banque privée, la gestion d'actifs, la banque d'investissement, le juridique, les risques et la conformité.

Solutions/produits innovants

- Scribe.am : rédacteur numérique des commentaires de la performance des fonds d'investissement ;
- Scribe.pm : reporting commercial de la performance des entités des réseaux d'agences bancaires ;
- Assistant juridique numérique : pour définir instantanément le contexte réglementaire des campagnes marketing ;
- Rédacteur numérique d'analyses des risques de contrepartie ;
- Rédacteur numérique de conventions bancaires de banque privée ;
- Rédacteur numérique de recommandation d'arbitrage pour les clients de la banque privée.

ADVESTIS

Christophe GEISSLER – Président
06 08 60 46 14 – cgeissler@advestis.com

Intelligence artificielle pour la gestion de portefeuille.

69, boulevard Haussmann, 75008 Paris
www.advestis.com

Chiffres-clés

Date de création : 20111
Effectif en 2018 : 6
CA en 2018 : 800 K€
Statut juridique : SAS
Projet(s) labellisé(s) : Machine learning appliqué aux métriques ESG des sociétés cotées.
Pays d'implantation : France.

Mission et offres

Marchés cibles : B2B.
Description du produit/service : Advestis décline son activité en deux modalités :

- Conseil aux investisseurs (institutionnels, sociétés de gestion), sur l'optimisation de l'usage de leurs données grâce à l'intelligence artificielle;
- Partenariats de gestion systématique sur mesure outillés par l'IA, appliqués à la sélection d'actions, à l'allocation d'actifs et à l'investissement global macro.

Expertise et savoir-faire

Advestis s'est spécialisé dès 2013 dans les applications de l'Intelligence artificielle interprétable. Loin de chercher à concurrencer les gérants, notre approche est au contraire d'installer en pleine coopération avec les utilisateurs des process de gestion automatisés, adaptés à leurs contraintes de portefeuille et aux sources de données dont ils/elles disposent. Les recommandations d'investissement sont restituées grâce à une interface graphique innovante. Advestis conseille depuis 2013 un fonds obligataire pour la gestion quotidienne de sa duration. La performance des recommandations a été positive pour les 6 années de 2013 à 2018 inclus.

Marchés visés

Advestis s'adresse exclusivement à des clients investisseurs professionnels, tels que des sociétés de gestion ou des investisseurs institutionnels.

Solutions/produits innovants

Création de surperformance nette pour des fonds d'investissement grâce à un traitement des innovant des données basé sur un large spectre de techniques d'IA.

ÆVATAR

Serge KRYWYK - Président
+33 6 47 82 02 34 - serge.krywyk@aevatar.com

La SCIC ÆVATAR® conçoit, produit et opère une plateforme coopérative de gestion d'identité numérique souveraine de niveau substantiel à élevé.

16, Place de la Bourse, Palais Brongniart, 75002 Paris
www.aevatar.com

Chiffres-clés

Date de création : 16 janvier 2017
Statut juridique : Société Coopérative d'Intérêt Collectif (SCIC)
Pays d'implantation : France

Mission et offres

Marchés cibles : B2C
Description du produit/service : accessible via une application dont l'accès est sécurisé par un agent conversationnel biométrique multifacteurs (selfie dynamique, vidéo, audio et comportemental), la plateforme Ævatar® de gestion d'identité numérique permet la création, par son utilisateur, d'un porte-identités (ID wallet) mobile. La plateforme est conçue pour faciliter la conformité des entreprises aux exigences des réglementations européennes sur l'identité numérique (eIDAS2+, Attribute-Based Credentials/Verifiable Claims), sur la protection des données personnelles (RGPD, GDPR, république numérique) et les services de paiements (DSP2, AML-D4/5).

Expertise et savoir-faire

Les dirigeants d'ÆVATAR® sont des experts de la gestion des identités et des données, tant en termes de conception, d'architecture et de plateformes, de sécurité et de conformité réglementaire, de développement commercial international, d'intelligence artificielle, que d'intégration dans la Blockchain.

Marchés visés

Gestion de l'identité numérique, protection des données personnelles, services de paiements.

Solutions/produits innovants

La solution Ævatar® inclut quatre produits :

- MyÆvatar®, une application de porte-identité qui génère des tokens biométriques multifacteurs valables qu'une seule fois (Biometric-One-Time-Token, BOTT), pour authentifier de façon forte et facile les citoyens dans leurs transactions de la vie quotidienne.
- Ævatar® Enterprise, une API ouverte, conforme aux environnements IAM du marché, qui gère les interactions entre l'application MyÆvatar® et les serveurs des entreprises.
- MyÆvatar® Room, le Personal Data Sore (PDS) qui se veut un coffre-fort de données personnelles qui reste sous le contrôle de l'utilisateur.
- My Ævatar® card, une carte, avec ou sans puce, sous le contrôle exclusif de l'utilisateur qui stocke les preuves biométriques de référence (le gabarit) et à partir desquelles l'authentification forte biométrique à deux facteurs est réalisée selon un mode «Match on Card» ou «Match On Code».

La plateforme Ævatar® (proposée en marque blanche) fédère les meilleures technologies de Cybersécurité et de CyberPrivacy du marché en termes de biométrie (Id3 technologies et Tiempo Secure), de gestion de la vie privée (CryptoExperts, leader des ABC4Trust. eu et de WhiteBox), de conteneurs optiques sécurisés de données (Advanced Track & Trace), de systèmes de Vision Biométrique (MODIvision), de validation de documents officiels (SURYS/KEESING) et de Signature électronique Distribuée (DPKI)… Pour la parfaite conformité aux bonnes pratiques et aux réglementations en matière de Cybersécurité et CyberPrivacy, Ævatar® fait appel respectivement à O'SERVICE2 et à la société d'avocats CAPRIOLI & Associés.

AGREEMENT AVOCAT

Jérôme DUPRÉ – Avocat, Docteur en droit
02 40 73 84 11 – contact@agreement-avocat.com

Cabinet d'avocat intervenant principalement en droit du numérique et des données personnelles.

10, rue Gaëtan Rondeau
www.agreement-avocat.com
Twitter : @AgreementAvocat

Chiffres-clés

Date de création : 2017
Statut juridique : SAS
Pays d'implantation : France

Mission et offres

Description du produit/service : Agreement Avocat vous accompagne dans les domaines suivants : Intelligence artificielle, robotique, données personnelles (RGPD), IoT, cybersécurité, réalité virtuelle, big data, cloud, licence et maintenance de logiciels, développements spécifiques, contrats informatiques.

Expertise et savoir-faire

Droit des contrats, droit du numérique, conseil juridique, contentieux civil et commercial, rédaction et négociation de contrats, élaboration d'une stratégie juridique, médiation.

Marchés visés

Entreprises.

Solutions/produits innovants

Utilisation de la solution Case Law Analytics.

AILANCY

Thibaut DE LAJUDIE – Associé
Business Team Investment Services et Asset Management
+33 6 60 59 21 31 - thibaut.delajudie@ailancy.com

Ailancy est un cabinet de conseil en organisation et management spécialisé dans l'industrie financière. Ailancy a développé une expertise spécifique sur la transformation digitale, les Fintech et les nouvelles technologies, notamment la Blockchain.

32, rue de Ponthieu, 75008 Paris
www.ailancy.com
www.linkedin.com/company/ailancy/
www.twitter.com/AilancyConseil

Chiffres-clés

Date de création : 2008
Effectif en 2018 : 100
CA en 2018 : 18 M€
Statut juridique : SAS
Pays d'implantation : France (Siège) et Maroc

Mission et offres

Marchés cibles : B2B.

Expertise et savoir-faire

Ailancy vous apporte une vision extérieure, indépendante et objective. Nous vous accompagnons en France et à l'international pour préparer l'avenir et piloter le changement. Un conseil personnalisé et une approche pragmatique nous permettent d'identifier les décisions stratégiques et d'orchestrer les opérations terrain, dans des environnements complexes.

ASTON ITF

Amaury DE LA LANCE – Président fondateur
03 83 46 46 03 – a.delalance@astonitf.com

Fintech BtoB, Plateforme SaaS de Credit Management et de Financement du poste clients

4, rue Piroux, 54000 Nancy
www.astonitf.com
www.linkedin.com/company/aston-itrade-finance

Chiffres-clés

Date de création : 2011
Effectif en 2018 : 25
Statut juridique : SAS
Projet(s) labellisé(s) : Aston iTF FINTECH de l'année 2015
Pays d'implantation : France + 40 % du chiffre à l'export

Mission et offres

Marchés cibles : B2B.
Description du produit/service : Agreement Avocat vous accompagne dans les domaines+ de CASH + VITE grâce au Cloud et à l'IA.
Pour les Entreprises : plateforme IT d'optimisation du poste clients :
- Analyse intelligente du poste clients ;
- Scoring du comportement de paiement des clients ;
- Automatisation intelligente du recouvrement ;
- Assistant digital pour l'Assurance-Crédit & Affacturage.

Pour les Banques : plateforme IT clés en main de financement à la facture :
- Portail client – Front office : Parcours 100 % digital KYC – Signature contrat - Financement…
- Back Office complet pour la Banque : scoring AI, financement, assurance credit, relance…

Expertise et savoir-faire

Aston iTF amène au marché 3 expertises clés :
- Métier : credit management, recouvrement, poste clients et son ecosystème (Assurance, Crédit, Affacturage, …) ;
- Technologique : full cloud, solutions SaaS, IA et Big Data;
- Clients : une très forte expérience de nos talents pour les grands comptes, les PMEs et les institutions bancaires.

Marchés visés

Entreprises B2B de toute taille de la TPE au Grand groupe souhaitant optimiser son BFR, sa Trésorerie et son poste clients. Banque et institutions Financières souhaitant accélérer leur Time To Market sur le marché du financement à la facture ou de l'e-dailly.

Solutions/produits innovants

Retrouvez toutes nos actualités et nos offres : www.astonitf.com.

BIRD & BIRD AARPI

Benjamine FIEDLER - Managing Partner
+33 1 42 68 60 00 - benjamine.fiedler@twobirds.com

Cabinet d'avocats – Conseil en matière de droit européen et droit de la concurrence, droit de la propriété intellectuelle et des nouvelles technologies, de contentieux, de droit social, de droit bancaire et financier et de droit immobilier.

3, Square Edouard VII, 75009 Paris
www.twobirds.com
fr.linkedin.com/company/bird-&-bird-llp
twitter.com/twobirds

Chiffres-clés

Date de création : 1er janvier 1999
Effectif en 2018 : 26 associés, 80 avocats, 72 salariés
CA en 2018 : 34 989 826 €
Statut juridique : AARPI
Pays d'implantation : France

Mission et offres

L'implication de longue date du cabinet dans le domaine des technologies nous a permis de développer une pratique centrée sur l'interaction complexe entre la réglementation bancaire et financière et la législation en matière de TIC et de cybersécurité. Depuis de nombreuses années, nous œuvrons pour le développement des services bancaires et financiers en ligne et mobiles, du paiement mobile, du financement participatif, de la monnaie virtuelle et autres solutions bancaires et systèmes de paiement innovants. En outre, nous fournissons l'assistance nécessaire à nos clients concernant les exigences et réglementations strictes qui s'appliquent dans de nombreux pays.

Marchés visés

Nous conseillons un grand nombre de clients renommés, qu'il s'agisse d'acteurs mondiaux, de startups ou d'investisseurs, sur les aspects réglementaires, juridiques du développement commercial de leurs activités liées aux FinTech.

Solutions/produits innovants

- Applications & internet des objets ;
- Plateformes de paiement numériques ;
- Nouveaux modèles de financement ;
- Investissement dans les fintech ;
- RegTech, LCB-FT et identités électroniques ;
- Réglementation conformité ;
- Gestion des risques ;
- Analyse des données, BigData, confidentialité et secret bancaire ;
- Cybersécurité ;
- Cloud computing ;
- Blockchain.

BLOCKCHAIN PARTNER

Alexandre Stachtchenko – Directeur Général
06 62 29 78 01 – claire@blokchainpartner.fr

Blockchain Partner est le leader français de l'accompagnement sur les technologies blockchain et crypto-actifs.

43, avenue de la république, 75011 Paris
www.blockchainpartner.fr
www.linkedin.com/company/blockchainpartner/

Chiffres-clés

Date de création : 2016
Effectif en 2018 : 10
CA en 2018 : 1,1 M€
Statut juridique : SAS
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B
Description du produit/service : La startup aide les entreprises (BNP Paribas, Aéroports de Paris…) et les institutions publiques (Banque de France, État de Genève…) à explorer et déployer les technologies et crypto-actifs, en s'appuyant sur un tripôle d'expertises - stratégie, technique, légal - unique en France. Blockchain Partner accompagne également des projets d'ICO dans l'ensemble des dimensions de ces opérations, et a développé une expertise en token-design.

Expertise et savoir-faire

Blockchain Partner a accompagné près d'1/3 des entreprises du CAC40 dans leur découverte, exploration et application des technologies blockchain. Notre équipe a accompagné les premières entreprises en France qui ont commencé à travailler sur la blockchain (BNP Paribas) ainsi que les premières institutions publiques (Banque de France à partir de 2016). Nous avons mis en production l'un des premiers projets blockchain en France (Banque de France). Blockchain Partner accompagne par ailleurs des porteurs de projets d'ICO (Initial Coin Offering) dans leur opération de levée, sur leurs besoins stratégiques, techniques, juridiques et marketing.

Marchés visés

Description (300 caractères max, espaces compris) : Nous souhaitons continuer à accompagner les entreprises, les institutions publiques et les porteurs de projet ICO en renforçant notre tripôle d'expertises (architecture, sécurité, mise en conformité…) et en proposant des services clefs en main (assurance retard, certification de documents…). Nous prévoyons également une expansion à l'international, d'abord dans des marchés cibles européens (Londres, Berlin…) et éventuellement des hubs asiatiques des blockchains (Hong Kong, Singapour…).

Solutions/produits innovants

Notre produit Datatrust (datatrust.fr) permet de certifier l'intégrité d'un document et de l'horodater sur la Blockchain.
Les avantages :

- Sécurisé : Les données ne sont pas directement stockées sur la blockchain, seule son empreinte numérique l'est. Une fois inscrite, cette dernière ne peut être ni modifiée ni supprimée ;
- Rapide : En moins de 24 heures, votre fichier est certifié et en quelques clics, son certificat peut être téléchargé au format PDF ;
- Simple : La certification de vos fichiers numériques et leur vérification par vos interlocuteurs se font en quelques clics.

BLUE DME

Cédric MORA – Directeur Marketing et Produit
06 10 99 02 92 – cmora@bluedme.com

Blue DME créé l'assistant virtuel du «commercial augmenté» : des actions personnalisées lui sont proposées pour conclure des ventes, changer un prix produit ou envoyer un message promotionnel.

31, rue du Pont, 92200, Neuilly-sur-Seine
www.bluedme.com
fr.linkedin.com/company/blue-dme

Chiffres-clés

Date de création : Avril 2015
Effectif en 2018 : 13
CA en 2018 : 925000
Statut juridique : SAS
Projet(s) labellisé(s) : Data Exchange
Pays d'implantation : France

Mission et offres

Marchés cibles : Entreprises B2C avec un cycle de vente long/complexe avec un focus sur les secteurs Assurance, Automobile, Immobilier et Voyage. Nous visons les PME avec une offre starter (sources de données standards) et les ETI/Grands groupes (sources de données et algorithmes prédictifs pouvant être spécifiques).
Description du produit/service : Blue DME permet d'aider les commerciaux à mieux vendre en leur donnant accès à des informations prédictives sur les meilleurs clients à contacter, à quel moment et leur proposer les meilleurs produits au bon prix. Le commercial devient un «commercial augmenté» qui est donc aidé au quotidien par un assistant virtuel qui lui apporte cette aide à la décision et s'adapte à sa façon de travailler.

Expertise et savoir-faire

Blue DME a développé des compétences sur les sujets suivants :
- Business : assistants virtuels/co-bots, vente intelligente, efficacité opérationnelle, commercial augmenté, conseiller augmenté ;
- Technologies : machine learning, technologies hadoop/Spark/Spark streaming, analyse de données temps reel, matching multi-sources, big data, intelligence artificielle.

Marchés visés

Description (300 caractères max, espaces compris) : Entreprises B2C avec un cycle de vente long/complexe avec un focus sur les secteurs Assurance, Automobile, Immobilier et Voyage. Nous visons les PME avec une offre starter (sources de données standards) et les ETI/Grands groupes (sources de données et algorithmes prédictifs pouvant être spécifiques).

Solutions/produits innovants

Blue DME propose une solution Smart Selling en mode SaaS permettant d'enrichir les applications existantes des commerciaux à partir de l'ensemble de données clients, données internes et données du marché pour proposer des «insights» : informations prédictives sur les meilleurs clients à contacter, à quel moment et leur proposer les meilleurs produits au bon prix. Ces «insights» sont ensuite disponibles dans les interfaces existantes des équipes commerciales (intégration avec notre API) : CRM, applications smartphone, Gestion de leads, etc. Nous innovons aussi sur la création de nouvelles interfaces vendeurs pour leur donner en temps réel leurs «Next Best Actions» (meilleures prochaines actions) : application smartphone, extension navigateur pour Salesforce, etc. ou simplement pousser des notifications.

BOLDEN

Tristan GRUÉ – Founder & CEO
01 80 04 10 39 – contact@bolden.fr

Bolden est une plateforme de référence du financement alternatif des PME. Notre mission : accélérer la croissance des entreprises avec des prêts rapides et flexibles.

9, rue Christophe Colomb
www.bolden.fr
www.linkedin.com/company/bolden-fr

Chiffres-clés

Date de création : 2015
Statut juridique : SAS
Projet(s) labellisé(s) : Scoring crédit semi-automatisé
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B
Description du produit/service : Bolden propose aux entreprises, artisans, professions libérales et franchisés d'accéder à des solutions de financement spécialisé pour **accélérer leur développement de façon simple, rapide et flexible**.

Expertise et savoir-faire

Un scoring credit robuste et évolutif : notre arbre de décision propriétaire analyse automatiquement plus de 400 variables. Nous combinons de façon unique des données d'Altares, de la Banque de France et de dizaines d'autres sources de données supplémentaires.

Marchés visés

Il est parfois compliqué pour les TPE/PME d'obtenir des financements pour leurs besoins de fonds de roulement et leurs projets de développement, les acteurs classiques du financement étant de plus en plus frileux et déshumanisés. Bolden est la plateforme de financement de ces professionnels.

Solutions/produits innovants

Bolden Advance est un crédit court terme, amortissable et à taux fixe, qui répond à tous les besoins de trésorerie des entreprises avec plus de flexibilité qu'un découvert bancaire classique. Les analyses financières Bolden sont plus rapides et plus souples que les analyses traditionnelles grâce à notre scoring credit évolutif et notre arbre de décision propriétaire. Elles nous permettent de répondre aux besoins des emprunteurs avec la plus grande réactivité.

CABINET MICHELLE ABRAHAM

Michelle ABRAHAM - Président, Avocat
01 85 08 80 40 – contact@cabinetmichelleabraham.fr

Cabinet d'affaires intervenant dans le domaine des blockchains et crypto-actifs.

2, rue Villaret de Joyeuse, 75017 Paris
www.cabinetmichelleabraham.fr
www.linkedin.com/in/michelle-abraham-7b45521

Chiffres-clés

Date de création : février 2016
Effectif en 2018 : 1
Statut juridique : SELAS
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B, B2C en France et à l'étranger.
Description du produit/service : Prestations juridiques en droit des affaires, droit des sociétés et dans le secteur des blockchains et crypto-actifs.

Expertise et savoir-faire

Droit des affaires, droit des sociétés et dans le secteur des blockchains et crypto-actifs. Rédactions d'articles en français et en anglais sur le domaine des blockchains et crypto-actifs. Michelle Abraham est membre de plusieurs associations spécialisées dans la blockchain et les crypto-actifs (Chaintech, le Cercle du Coin, le comité blockchain de l'AFNOR). Elle donne des cours dans différentes universités et écoles de commerce sur les blockchains et en droit des sociétés.

Marchés visés

Sociétés françaises et étrangères souhaitant s'implanter en France.

CADRE DE VIE

Stéphane VIE – CEO
06 14 64 85 97 - svie@cadredevie.fr

Cadre de Vie aide les marques du changement de logement à détecter qui parmi leurs internautes est sur le point de changer de domicile.

6, rue du lavoir, 69 650 Saint-Germain au Mont d'Or
www.cadredevie.fr
www.linkedin.com/company/cadredevie

Chiffres-clés

Date de création : 2016
Effectif en 2018 : 5
CA en 2018 : 350 K€
Statut juridique : SAS
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B.
Description du produit/service : Notre mission : l'engagement client pour les grandes marques lors des moments de vie. Nous aidons les grandes marques (banque, assurance, énergie, télécoms, commerce, travaux …) à fidéliser leurs clients lorsqu'ils changent de domicile, grâce à une plateforme API innovante qui détecte et qualifie les foyers susceptibles de déménager. Pour cela, nous proposons aux 3 millions de foyers qui changent de domicile tous les ans et qui visitent les sites de ces marques plusieurs services pertinents et des contenus qui les intéressent vraiment, en lien avec leur projet et leur futur logement. Nous leur donnons accès à des annonces immobilières de qualité, et plus précisément à la majorité des mandats exclusifs signés par les professionnels de l'immobilier en France. Un mandat exclusif permet au propriétaire qui vend son logement d'avoir une vraie relation de confiance avec son agence immobilière. Pour l'acheteur, l'expérience utilisateur sera meilleure puisque le logement en question sera géolocalisé précisément sur une carte. Ces services prennent la forme d'un portail immobilier, derrière lequel nous avons construit une plateforme d'intégration complète de datas et services pour une diffusion via des API sur les sites des grandes marques du changement de domicile. Visitez : – notre plateforme d'engagement clients avec diffusion multisites : www.cadredevie.fr – le site des propriétaires mandants : www.mandatsexclusifs.fr – l'espace immobilier de BNP Paribas, intégrant la plateforme Cadre de Vie : https://mabanque.bnpparibas/fr/notre-offre/credits/credits-immobiliers.

Expertise et savoir-faire

IA/API/cartographie/RGPD.

Marchés visés

Nos marchés sont les marques du changement de logement qui peuvent perdre jusqu'à 50 % durant ce moment de vie :
- Banques ;
- Assurances ;
- Énergie ;
- FAI.

Solutions/produits innovants

Nos API sont réparties selon 4 familles :
- Recherche immobilière (géolocalisation, recherche par temps de trajet, éligibilité des logements au haut débit…) ;
- Accompagnement (inspiration…) ;
- Financement ;
- Bons plans.

CDLK SERVICES

Benoît GRUET – CEO & Co-Fondateur
+33 (0)6 03 42 69 61 – benoit.gruet@cdlkservices.com

Spécialiste de la transformation de données transactionnelles en cas d'usages pour la banque.

28, rue du Panorama, 78100 Saint-Germain-en-Laye
www.cdlkservices.com
LinkedIn ou autre :
www.linkedin.com/company/cardlink%27in
www.twitter.com/cdlkservices?lang=fr

Chiffres-clés

Date de création : 2013
Effectif en 2018 : 10
CA en 2018 : 570 K€
Statut juridique : SAS
Projet(s) labellisé(s) : PDMP
Pays d'implantation : France

Mission et offres

Marchés cibles : Notre marché B2B cible l'innovation des services digitaux dans le domaine des banques de détail, avec des solutions destinées, in fine, aux différents segments de clientèle de la banque : particuliers, professionnels, entreprises.
Description du produit/service : CDLK propose aux banques d'accélérer leur transition digitale grâce à une solution technologique de type Big Data combinant algorithmes & machine learning (AI). Le principe vise à transformer la donnée brute de paiement en nouveaux services à valeur ajoutée.

Expertise et savoir-faire

CDLK a développé une solution technologique unique sur le marché, la PDMP (Payment Data Management Platform), capable de de traiter des millions de transactions chaque jour pour identifier, géolocaliser et catégoriser précisément les dépenses carte bancaire. Plus précisément, il s'agit d'une technologie de retraitement des données monétiques de type machine-learning. Cette solution adresse la problématique, pour une banque, de l'exploitabilité de la data transactionnelle dans le cadre de l'innovation de type PIVAS (Payment Information Value Added Services © Gartner). La solution CDLK vient ainsi identifier précisément la signature monétique des commerces en croisant différentes sources monétiques avec des données externes, permettant de faire progresser notamment le taux de complétude de la catégorisation des dépenses d'environ 65% à plus de 99 %. Pour le marché français, à partir d'une base de plus 3 millions de signatures monétiques, la PDMP crée un référentiel marchand d'environ 1,2 millions de points de vente. Ce référentiel marchand est rafraichi quotidiennement grâce aux traitements des flux monétiques bruts par la plateforme CDLK. Grâce à ce travail de raffinage et d'enrichissement des données monétiques brutes, la PDMP permet aux banques de proposer de nouveaux services utiles à leurs clients particuliers et commerçants.

Marchés visés

Notre cœur de cible sont les banques de détail émettant un volume significatif de porteurs de cartes, prioritairement sur le marché français (+ de 70 Millions essentiellement détenus par 7 Enseignes) dans un premier temps. En cible secondaire viennent les néo-banques et tous autres émetteurs de titres de paiement.

CHAPPUIS HALDER & CO.

Stéphane EYRAUD – CEO
+33 1 75 77 27 80 – seyraud@chappuishalder.com

Augmented consulting for financial services.

20, rue de la Michodière, 75002 Paris
www.chappuishalder.com

Chiffres-clés

Date de création : 2009
Effectif en 2018 : 250
Pays d'implantation : Genève, Paris, Londres, Singapour, Hong-Kong, Montreal, New-York, Budapest, Francfort

Mission et offres

Marchés cibles : Institutions financières. Nous comptons parmi nos clients les plus grands groupes bancaires européens (retail, CIB, gestion de fortune), de l'assurance, des security services (pré et post trade), de l'asset management et des fonds d'investissement alternatifs (real estate et private equity).
Description du produit/service : Nous proposons à nos clients le meilleur du conseil en management, de l'innovation et de l'expertise des services financiers avec 3 practices (Biz Dev & Transformation, Finance Risk & Compliance, et Data, Tech & Cyber Security), 2 Centres d'Expertise et notre solution Augmented Consulting.

Expertise et savoir-faire

Nous avons construit deux pôles d'expertise internes en matière de modélisation des risques (Global Research & Analytics) et dans le domaine de la réglementation et de la compliance (Regulatory Watchtower).

Marchés visés

Notre ambition est de devenir le conseil préféré des organisations financières qui, en mobilisant des capacités nouvelles, sera en capacité de créer à leurs côtés les services financiers utiles de demain.

Solutions/produits innovants

Nous proposons aujourd'hui l'offre Augmented Consulting pour apporter des solutions d'innovation sur-mesure, clef en main et dans un délai court à nos clients. Nos équipes intègrent des experts du conseil en management et de la technologie (développeurs au sein de notre propre Lab, fintech, partenaires) ainsi que des méthodologies dédiées pour accompagner les clients à chaque étape de leur transformation. Couvrant le cycle de l'idéation au marché, notre écosystème s'appuie sur un accélérateur, Alpha, notre Lab à Budapest dédié au prototypage de solutions technologiques et la CH Alliance, notre réseau composé de 300 experts dans le monde. Quelques produits innovants issus de notre Lab et de l'accélérateur Alpha : Coqonut, le service de gestion de portefeuille en cryptomonnaies (disponible sur Android et Appstore), ou encore le service d'analyse des communications HighwaytoMail.

COWORK.IO

Pierre-André SVETCHINE - CEO et fondateur
06 63 43 66 70 - pasvetchine@cowork.io

CoWork.io est une solution de gestion d'espaces de travail flexible qui est centrée sur l'Humain. Notre offre (une solution SaaS en marque blanche, des objets connectés et des services) permet de créer du bien être et de l'engagement dans tous les espaces de travail : coworking, bureaux partagés, open-space, flex-office, immeubles multi-locataires...

9, rue du Faubourg Poissonnière, 75 008 Paris
www.cowork.io/
www.linkedin.com/company/cowork.io
www.twitter.com/Cowork_io
www.facebook.com/coworkio
www.instagram.com/cowork.io

Chiffres-clés

Date de création : 2014
Effectif en 2018 : 15
Statut juridique : SAS
Pays d'implantation : Siège en France. Clients en France, Belgique, Suisse et Canada

Mission et offres

Marchés cibles : B2B (espaces de coworking, entreprises, immeuble de bureaux).
Description du produit/service : Depuis sa création en 2014, CoWork.io s'est donné pour mission d'apporter du bien-être et de l'engagement dans les espaces de travail en créant une expérience digitale unique pour les employés. Composée d'un logiciel desktop, d'une application mobile, d'objets connectés et de services ; la solution CoWork.io offre la possibilité de gérer tous les usages au sein des espaces de travail flexibles. Son offre complète, innovante et robuste, s'adresse à tous types d'espaces tels que le flex office / smart office, le coworking, les bureaux partagés ou les immeubles multi-locataires. La solution CoWork.io permet de simplifier la vie au bureau : réservation de salle de réunion et de ressources, accès à une offre de services sur une marketplace, cartographie indoor... et inclut des outils d'analyse de la performance et de la consommation de l'espace de travail à destination des gestionnaires. Basée à Paris, CoWork.io est une startup française qui a déjà séduit de nombreux clients (Le Village by CA, The Bureau, Deskopolitan, Nexity, BNP Paribas Real Estate...) et souhaite accélérer son internationalisation fin 2018.

Expertise et savoir-faire

Notre solution est en marque blanche, nos clients ont ainsi une application intégrant totalement leur univers. Ce qui est parfait pour valoriser leur image de marque employeur. D'un point de vue technologique, notre solution est bâtie sur un écosystème ouvert (Full API), nous nous appuyons aussi sur un large réseau de services partenaires. Ainsi, CoWork.io s'adapte facilement aux contraintes techniques de ses clients et surtout à leurs besoins. En quelques mots : CoWork.io se distingue par le fait de créer une expérience digitale unique, personnalisée et évolutive.

DEVENEZ PROPRIO

Ludovic LABORDE – Directeur Général
06 42 17 58 33 – l.laborde@devenez-proprio.fr

Devenez Proprio est l'unique plateforme de dons qui favorise l'accession à la propriété via la love money.

8, quai de la Madeleine, 45000 Orléans
www.devenez-proprio.fr

Chiffres-clés

Date de création : 2015
Effectif en 2018 : 5
CA en 2018 : + 140 k€
Statut juridique : SAS
Pays d'implantation : France

Mission et offres

Marchés cibles : B2C
Description du produit/service : Devenez Proprio est une plateforme de financement participatif à destination des particuliers qui leur permet de réduire leur endettement et/ou d'augmenter leur capacité d'emprunt.

Expertise et savoir-faire

Devenez Proprio propose aux particuliers d'ouvrir une cagnotte immobilière afin d'obtenir son prêt immobilier avec de meilleures conditions. Acheter son bien immobilier est un réel évènement de vie que l'on partage avec son entourage. Il est donc tout naturel que ceux qui vous sont chers puissent y participer en contribuant à votre cagnotte ! Comme une liste de mariage ou une crémaillère, votre famille, vos amis, vos collègues... deviennent de véritables alliés dans la réalisation de votre projet immobilier. Ce nouvel accompagnement solidaire répond à un double objectif :

- Réduire son endettement ;
- Augmenter sa capacité d'emprunt.

Nous misons sur les valeurs humaines et collaboratives pour réussir votre projet immobilier. Devenez Proprio en quelques chiffres : 1126 projets immobiliers – 8417 participants - 2 213 880 € d'apport.

Marchés visés

B2C : 1 million de transactions immobilières chaque année en France.

Solutions/produits innovants

Création d'une communauté via la love money.

DREAMQUARK

Nicolas MERIC - CEO
06 98 24 78 15 - nicolas.meric@dreamquark.com

Sharpen decisions in Financial Services with explainable Deep Learning.

29, rue de Courcelles, 75008 Paris
www.dreamquark.com
fr.linkedin.com/company/nicolas-meric-dreamquark
twitter.com/DreamQuark

Chiffres-clés

Date de création : 2014
Effectif en 2018 : 25
CA en 2018 : 375 000 €
Statut juridique : SAS
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B, Services Financiers (Banques, Assurances, Asset Managers).
Description du produit/service : DreamQuark édite une plateforme qui automatise et optimise les tâches de Data Science inhérentes à la création d'une application d'IA pour la fraude, le risque, le marketing ou la conformité. Les Services Financiers peuvent entrainer et déployer des modèles prédictifs basés sur le Deep Learning en quelques clics et générer des scores lisibles via l'explicabilité individuelle fournie.

Expertise et savoir-faire

DreamQuark se compose de 30 employés dont la majorité possède une double expertise, à la fois technique (Data Science) et métier (Services Financiers). 30 % des effectifs possèdent un PhD en mathématique, physique ou informatique, dont le fondateur lui-même. Le département R&D de DreamQuark possède une expertise et une avance technologique reconnues dans de nombreux domaines liés à l'intelligence artificielle incluant l'explicabilité des modèles de Deep Learning ou encore la reconnaissance d'émotions dans la voix en temps réel. DreamQuark compte une dizaine de clients majeurs de la banque et l'assurance dont BNP Paribas, AG2R La Mondiale, GAN Prevoyance et Groupement Cartes Bancaires et est régulièrement primé pour son innovation (récemment élu Meilleure Solution Cognitive par Banque & Innovation 2017, Fintech de l'Année par Finance Innovation, Startup IA de l'année par La Tribune). Nicolas Meric a été entre autres reconnu en 2017 comme l'un des « 10 cerveaux français qui fascinent » (source Alliancy) dans le domaine de l'Intelligence Artificielle.

Marchés visés

DreamQuark adresse les besoins des Services Financiers sur les problématiques de fraude, risque, marketing et conformité. Acteur majeur en France, DreamQuark s'étend actuellement à travers l'Europe et prévoit de pénétrer le marché américain avant 2020.

DRIVEQUANT

Augustin LEMAN - Commercial & marketing
06 36 93 92 77 - hello@drivequant.com

Solution télématique smartphone et services de conduite connectée (sécurité, consommation carburant, éco-conduite, maintenance prédictive, engagement client…).

46, rue René Clair, 75018 Paris
www.drivequant.com

Chiffres-clés

Date de création : 6 février 2017
Effectif en 2018 : 8
CA en 2018 : 160k€
Statut juridique : SAS
Projet(s) labellisé(s) : Solution télématique basée sur le smartphone
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B2C.

Expertise et savoir-faire

DriveQuant est une société issue du monde automobile et de la recherche qui développe des services de mobilité connectée basés sur des modèles mathématiques et physiques tels que l'optimisation de la consommation de carburant, la mesure et l'amélioration de l'impact environnemental de la conduite, la sécurité au volant ou encore de la maintenance prédictive. Ainsi, DriveQuant accompagne ses partenaires dans la collecte de la donnée connectée de conduite, dans sa compréhension et sa valorisation en services pour le conducteur.

Marchés visés

DriveQuant accompagne tous les acteurs de la mobilité au sens large : assureurs, constructeurs et équipementiers automobile, leasers, acteurs de l'auto-partage et du co-voiturage, gestionnaires de flottes, formateurs… en France et à l'international à partir de 2018.

Solutions/produits innovants

Sur la base d'une expertise dans le traitement et la valorisation des données de conduite ainsi que le développement d'une solution télématique sur smartphone, DriveQuant offre aux assureurs :

- Une meilleure appréciation du risque routier au travers de notre indicateur de perte d'adhérence plus fin que la simple observation d'événements de conduite ;
- Une opportunité d'engager les assurés en leur proposant des services de conduite connectée afin de réduire leur consommation de carburant, de comprendre et améliorer l'impact environnemental de leur mobilité, de mieux maitriser leur budget auto… et de se comparer entre eux dans le cadre de challenges de conduite ;
- Une solution de collecte de données sur smartphone en intégrant nos services à une application existante ou en déclinant notre app marque blanche afin de déployer simplement, instantanément et à moindre risque une offre connectée d'assurance ou de prévention.

ELCIMAÏ FINANCIAL SOFTWARE

Pascal DENIER - PDG
01 64 10 47 20 – pdenier@elcimai.com

3, Rue de la brasserie Gruber, 77000 Melun
www.software.elcimai.com/efs/accueil-efs.jsp
www.linkedin.com/company/5260890/admin

Chiffres-clés

Effectif en 2018 : 5
CA en 2018 : 2 982 000 €
Statut juridique : SASU
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B
Description du produit/service : Elcimaï Financial Software, filiale du Groupe Elcimaï, est un éditeur de logiciels spécialisé dans la dématérialisation et la gouvernance des flux. Son offre logicielle riche, modulaire et évolutive permet à ses clients, banques ou entreprises, de répondre efficacement et rapidement à leurs enjeux stratégiques d'optimisation des coûts, de digitalisation des usages et de conformité règlementaire.
WeBank Core : Application EDI (eBics, SWIFT, PeSIT, FTPS, SFTP, S/MIME, SEPAmail, eBAM...)
WeBank Online : Site eBanking (DSP2, Agrégation, Tableau de bord personnalisable, Saisie d'ordre, Signature électronique, Délégation, GéoSécurisation, Coffre-fort, Souscription en ligne...)
WeBank Mobile : Application mobile (Agrégation, Saisie d'ordre, Signature électronique via QR-Code ou OTP, Saisie d'ordre).

Expertise et savoir-faire

Édition de logiciels, expertise MOA, expertise MOE.

Marchés visés

Banques, assurance, mutuelles.

Solutions/produits innovants

Elcimaï Financial Software édite des produits innovants :
WeBank Core : Application EDI (eBics, SWIFT, PeSIT, FTPS, SFTP, S/MIME, SEPAmail, eBAM...) ;
WeBank Online : Site eBanking (DSP2, Agrégation, Tableau de bord personnalisable, Saisie d'ordre, Signature électronique, Délégation, GéoSécurisation, Coffre-fort, Souscription en ligne...) ;
WeBank Mobile : Application mobile (Agrégation, Saisie d'ordre, Signature électronique via QR-Code ou OTP, Saisie d'ordre) ;
Station client : eBics, Saisie SEPA, Convertisseur, eBAM, SEPAmail.

ESTIMEO

Florian BERCAULT – Président
06 95 35 47 30 – florian.bercault@estimeo.com

Estimeo est une plateforme d'information, de notation automatique et de valorisation des startups et de l'innovation.

28, rue du Chemin Vert, 75011 Paris
www.estimeo.com/
www.linkedin.com/company/estimeo
www.twitter.com/estimeo

Chiffres-clés

Date de création : 1er janvier 2017
Effectif en 2018 : 5
Statut juridique : SAS
Projet(s) labellisé(s) : Oui
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B.
Description du produit/service : notre proposition de valeur est de collecter de l'information sur les startups, l'enrichir, la fiabiliser et la structurer pour la redistribuer aux investisseurs, aux structures d'accompagnement et à tous les acteurs qui veulent collaborer avec les startups. Grâce à la notation algorithmique de startups, nous offrons une solution de compréhension, identification, évaluation, sélection, suivi.

Expertise et savoir-faire

- Collecte, extraction, nettoyage, enrichissement et traitement de données startups;
- Connaissance des startups et de l'écosystème du capital-innovation.

Marchés visés

Estimeo s'adresse à l'écosystème de l'innovation dans sa globalité : startups, incubateurs, investisseurs, banques, grands-groupes. Aujourd'hui majoritairement français, notre marché s'étend hors des frontières de l'hexagone, en Europe.

Solutions/produits innovants

- La notation algorithmique de startups et son débriefing;
- Startup Pool : base de données qualifiée et dynamique de startups;
- Accès à la plateforme de notation automatique de startups ou en marque blanche;
- Formation à l'écosystème startup;
- Réalisation d'études économiques et d'événements.

EXPENSYA

Karim JOUINI – CEO – Co-fondateur
33 6 23 31 08 44 – karim.jouini@expensya.com

Expensya, startup fondée en 2014 par Karim JOUINI et Jihed OTHMANI, offre une solution intelligente qui automatise la gestion des notes de frais pour les entreprises de toutes tailles.

25, Rue de la Reynie, 75001 Paris
www.expensya.com/fr
www.linkedin.com/company/expensya
www. twitter.com/expensya
www.facebook.com/expensya

Chiffres-clés

Date de création : 2014
Effectif en 2018 : 40
CA en 2018 : 1 million d'euros
Statut juridique : SAS
Projet(s) labellisé(s) : Expensya
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B.
Description du produit/service : Expensya est une solution web et mobile de gestion des notes de frais. La solution automatise ce processus du reçu jusqu'à l'intégration comptable grâce à des technologies comme l'Intelligence Artificielle, le Machine Learning, le mobile et le stockage dans le Cloud. Expensya libère les professionnels et les experts-comptables de ce processus fastidieux et chronophage.

Expertise et savoir-faire

- Automatisation de la gestion des notes de frais : saisie automatique, automatisation des flux d'approbation, automatisation du respect de la politique de dépenses ;
- Technologie OCR+ basée sur l'intelligence artificielle et les algorithmes de Machine Learning ;
- Stockage dans le Cloud ;
- Statistiques intelligentes et Business Intelligence ;
- Intégration comptable ;
- Archivage numérique à valeur probante.

Marchés visés

Après le marché français, Expensya commence à proposer sa solution à l'international et elle équipe déjà les filiales de ses clients français répartis sur les 5 continents. La startup est à présent dans sa phase d'internationalisation, et la solution Expensya a été déclinée en six langues supplémentaires pour conquérir le marché européen et international.

Solutions/produits innovants

Expensya libère l'utilisateur de la saisie manuelle, il suffit juste de prendre en photo sa facture, et la fonctionnalité de reconnaissance intelligente s'occupe d'extraire toutes les informations pertinentes en quelques secondes (montant, TVA, catégorie de la dépense, devise, date, etc.). Le tout est ensuite stocké dans le Cloud afin de garder les justificatifs des dépenses. L'application gère également les flux de validation, l'automatisation des politiques de dépenses, l'intégration dans les systèmes comptables, et même l'archivage numérique à valeur probante. Expensya propose également un produit dédié aux experts-comptables : une solution spécifique à leurs besoins a été développée et est entièrement adaptée à la profession comptable « Expensya Expert ».

FANVOICE

Gael MULLER - CEO
06 72 67 30 42 - g.muller@fanvoice.com

FANVOICE permet aux marques et institutions de détecter des insights, co-créer des produits et services, puis bêta-tester leurs innovations avec des clients et/ou collaborateurs.

80, rue des haies, 75020 Paris
www.fanvoice.com
www.linkedin.com/company/fanvoice

Chiffres-clés

Date de création : 1er janvier 2014
Effectif en 2018 : 15
CA en 2018 : 900 000 €
Statut juridique : SASU
Projet(s) labellisé(s) : 1
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B Description du produit/service.
Description du produit/service : FANVOICE est une plateforme de co-création clé en main qui facilite la récolte d'idées, accélère l'analyse de feedbacks clients/collaborateurs pour améliorer et/ou bêta-tester un produit ou un service.

Expertise et savoir-faire

La solution FANVOICE :

- améliore l'image de marque (transparence, écoute, échange) ;
- transforme des données non-structurées (verbatims) en Smart Data réexploitable par la marque/l'institution ;
- divise par 2 le temps de mise en place d'une campagne de co-création ;
- est la première plateforme de cocréation à embarquer un outil d'analyse BIG DATA clé en main ;
- favorise la récolte de datas et améliore la connaissance client ;
- accélère l'analyse des contributions (jusqu'à 100 000/an d'économies en frais d'analyse de feedbacks).

Marchés visés

Études marketing et tests en ligne, sur tous types de secteurs avec forme d'expertise banque – assurance

Solutions/produits innovants

FANVOICE est la première plateforme de co-création « Big Data » clé en main, conçue pour aider les marques à mieux comprendre les attentes de leurs clients et collaborateurs. La solution combine les techniques de l'open innovation à plusieurs technologies (BIG DATA et Text Mining), méthodes (gamification et animation de communautés) et leviers pour favoriser la collaboration entre internautes autour d'un projet participatif, et automatiser l'analyse des données récoltées. En plus de récolter des « idées » brutes (comme d'autres plateformes de co-création), la solution permet de faire émerger les attentes « communes » des consommateurs (« clustering » d'idées, analyse du sentiment, détection d'insights et « data visualization »), tout en minimisant les traitements manuels et les coûts liés à ces opérations.

FIELDFISHER (FRANCE) LLP

Arnaud GRÜNTHALER - Associé
01 70 37 81 00 – arnaud.grunthaler@fieldfisher.com

Bruno PACCIONI - Managing Partner
01 70 37 81 00 - parisinfo@fieldfisher.com

Fieldfisher France est un cabinet européen d'affaires basé à Paris. Nous accompagnons une clientèle française et internationale dans tous les domaines du droit des affaires. Conseil et contentieux forment deux axes indissociables constituant l'identité de notre cabinet et notre référence sur le marché.

48, rue Cambon, 75001 Paris
www.fieldfisher.com/locations/paris
www.linkedin.com/company/fieldfisher
www.twitter.com/Fieldfisher?lang=fr

Chiffres-clés

Date de création : 2007
Effectif en 2018 : 70
Statut juridique : LLP
Pays d'implantation : Allemagne, Belgique, Chine, États-Unis, France, Italie, Luxembourg, Pays-Bas, Royaume-Uni

Mission et offres

Marchés cibles : majorité B2B.
Description du produit/service : Assistance en conseil et contentieux dans tous les domaines du droit des affaires, et plus particulièrement en ce qui concerne les fintechs. Nous sommes considérés comme une «go to firm» dans ce secteur et conseillons nos clients dans le cadre d'Initial Coin Offering (ICO), du traitement de problématiques relatives aux cybermonnaies, aux projets blockchain et de digitalisation de services notamment financiers.

Expertise et savoir-faire

Corporate M&A – Private Equity, Bourse et Marchés de Capitaux, Banque et Finance, Restructuration et Procédures Collectives, Droit Fiscal, Droit Social, Droit de la Concurrence, de la Distribution et des Contrats, Propriété Intellectuelle, Télécoms et Technologies, Environnement, Life Sciences, Afrique, Contentieux, Arbitrage, Immobilier, Blockchain, Énergie et Ressources Naturelles, Compliance.

Marchés visés

Établissements de crédit, sociétés de gestion, Fintech, AssurTech, sociétés souhaitant organiser leur financement via le lancement d'une ICO, projets Blockchain, prestataires de services offrant des services d'achat/vente, de conseil en investissement sur cybermonnaies, d'échange, de trading, de conservation de cybermonnaies

Solutions/produits innovants

- ICO (conseil juridique et fiscal) ;
- Mandat de gestion cybermonétaire ;
- Conseil en investissement cybermonétaire.

Nous avons conseillé parmi les ICO les plus significatives réalisées en France depuis 2016 jusqu'à ce jour (Ark Ecosystem, iEx.ec, Legolas Exchange (LGO Market), Gimli, Booking Token Unit (BTU), Galion, Varanida, IOV, CleverPlace, Arianee, Investig.io. Nous avons également assisté des acteurs tels que Coinhouse, Cryptobjectif, Consensy's (VariabL) ou Digital Services (Zebitcoin) dans la mise en place de solutions innovantes et conseillons actuellement des projets innovants de création d'applications, de plateforme ou de protocole utilisant les cybermonnaies et des blockchains publiques.

FINANCES & CRÉATION

Hervé DEREUMAUX – Gérant
06 76 40 15 69 – h.dereumaux@financesetcreation.fr

Édition et stratégie digitale.
99 bis, rue Lecocq, 33000 Bordeaux
www.financesetcreation.fr

Chiffres-clés

Date de création : septembre 2004
Effectif en 2018 : 7
CA en 2018 : 500 K€
Statut juridique : SARL
Projet(s) labellisé(s) : Mobile Finance (2015)
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B2C et B2B.
Description du produit/service : conception sur mesure de solutions digitales à l'attention des clients/prospects ou des conseillers commerciaux.

Expertise et savoir-faire

Transformation digitale de la relation clients axée sur une forte «expertise métier». Outils digitaux «sur mesure» à destination des conseillers commerciaux.

Marchés visés

Banques, Assurances et Mutuelles.

Solutions/produits innovants

Ensemble de supports digitaux (Application mobile, Vidéo Motion, Quiz interactif, Infographie…) à destination des clients et prospects sur les trois marchés : Particuliers, Professionnels et Entreprises sur l'ensemble des sujets de type patrimonial, social ou IARD.

FORMEE

Erwann BERTHELEME – Directeur Général
06 78 88 24 54 – erwann@formee.fr

Le coach financier des entrepreneurs.

23, rue de vienne, 75008 Paris
www.formee.fr

Chiffres-clés

Date de création : 2016
Effectif en 2018 : 5
Statut juridique : SAS
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B.
Description du produit/service : Pour les entrepreneurs qui se retrouvent seuls face à leur gestion, FORMEE automatise le suivi d'indicateur de gestion et la réalisation d'un prévisionnel de trésorerie. Il dispose ainsi, en temps réel, et sans effort, de tableaux de bord pour un pilotage efficace.

Expertise et savoir-faire

Gestion de trésorerie, Prévisionnel, machine learning, financement, coaching.

Marchés visés

Micro-entreprise, entrepreneur, TPE < 10 salariés.

Solutions/produits innovants

Le moteur de machine learning développé par FORMEE permet d'automatiser la réalisation d'un prévisionnel de trésorerie pour donner de la visibilité à l'entrepreneur sur son activité et son business.

FORTIA FINANCIAL SOLUTIONS

Rui Jorge LOPES – Strategy & Sales Manager
01 49 53 95 81 – ruijorge.lopes@fortia.fr

FORTIA est une start-up RegTech basée à Paris qui offre des solutions innovantes pour les établissements financiers. Notre plateforme basée sur l'Intelligence Artificielle accompagne nos clients dans l'automatisation et la digitalisation de leurs processus réglementaires, opérationnels et clients.

17, Avenue George V, 75008 Paris
www.fortia.fr
www.linkedin.com/company/fortia-financial-solutions

Chiffres-clés

Date de création : 2012
Effectif en 2019 : 93
CA en 2018 : 10 M€
Statut juridique : SAS
Projet(s) labellisé(s) : Innova
Pays d'implantation : France , en cours US courant Q1/2019

Mission et offres

Marchés cibles : Banque Dépositaire, Asset Manager, Banque de détail, Investment Banking, Wealth Management, Assurance.
Description du produit/service : dans les projets que nous avons déjà menés et que nous menons aujourd'hui avec de nombreux établissements bancaires et sociétés de gestion de fonds tant en Europe qu'aux États-Unis, **notre objectif est la digitalisation des processus réglementaires, opérationnels et clients**. Nos solutions sont basées sur des technologies de ruptures et alimentées par un centre de recherche composé de **16 Data Scientists et plus de 40 ingénieurs** diplômés des plus prestigieuses écoles et universités au niveau mondial.

Expertise et savoir-faire

Financière : FORTIA a été fondée par des professionnels de la gestion d'actifs. **Intelligence Artificielle :** déjà 6 brevets déposés et de nombreux concours gagné en France, US et Asie. Département de 16 Data Scientists avec PhD's.

Marchés visés

Europe, USA et asie.

GARANTME

Thomas REYNAUD - Fonction : CEO
+33 6 32 97 07 44 - thomas.reynaud@garantme.fr

Garantme facilite l'accès à la location des locataires sans garant grâce à sa caution distribuée 100 % en ligne.

5, rue Oberkampf, 75011 Paris
www.garantme.fr
www.facebook.com/garantme

Chiffres-clés

Date de création : octobre 2017
Effectif en 2018 : 2
Statut juridique : SAS
Projet(s) labellisé(s) : Garantme
Pays d'implantation : France

Mission et offres

Marchés cibles : Les 6 millions de locataires sans garant en France, étudiants, jeunes actifs, autoentrepreneurs, CDD…
Description du produit/service : Garantme est la première solution de garantie locative 100 % digitale et gratuite pour les bailleurs. Nous analysons, certifions et garantissons le dossier des locataires sans garant sur www.garantme.fr. La garantie est financée par la communauté de locataires. Nous facilitons la signature du bail pour le gestionnaire ou le bailleur en émettant la garantie dans la journée.

Expertise et savoir-faire

Notre expertise réside dans plusieurs domaines : le scoring de locataires, la gestion des flux et l'accompagnement vers la location.

Marchés visés

Nos marchés sont les marques du changement de logeAujourd'hui uniquement en France, nos marchés sont au Royaume-Uni, aux États-Unis et au Canada.

Solutions/produits innovants

Notre produit actuel est une garantie de loyers. Elle est enrichie à travers deux offres complémentaires : une assurance multirisque habitation et une offre de financement du dépôt de garantie.

GRANADA

Guillaume LANGÉAC – CEO
06 83 27 89 84 – guillaume@granada-project.com

Granada est la première marketplace internationale de données clients certifiées visant à améliorer les processus KYC/AML/CFT pour toute la communauté financière.

26, rue du Quatre Septembre, 75002 Paris
www.granada-kyc.com
LinkedIn : @granada-network
Twitter : @granadaKYC

Chiffres-clés

Date de création : 2017
Effectif en 2018 : 10
CA en 2018 : 200 K€
Statut juridique : SAS
Projet(s) labellisé(s) : Label Finance Innovation en juin 2018
Pays d'implantation : France, Luxembourg, Hong-Kong, Singapour

Mission et offres

Marchés cibles : B2B.
Description du produit/service : Granada est la première marketplace internationale de données clients certifiées. Face à la pression réglementaire et les coûts liés au KYC, Granada offre une nouvelle méthode de partage de données clients basée sur une blockchain privée (DLT) garantissant un haut niveau de sécurité. Granada aide ainsi les institutions financières à accéder à des données de qualité certifiées par leurs pairs

Expertise et savoir-faire

Granada cherche à mutualiser les efforts des institutions financières en échangeant des données clients certifiées par ces institutions elles-mêmes. La plateforme repose sur un arbre de décision basé sur les conditions de partage de données, reflétant les spécificités juridictionnelles de plus de 30 pays. La mutualisation de données KYC immuables, précises et échangeables de manière totalement sécurisée permettrait de :

- réduire les risques réglementaires et de réputation, voire de générer de nouveaux revenus;
- améliorer la qualité des données clients;
- optimiser l'expérience client.

Marchés visés

Granada s'adresse à l'ensemble des acteurs de l'industrie financière soumis aux mêmes exigences en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme, souhaitant mutualiser et valoriser leurs efforts de conformité réglementaire.

Solutions/produits innovants

La marketplace Granada offre de nouvelles méthodes de stockage, de partage et d'accès aux données clients (KYC/AML/CFT) pour la communauté financière, rendues possible grâce à une technologie DLT (Distributed Ledger Technology). Granada représente une proposition forte pour la communauté financière en termes de sécurité, de conformité et de réduction des coûts. Le partage des données clients aidera ainsi à relever le défi de l'inflation réglementaire.

HOMELINKS

Franck DE DIEULEVEULT – CEO
09 80 88 55 88 – franck@homelinks.eu

Lancé en 2018, Homelinks offre des services innovants pour faciliter le travail des gestionnaires d'immeubles résidentiels et d'entreprises.

1, villa Pilaudo
www.homelinks.eu
www.linkedin.com/company/homelinks-au-service-de-l-immeuble
Twitter : @homelinks_eu
www.youtube.com/channel/UCsjxZYPhqMI0TPsRm3yBopw

Chiffres-clés

Date de création : septembre 2017
Effectif en 2018 : 5
Statut juridique : SAS
Projet(s) labellisé(s) : Projet Alliance by Homelinks
Pays d'implantation : France

Mission et offres

Homelinks offre des services innovants pour faciliter le travail des gestionnaires immobiliers. Inspirés par les nouveaux usages, nos services sont conçus pour simplifier le quotidien des professionnels immobiliers en relation avec les occupants d'immeubles. Homelinks désamorce les problèmes au quotidien avant qu'ils ne se développent… pour une plus grande rentabilité partagée ! Notre mission est de centraliser la donnée des professionnels de l'immobilier de manière à rationaliser leur travail afin de leur dégager du temps pour un service de qualité personnalisé à chacun de leurs interlocuteurs. C'est pourquoi nous avons développé une offre qui s'adapte aux besoins de nos clients, véritable trait d'union entre les professionnels et les particuliers.

Expertise et savoir-faire

Notre expertise repose sur l'équipe qui est complémentaire dans ses profils. D'ailleurs les associés regroupent les expertises suivantes : Stratégie | Technologie | Commercial | Finance | Opérations. Ces expertises sont complétées par celles de l'équipe et de ses partenaires. Nos expériences ont été acquises dans des start up mais aussi au sein de groupes internationaux, en France et à l'étranger. Nous sommes avant tout des experts de l'immobilier et notre savoir-faire reposent sur l'expérience et l'apprentissage acquise au fil des ans. Enfin, notre capacité à nous remettre en question doublée d'un apprentissage continuel nous donne un avantage sur tous les changements à anticiper.

Marchés visés

Nous proposons nos services aux sociétés en charge de la gestion d'immobilier résidentiel et d'entreprise. Nos catégories de client sont les administrateurs de biens (syndic et gestion locative), les gestionnaires de patrimoine immobilier (ex : collectivités, caisses d'assurance), les bailleurs sociaux (ESH, OPH, sociétés coopératives d'HLM) et les promoteurs immobiliers. Une catégorie de client complémentaire est celle des prestataires d'immeubles qui sont les sociétés en charge des travaux et de l'entretien. Enfin, les bénévoles (conseil syndical et syndic bénévole) sont aussi visés comme catégorie de marché des particuliers.

IMMO FACTORY

Pierre VERGER – Directeur Général
07 89 53 24 89 – pverger@immo-factory.fr

Le digital au service de l'immobilier.
23, rue du roule, 75001 Paris
www.immo-factory.fr

Chiffres-clés

Date de création : 2014
Effectif en 2018 : 9
CA en 2018 : 1,4 M€
Statut juridique : SAS
Projet(s) labellisé(s) : CRM innovante
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B.

Expertise et savoir-faire

Digitalisation de l'achat/vente d'immobilier neuf.

Marchés visés

Professionnels de l'immobilier neuf : promoteurs, commercialisateurs, constructeurs, foncières.

ICARE TECHNOLOGIES SAS

Jeremy NEYROU - Président
0660794755 - jeremy.neyrou@icaretech.fr

Start-up dont le siège social se situe à Ajaccio. L'entreprise possède également des bureaux à la Grande Arche à la Défense de Paris. ICARE Technologies compte aujourd'hui une vingtaine d'employés

Immeuble Castellani, 4, av. du Mont Thabor 20090 Ajaccio
www.icaretechnologies.com/fr
www.linkedin.com/company/icaretechnologies

Chiffres-clés

Date de création : 14 avril 2016
Effectif en 2018 : 9
CA en 2018 : 9600 euros
Statut juridique : SAS
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B & B2C.
Description du produit/service : une bague intelligente autonome baptisée **Aeklys** qui permet de remplacer votre portefeuille et votre trousseau de clé. Vous allez pouvoir payer avec, ouvrir et démarrer votre voiture, accéder à vos locaux… Cette bague doit être synchronisée via une application mobile développée en interne qui permettra de gérer l'utilisation de la bague et ses diverses fonctionnalités. Nous avons également implémenté la technologie du « wave control », un contrôle total de l'émission via un bouton d'activation.

Marchés visés

Notre bague Aeklys s'insère dans plusieurs marchés : le Resort, le Stadium pour l'identification & le contrôle d'accès, le paiement, l'automobile pour le démarrage et le déverrouillage du véhicule.

INCUBE

Philippe LEPEUPLE – Président et Fondateur
+33 1 822 855 32 – philippe.lepeuple@incube.fr

Fintech - inCube a conçu et développé PolySeme, une plateforme digitale en marque blanche qui permet au Client de piloter son contrat d'assurance vie multisupport à travers ses Projets de vie.

82, rue d'Amsterdam 75009 Paris
www.incube.fr
www.twitter.com/PolySeme_by_in3
www.linkedin.com/company/polyseme_by_incube
www.youtu.be/48dZ5Wc6eJk

Chiffres-clés

Date de création : 2013
Effectif en 2018 : 3 (hors externes)
Statut juridique : SAS
Projet(s) labellisé(s) : PolySeme
Pays d'implantation : France

Mission et offres

Marchés cibles : La solution PolySeme développée par inCube est une plateforme en marque blanche, destinée aux assureurs, bancassureurs et distributeurs de produits d'assurance vie. B2B, et B2B2C.
Description du produit/service : inCube redonne du sens à l'épargne :

- En agissant sur ses Projets de vie à travers une interface intuitive, le Client pilote son contrat, seul ou avec un Conseiller ;
- L'allocation d'actifs est dynamiquement déterminée et intégrée au back-office ;
- PolySeme peut être déployé sur des Stocks ou Affaires Nouvelles et agit sur les leviers de rentabilité ;
- PolySeme s'interface simplement avec l'environnement de l'assureur.

Expertise et savoir-faire

- La solution développée par inCube a été labellisée par le Pôle Finance Innovation et est lauréate de l'Argus d'Or de l'Innovation 2016 ;
- La Fintech inCube capitalise à ce jour plus de 4 années de R&D, 2 ans de développements IT et 3,7 M€ d'investissements ;
- InCube s'est appuyé sur l'expertise de son équipe, des personnalités expérimentées dans le domaine des services financiers et de l'assurance, dont les compétences sont complémentaires : Assurance de personnes, Distribution, UX, IT, Back Office, Algorithmique, Finance, Marketing, Gestion agile de Projets, Transformation.

Marchés visés

La solution vise principalement une clientèle d'épargnants mass affluent et au-delà. Elle peut être déployée et adaptée à tout type de distribution : intermédiée (agents, courtiers, réseaux de conseillers), ou directe. La plateforme est nativement multilingue et fonctionne déjà en français, anglais et portugais.

Solutions/produits innovants

- PolySeme by inCube, labellisée par le Pôle Finance Innovation et est lauréate de l'Argus d'Or de l'Innovation 2016.

INSTITUT DE RECHERCHE BIOMÉDICALE DES ARMÉES

Médecin Général Inspecteur Anne SAILLOL – Directrice

L'Institut de recherche biomédicale des armées (Irba) est un organisme public français spécialisé dans la recherche biomédicale, il est une des composantes du Service de santé des armées (SSA) placé sous l'autorité du ministère de la Défense.

1, place Valérie André, 91223 Brétigny-sur-Orge Cedex
www.defense.gouv.fr/sante/notre-expertise/recherche-biomedicale/recherche-biomedicale

Chiffres-clés

Date de création : 1er mars 2009

Expertise et savoir-faire

L'Irba a une double mission :
- répondre aux besoins exprimés par les États-majors en matière de protection du combattant ;
- anticiper les besoins en comblant les lacunes capacitaires des Forces armées françaises.

Les travaux réalisés à l'Irba s'inscrivent dans les champs de la défense et de la sécurité. Ses recherches ont pour objectifs de protéger et prévenir les militaires français des menaces et des contraintes particulières induites par le contexte opérationnel, mais aussi d'améliorer la prise en charge et le traitement des maladies et des blessés. L'Irba contribue également à la mission de santé publique en participant aux différents plans d'urgence gouvernementaux destinés à faire face aux risques NRBC d'origine accidentelle ou terroriste.

INVIVOO

Guillaume MOREL - PDG
+33 1 80 88 70 00 - admin@invivoo.com

En combinant l'expertise métier à l'expertise technologique, Invivoo transforme les systèmes d'information à tous les niveaux des entreprises du secteur financier.

France : Tour Franklin, 100-101, terrasse Boieldieu, 92042 Paris La Défense Cedex
Royaume-Uni : Landsdowne House / City Forum, 250 City Road, London EC1V 2PU
www.invivoo.com/
www.linkedin.com/company/invivoo

Chiffres-clés

Date de création : 2004
Effectif en 2018 : 240
CA en 2018 : 22 M€
Statut juridique : SAS
Pays d'implantation : France, Royaume-Uni

Mission et offres

Marchés cibles : B2B.
Description du produit/service : Nous combinons notre activité de conseil, d'audit et d'édition de logiciel afin de concrétiser les exigences métier de nos clients. Aussi, nous accompagnons nos clients dans le développement de leurs compétences à travers un catalogue de formations.

Expertise et savoir-faire

La valeur ajoutée d'Invivoo est la maîtrise des différentes technologies dont la robotisation, le big data, l'intelligence artificielle (IA), les systèmes temps réel, ainsi que la blockchain en leur donnant du sens dans le cadre des activités métiers de nos clients.

Marchés visés

Dans un contexte toujours plus complexe, s'appuyer sur des solutions informatiques performantes est un enjeu vital. C'est pourquoi Invivoo souhaite apporter son expertise technologique, méthodologique et organisationnelle au service des équipes métier de tous les secteurs.

Solutions/produits innovants

Chatbot Fabric est la plateforme de développement de chat bot modulaire et multicanal basée sur des modules d'intelligence artificielle et de gestion de contextes conversationnels à destination d'utilisateurs non techniques. Grâce à son interface web, Chatbot Fabric vous permet :
- Une gestion d'inputs conversationnels hétérogènes (texte, image, voix...);
- Une gestion de conversation multi-contextes,
- Une gestion de conversation multi-langues,
- Une gestion de message multi-intentions et d'entités composites;
- Une intégration facilitée au système d'information de l'entreprise;
- De bénéficier de modèles cognitifs préconstruits et de composants réutilisables;
- De disposer de bases de connaissance intégrées.

XComponent Koordinator est un portail web où chaque utilisateur est identifié. Celui-ci peut accéder selon ses droits, à un environnement complet de design, de gestion, et d'exécution de scénarios, avec des applications dans de nombreux domaines comme le Big Data, le SI-RH, la gestion d'opération de production ou plus généralement la modélisation de processus métier. XComponent Koordinator est un client web léger. Sans aucune installation sur le poste, la plateforme permet d'accéder à de nombreuses fonctionnalités applicatives.

IXTEL

Jacques BAUDRON – Gérant
06 60 62 79 74 – jacques.baudron@ixtel.fr

Ingénierie Conseil Services Telecom. Recherche, conseil et formation en télécoms blockchain, Intelligence Artificielle et Information quantique auprès des étudiants et des milieux professionnels.

36, avenue d'Assas, 78470 Saint-Rémy-lès-Chevreuse
www.ixtel.fr

Chiffres-clés

Date de création : 1998
Effectif en 2018 : 1
Statut juridique : EURL
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B.
Description du produit/service :
- Simulation comportementale,
- Formations et séminaires sur Blockchain, Intelligence Artificielle et Information quantique

Expertise et savoir-faire

Pédagogie Blockchain, Intelligence Artificielle et Information quantique. Qualité des données, simulation comportementale.

Marchés visés

Universités, séminaires professionnels.

IZNES

Jean-Robert HERVY – Directeur Général
+33 6 62 66 52 08 – jean-robert.hervy@iznes.io

Plateforme internationale d'achat et de vente de parts d'OPC européens développée en Blockchain par des sociétés de gestion.

8, rue Lamennais, 75008 Paris
www.iznes.io
www.linkedin.com/company/iznes
www.twitter.com/IZ_NES - @IZ_NES

Chiffres-clés

Date de création : 2017
Effectif en 2018 : 2
CA en 2018 : 60 000 €
Statut juridique : SAS
Projet(s) labellisé(s) : Iznes
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B.
Description du produit/service : IZNES est une plateforme internationale d'achat et de vente de parts d'OPC européens développée en Blockchain par des sociétés de gestion et SETL. IZNES fournit aux investisseurs et aux sociétés de gestion un service complet : entrée et suivi de la relation entre investisseurs et sociétés de gestion, référentiel OPC complet, souscriptions et rachats de parts d'OPC en direct, tenue de registre en temps réel et reportings. Grace à la technologie Blockchain de SETL, IZNES réduit les coûts d'achat et de vente de parts de fonds, apporte plus de transparence et simplifie les relations entre investisseurs et sociétés de gestion.

Expertise et savoir-faire

- Gestion des dossiers clients (KYC, LAB/FT, MIF 2);
- Référentiel OPC;
- Souscriptions et Rachats de parts d'OPC;
- Gestion d'Actif;
- Blockchai.

Marchés visés

- Investisseurs Institutionnels et Corporates;
- Assureurs Vie;
- Sociétés de Gestion d'OPC, de mandats d'investisseurs institutionnels ou de mandats de personnes physiques;
- Distributeurs de parts d'OPC;
- Conseillers en Gestion de Patrimoine (CGP)...

Solutions/produits innovants

La nature même d'IZNES est innovante. IZNES est le seul Asset Servicer dont la conception des services et la gouvernance sont assurées directement par des sociétés des gestion. Par ailleurs, la solution technologique Blockchain de SETL permet d'avoir une solution digitale disruptive et efficace.

KERNIX

François-Xavier BOIS – Gérant
01 53 98 73 40 – fxbois@kernix.com

Cabinet d'expertise en technologies reposant sur une Digital Factory et un Data Lab.

6, rue Lalande 75014 Paris
www.kernix.com
fr.linkedin.com/company/kernix

Chiffres-clés

Date de création : 2001
Effectif en 2018 : 45
CA en 2018 : 3,9 M€
Statut juridique : SAS
Projet(s) labellisé(s) : Scoring ML
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B.
Description du produit/service : conception, Réalisation et maintenance de plateformes digitales.

Expertise et savoir-faire

Datasciences, IA, Graph Mining, Traitement automatique de données non structurées (textes, images).

Marchés visés

Kernix s'adresse à toutes les entreprises cherchant à transformer leurs idées en réalisations digitales sûres et performantes

Solutions/produits innovants

Kernix combine ses expertises en digital en en data pour fournir à ses clients des plateformes numériques complètes.

KRIPTOWN

Mark KEPENEGHIAN – Président
06 72 99 79 46 – mark@kriptown.com

La Bourse des start-up – Nouvelle forme d'investissement liquide pour contribuer au financement des start-up.

118, Avenue du général Leclerc, 75014 Paris
www.krip.town
www.linkedin.com/company/kriptown

Chiffres-clés

Date de création : mars 2018
Statut juridique : SAS
Projet(s) labellisé(s) : Kriptown
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B (start-up) et B2C (investisseurs).
Description du produit/service : Kriptown démocratise l'investissement en start-up en proposant à des investisseurs d'acheter, dès un euro, des tokens de la start-up liés à la valeur de ses parts. Grâce à l'utilisation d'une blockchain privée, la plateforme permet d'offrir de la liquidité en donnant l'accès à un marché secondaire permettant de revendre ou d'acheter des tokens à tout instant.

LABORATOIRE INFORMATIQUE GRENOBLE CNRS – UGA – GINP – INRIA

Éric GAUSSIER – PROF UGA
04 57 42 15 00 – eric.gaussier@univ-grenoble-alpes.fr

L'ambition est de s'appuyer sur la complémentarité et la qualité reconnue des équipes de recherche du LIG pour contribuer au développement des aspects fondamentaux de l'informatique (modèles, langages, méthodes, algorithmes) et pour développer une synergie entre les défis conceptuels, technologiques et sociétaux associés à cette discipline.

Bât. IMAG, 700 avenue Centrale, 38401 St-Martin d' Hères
www.liglab.fr/fr

Chiffres-clés

Date de création : 2007
Effectif en 2018 : 500
Pays d'implantation : France

Expertise et savoir-faire

La diversité et la dynamicité des données, des services, des dispositifs d'interaction et des contextes d'usage imposent l'évolution des systèmes et des logiciels pour en garantir des propriétés essentielles telles que leur fiabilité, performance, autonomie et adaptabilité. Relever ces défis trouve une résonance dans les cinq axes thématiques de recherche explorés au LIG :

- Génie des Logiciels et des Systèmes d'Information ;
- Méthodes Formelles, Modèles et Langages ;
- Systèmes Interactifs et Cognitifs ;
- Systèmes Répartis, Calcul Parallèle et Réseaux ;
- Traitement de Données et de Connaissances à Grande Échelle.

Le LIG se veut un laboratoire centré sur les fondements et le développement des sciences informatiques, tout en veillant à une ouverture ambitieuse sur la société pour en accompagner les nouveaux défis.

LE PARTENAIRE

Ludovic LABORDE – Directeur Général
06 42 17 58 33 – l.laborde@le-partenaire.fr

Précurseur de la digitalisation et de l'automatisation du parcours client sur le marché du crédit et de l'assurance.

8, quai de la Madeleine, 45000 Orléans
www.le-partenaire.fr

Chiffres-clés

Date de création : 2014
Effectif en 2018 : 12
CA en 2018 : + 500 k€
Statut juridique : SAS
Projet(s) labellisé(s) : 2017
Pays d'implantation : France

Mission et offres

Marchés cibles : B2C et B2B.
Description du produit/service : Digitalisation de la distribution crédits & assurances pour les particuliers et les professionnels.

Expertise et savoir-faire

Nous automatisons l'approche bancaire et assurantielle au niveau du parcours client afin de commercialiser des offres dédiées et qualifiées. Nos algorithmes prédictifs génèrent un matching des offres pour chaque profil client :

- Analyse et Traitement de l'information disponible en BDD ;
- Rapprochement Profil client/Offres pour proposer la meilleure solution personnalisée : crédit + assurance ;
- Analyse prédictive des besoins tout au long du projet

Les bénéfices clients :

- Le client génère en quelques clics un contrat via une expérience enrichissante ;
- Souscription dématérialisée via paiement en ligne et signature électronique ;
- Personnalisation du parcours client, avec un mix humain/digital.

Le Partenaire en quelques chiffres :

- 1 700 000 annonces immobilières et plus de 50 000 professionnels ;
- + 70 000 particuliers ;
- + 3 200 prospects/mois.

Marchés visés

- B2C : 3 millions de Français chaque année en phase de changement de vie immobilière ;
- B2B : TNS, TPE et petite PME.

Solutions/produits innovants

Capter et transformer à moindres coûts des prospects en recherche de crédit et d'assurance. Développer des portails web permettant aux clients de réaliser leurs démarches en ligne de manière simple, fluide et rapide (une expérience client unique et novatrice). Concevoir une plateforme digitale de distribution BtoBtoC de crédits et d'assurances à destination de l'ensemble des professionnels de l'immobilier, du crédit et de l'assurance (affiliés).

LEXING ALAIN BENSOUSSAN AVOCATS

Alain BENSOUSSAN – Président
01 82 73 05 05 – alain-bensoussan@alain-bensoussan.com

Réseau international d'avocats dédié au droit du numérique et des technologies avancées.

58, boulevard Gouvion-Saint-Cyr, 75017 PARIS
www.alain-bensoussan.com
LinkedIn, Facebook et Twitter (@AB_Avocats)

Chiffres-clés

Date de création : 1978
Effectif en 2018 : 120 personnes, dont une centaine d'avocats
Statut juridique : SELAS
Pays d'implantation : Une trentaine de cabinets sur les cinq continents.

Expertise et savoir-faire

Depuis sa création en 1978, le cabinet Lexing Alain Bensoussan Avocats se consacre au droit des nouvelles technologies, dans le domaine du droit de l'informatique, des télécommunications et de la propriété intellectuelle. Ce choix précurseur lui a permis de développer son expertise et d'être à la pointe des meilleures pratiques juridiques dans tous les domaines du numérique et des technologies avancées au fur et à mesure de leur développement. Novateur dans son organisation, sa gestion et son système qualité, il devient le premier cabinet d'avocat français à être certifié ISO en 1998. Son équipe composée d'avocats technologues associe la connaissance des secteurs techniques et du droit spécifique qui s'y applique, et apporte son savoir-faire dans tous les axes d'exercice du métier.

Marchés visés

Le cabinet conseille et assiste, en conseil comme en contentieux, la totalité des activités dédiées aux technologies avancées, par secteurs technologiques, économiques et juridiques :

- Éditeurs & prestataires, dans tous les domaines technologiques ;
- Utilisateurs dans tous les secteurs : assurance, service, banque, industrie, santé… ;
- Grands comptes internationaux et français ;
- Collectivités territoriales et ministères ;
- Start up & incubateurs.

Solutions/produits innovants

Le cabinet, qui a fait de l'innovation sa première valeur et son marqueur de différenciation, continue d'offrir de nouveaux services juridiques : depuis 2016, il propose à ses clients une plateforme d'outils juridiques simples, intuitifs et accessibles en mode SaaS depuis n'importe quel équipement connecté à internet (ordinateur, tablette, smartphone) et dont les contenus sont à jour des dernières évolutions législatives, réglementaires et jurisprudentielles.

LINGUA CUSTODIA

Olivier DEBEUGNY – Président
06 12 73 85 87 – olivier.debeugny@linguacustodia.com

Lingua Custodia est le spécialiste de l'intelligence artificielle appliquée à la traduction financière.

1, place Charles de Gaulle, 78180 Montigny-le-Bretonneux
www.linguacustodia.finance
www.linkedin.com/company/lingua-custodia

Chiffres-clés

Date de création : 2011
Effectif en 2018 : 10
Statut juridique : SAS
Projet(s) labellisé(s) : 2014
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B, institutions financières (buy side and sell side), Directions financières de grands groupes.
Description du produit/service : Lingua Custodia applique des techniques de machine learning à la linguistique financière pour développer des outils de traduction automatique personnalisables et spécialisés dans le domaine financier. Ces outils disponibles en ligne réduisent les coûts de communication multilingue des institutions financières grâce à des résultats de plus en plus pertinents au fur et à mesure de leur utilisation.

Expertise et savoir-faire

- Natural Language processing ;
- Machine Learning ;
- Deep Learning ;
- Big Data ;
- Sémantique et linguistique financière.

Marchés visés

Lingua Custodia aide les professionnels de la finance à gérer les traductions traitées en interne du fait de leur urgence ou de leur technicité et leur permet d'y consacrer moins de temps et de ressources. La société fournit aussi un service de traduction finalisée par forfait grâce à sa technologie.

Solutions/produits innovants

Lingua Custodia a conçu et développé VERTO, un outil qui permet de diviser par trois le temps passé en traduction par les professionnels de la finance. VERTO a cette particularité de pouvoir « apprendre » des textes précédemment traduits par ses utilisateurs et de prendre en considération chacune des corrections effectuées sur les résultats proposés.

MARGO

Xavier LAGARRIGUE – Associé Fondateur
+33 6 61 37 11 55 – xavier.lagarrigue@margo-group.com

Tech native, Margo est une société de conseil qui accompagne les entreprises dans leur transformation digitale sur des sujets à forte complexité technologique.

#LaPiscine – 9, rue Christophe Colomb, 75008 Paris
www.margo-group.com
www.linkedin.com/company/margofr

Chiffres-clés

Date de création : 2005
Effectif en 2018 : 300
CA en 2018 : 25,6 millions d'euros
Statut juridique : SAS
Pays d'implantation : France – Angleterre – Pologne

Mission et offres

Marchés cibles : B2B.
Description du produit/service : Les offres de Margo s'organisent autour de 4 piliers de savoir-faire : Business Agility, Haute performance IT, Data to Business et Modernisation de SI. En plaçant l'innovation au cœur de son modèle, Margo guide les entreprises dans leurs choix stratégiques et la création de technologies innovantes, dans l'objectif d'acquérir un avantage concurrentiel.

Expertise et savoir-faire

Design IT competitive advantage whatever business sector
De plus en plus, les entreprises mettent l'IT au cœur de leur Business model car elles ont besoin de se doter d'outils qui seront des avantages concurrentiels. Grâce à son offre de Business Agility, Margo crée d'abord les conditions favorables à la transformation à tous les niveaux, Management, Business et IT. Ensuite nous intervenons sur des sujets clés à forte complexité technique : la Haute Performance IT, la Data to Business et la Modernisation de SI. Nous investissons aussi en R&D sur des sujets de Code-Mining et profitons de l'écosystème des startups créées par nos fondateurs. Et nous vivons d'ailleurs dans un start-up studio qui s'appelle #LaPiscine.

Marchés visés

Expert historique en Finance de marché, Margo accompagne les entreprises de toutes tailles et tous secteurs d'activité (Finance, Assurance, Énergie, Retail, Industrie, Telecom, Secteur Public…) sur leurs projets de transformation digitale en France et à l'international.

Solutions/produits innovants

CodeCase, a technology from the R&D program "Code Mining", accelerates and securizes code modernization projects.

MIEUXPLACER.COM

Guillaume-Olivier DORÉ - Fondateur et CEO
06 70 79 70 90 – guillaume-olivier.dore@mieuxplacer.com
Matthieu SÉNÉCHAL – cofondateur et Chief Science Officer
06 50 85 46 74 – matthieu.senechal@mieuxplacer.com

Mieuxplacer.com, une plateforme grand public de distribution de produits financiers première de son espèce en France. Sécurisée, gratuite et personnalisée, elle accompagne, grâce à l'intelligence artificielle, ses clients dans leurs choix, le suivi des performances et l'évolution de leurs placements.

9, rue André Darbon, 33300 Bordeaux (siège social)
16 avenue Kléber, 75016 Paris
www.mieuxplacer.com/
www.linkedin.com/company/mieuxplacer-com

Chiffres-clés

Date de création : 2016
Effectif en 2018 : 15
Statut juridique : SAS
Projet(s) labellisé(s) : mieuxplacer.com a été labellisé le 8 décembre 2018 par le pôle de compétitivité Finance Innovation.
Pays d'implantation : France

Mission et offres

Marchés cibles : B2C.
Description du produit/service : L'épargne digitale et performante, accessible à tous ! Sécurisée, gratuite et personnalisée, la plateforme mieuxplacer.com utilise le meilleur de l'intelligence artificielle appliquée à la finance pour identifier les placements adaptés à votre profil et à vos objectifs d'épargne.

Expertise et savoir-faire

Notre expertise repose sur notre capacité à profiler notre utilisateur afin de lui proposer une recommandation globale et personnalisée de produits financiers. Grâce à nos outils de data science, nous analysons son comportement afin de nourrir l'intelligence artificielle et le machine learning de notre plateforme. Développée en interne par notre département R&D, notre IA a été pensée en étroite collaboration avec notre équipe d'experts en gestion de patrimoine. Leur mission est double pour mieuxplacer.com :

- ils nous permettent de la faire évoluer afin de la rendre la plus humaine possible dans ces choix ;
- ils sourcent et identifient les meilleurs produits de placements disponibles sur le marché pour l'épargne de nos clients.

Marchés visés

Notre ambition est de démocratiser le conseil en Gestion de Patrimoine, encore trop souvent réservé à une élite. Nous cherchons à toucher le grand public : quel que soit leur profil, quels que soient les objectifs, tous les épargnants peuvent investir et bénéficier de conseils gratuits sur mieuxplacer.com.

Solutions/produits innovants

Notre plateforme d'épargne assistée par l'intelligence artificielle.

MONEMPRUNT.COM

Gaëlle AUBREE – Directrice générale adjointe
06 17 23 45 26 – gaelle.aubree@monemprunt.com

monemprunt.com est la solution qui simplifie l'accès au crédit immobilier pour les particuliers > 100% en ligne, gratuit, rapide.

1, rue Robert Duvivier, 35000 Rennes
Grande Arche de La Défense
www.monemprunt.com
LinkedIn/Facebook/Twitter : monemprunt.com

Chiffres-clés

Date de création : juillet 2016
Effectif en 2018 : 6
Statut juridique : SAS
Projet(s) labellisé(s) : Finance Innovation – Le Swave.
Pays d'implantation : France

Mission et offres

Monemprunt.com est une plateforme qui digitalise, simplifie, accélère toutes les étapes de la demande de crédit jusqu'au déblocage des fonds. Elle s'appuie sur de puissants algorithmes qui recherchent en temps réel les meilleures offres des banques en fonction du projet et du profil (pré-accord de faisabilité instantané) et sur une équipe d'experts financier qui prennent en charge les dossiers des clients de A à Z.

Expertise et savoir-faire

Monemprunt.com facilite le parcours de tous les acteurs du financement immobilier : acquéreur, courtier, banquier, agent immobilier. Le back off de l'étude de financement est réalisé par monemprunt.com : avec une partie automatisée et scorée et une partie par nos experts. Seuls les dossiers complets, analysés et finançables sont transmis aux banques les plus pertinentes en fonction de leurs conditions du moment. Un gain de temps pour les banques et pour les clients qui reçoivent une réponse en quelques jours.

Marchés visés

- Cible de jeunes urbains particuliers de 25 à 40 ans : première acquisition immobilière;
- Les acteurs immobiliers, sensibles à l'innovation, qui souhaitent améliorer leur processus de vente et accélérer la signature des compromis via un financement rapidement ficelé;
- Les banques régionales et nationales qui souhaitent acquérir de nouveaux clients.

Solutions/produits innovants

Le caractère innovant repose sur :

- La simplification du process pour l'emprunteur qui réalise un achat immobilier et obtient un service de recherche de financement 4 étoiles, sans déplacement, sans frais, dans des délais très courts. Il obtient instantanément un pré accord de faisabilité ainsi que sa capacité maximum d'emprunt.
- Le temps de traitement et d'analyse divisé par 3 pour l'équipe d'experts financiers monemprunt.com par rapport à un traitement classique dans un cabinet de courtage => grâce aux algorithmes, aux contrôles automatiques, à la génération automatique des synthèse et des alertes au client emprunteurs et aux banques.
- Pour les banques : dossier scoré correspondant à leur cible, complet avec l'ensemble des pièces administratives accessible en 1 clic.
- Pour les acteurs immobiliers, des outils de validation immédiate de la capacité d'emprunt permettent de verrouiller et accélérer les ventes en rassurant les vendeurs et les acquéreurs.

MONUMA

Emmanuel MOYRAND – Président
06 87 40 62 76 – e.moyrand@monuma.fr

Un expert dans votre poche 24/24. PARIMONIA : première application blockchain valorisant les objets de valeurs par photographies, constatant des situations par blockchain, et valorisant globalement des risques. TRANSPORT : Première application blockhain scannant toute la chaine du transport, avec un expert encapsulé en back.

41, allée du butard 92420 Vaucresson
Bureau parisien : station F 75013
www.monuma.fr
monuma/@mouma_art/blog monuma

Chiffres-clés

Date de création : 2017
Effectif en 2018 : 2
CA en 2018 : 100 000 €
Statut juridique : SAS
Projet(s) labellisé(s) : Blockchain Patrimonia
Pays d'implantation : France, Espagne, Monaco

Mission et offres

Marchés cibles : assureurs, banques, immobilier, collaboratif.
Description du produit/service : Première application blockchain valorisant les objets de valeurs par photographies, constatant des situations par blockchain, et valorisant globalement des risques. Première application blockhain scannant toute la chaine du transport, avec un expert encapsulé en back. En un mot : le tiers de confiance blockchain dans votre poche.

Expertise et savoir-faire

Biens de valeurs, transport, assurance, expertise valorisation.

Marchés visés

Assureurs, banques, immobilier, collaboratif, marques de luxe.

Solutions/produits innovants

PARIMONIA : Première application blockchain valorisant les objets de valeurs par photographies, constatant des situations par blockchain, et valorisant globalement des risques. TRANSPORT : Première application blockhain scannant toute la chaine du transport, avec un expert encapsulé en back.

MYDATABALL

Stéphane CHAUVIN – CEO
06 79 86 42 01 - stephane.chauvin@mydataball.com

Plateforme visual data analytics et IA collaboratif.

38, rue de la blauderie, 79000 Niort
www.myDataBall.com
www.linkedin.com/in/schauvin

Chiffres-clés

Date de création : janvier 2010
Effectif en 2018 : 5
CA en 2018 : 250
Statut juridique : SAS
Projet(s) labellisé(s) : MyDataBall
Pays d'implantation : France

Mission et offres

Marchés cibles : banque assurance, énergie, eau.
Description du produit/service : nous éditons la solution MyDataBall, plateforme analytics qui accélère la capacité à analyser de grands volumes de données et détecter les insights d'optimisation métier, de mettre l'expérience des collaborateurs au centre de la performance des entreprises.

Expertise et savoir-faire

Machine learning pour marketing analytique, finance optimisation, CdG performance, Risk Management, Knowledge Discovery Management, performance commerciale multicanal.

Marchés visés

Notre offre se porte pour toute activité qui consomme de la donnée pour l'aide à la décision. Nos verticaux sont construits sur les métiers de la performance des entreprises.

Solutions/produits innovants

Le processus MyDataBall de fabrication industrielle de consommation de données par l'IA permet de :

- Pour accéder rapidement au patrimoine numérique métier étendu ;
- Pour accélérer la capacité d'analyse ;
- Pour synthétiser la détection des diagnostics métier par votre IA ;
- Pour répondre aux enjeux de la communication des chiffres et d'optimiser les tableaux de bord corporate par l'IA ;
- Pour capitaliser sur les connaissances métiers des collaborateurs.

Grâce à notre moteur MyDataBall, les utilisateurs peuvent créer leurs propres règles afin de profiler les insights à fort retour sur investissement et d'augmenter la performance par l'expérience des utilisateurs métiers. Notre innovation rompt les verrous technologiques de l'auditabilité de l'IA par la spécificité de mise à disposition visuelle et multidimensionnelle des résultats des machines learning co-construits par les collaborateurs. Le livrable des projets est une industrialisation des insights métiers par la plateforme MyDataBall.

NAPOLEON INDEX

Arnaud DARTOIS – CEO
+33 6 17 62 52 95 – arnaud@napoleonindex.com

Agent Calculateur & Administrateur d'indices offrant publication classique et certification sur la blockchain.

59 Rue Montmartre, 75002 Paris
www.napoleonindex.com
www.linkedin.com/company/napoleonx

Chiffres-clés

Date de création : avril 2018
Statut juridique : SAS
Projet(s) labellisé(s) : en cours – Soutenance du 21 Mars 2019
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B.
Description du produit/service : Napoleon Index est un administrateur d'indices selon la directive benchmark (enregistrement en cours auprès de l'AMF). Au delà du calcul et de l'administration d'indices, Napoleon Index ambitionne d'utiliser au mieux la blockchain pour élever les standards de transparence dans cette activité, en proposant un audit track blockchainé via son moteur de certificats horodatés.

Expertise et savoir-faire

Napoleon Index se démarque par une expertise et un savoir-faire uniques :

- Administrateur de benchmark : enregistrement en cours selon la directive benchmark (enregistrement annoncé pour le 15 février). Seulement la deuxième société en France avec cette certification;
- Calculateur d'indice et Review (révision des indices) : plateforme unique et sécurisée, structurée en micro services redondants et facilement adaptable à une montée en charge importante;
- Certification Blockchain : moteur de publication de certificats horodatés sur la blockchain. Certification à révélation différentiée applicable au paper trading de solutions d'investissement algorithmiques, aux analyses d'actions prospectives et aux recommandations.

Marchés visés

Napoleon Index propose des solutions de calcul d'indices à des clients professionnels tels que des banques, gestionnaires d'actifs et courtiers. Napoleon Index a pour ambition de s'imposer comme une alternative Française, technologique et économique, sur le marché de la publication et de l'administration d'indices.

Solutions/produits innovants

Outre le calcul et l'administration classique d'indices, Napoleon Index est le seul acteur à proposer un audit-track basé sur la blockchain et un moteur de certificats horodatés applicables aux recommandations et analyses d'opérations sur titres.



NEPHELAI

Eléonore DE VIAL – Présidente
06 85 74 21 25 – eleonore.devial@nephel-ai.com

Nephelai est une solution d'assistance à la saisie d'ordres et de transactions financières pour les banques et sociétés de gestion.

34, rue Dombasle, 75015 Paris
www.nephelai.eu/
www.linkedin.com/company/nephel-ai/about

Chiffres-clés

Date de création : novembre 2018
Effectif en 2018 : 5
CA en 2018 : 60 000 €
Statut juridique : SAS
Projet(s) labellisé(s) : oui
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B, banques d'investissement, gestionnaire d'actifs, asset servicers.
Description du produit/service : Nephelai utilise le Machine Learning pour détecter les erreurs sur les transactions/instruments financières, afin d'aider les institutions financières à contrôler leurs coûts de transactions et atteindre l'excellence opérationnelle. La solution se branche dans la chaine de traitement des opérations à différents niveaux pour détecter plus de 90% des erreurs le jour de négociation.

Expertise et savoir-faire

Notre équipe fondatrice se compose de 5 associés aux compétences et expériences complémentaires. Elle cumule en particulier 35 années d'expérience dans l'édition de logiciels financiers, la création d'une précédente startup à succès, 3 ans d'étude spécifique sur l'application d'algorithmes de Machine Learning à la détection d'erreurs dans les transactions et une expertise des métiers de la gestion d'actifs. La combinaison de la connaissance métier et de l'IA fait la force de Nephelai. Notre solution montre d'excellents résultats tout en répondant aux exigences métier. Les alertes sont enrichies d'explications détaillées pour guider les utilisateurs, les prédictions sont réalisées en quelques millisecondes pour un impact minimal sur la chaine de traitement des opérations, les données des transactions passées sont consommées au fil de l'eau et non stockées pour garantir leur confidentialité.

Marchés visés

Notre solution s'adresse à toutes les institutions financières ayant des volumes de transactions significatifs (plus de 200 transactions par an et par classe d'actif.) En particulier, notre solution intéresse les sociétés de gestion qui traitent des titres et produits dérivés.

Netheos
Accélérez votre confiance digitale

NETHEOS

Olivier DÉTOUR – CEO & Fondateur
06 17 37 14 71 – o.detour@netheos.net

Netheos accompagne les institutions financières dans leur parcours de souscription digitalisé conciliant KYC et expérience utilisateur.

1025, Henri Becquerel, Parc Club du Millénaire, Bat 18, 34000 Montpellier
www.netheos.com
fr.linkedin.com/company/netheos
www.twitter.com/Netheos

Chiffres-clés

Date de création : 2004
Effectif en 2018 : 15
CA en 2018 : 2 M€
Statut juridique : SAS
Projet(s) labellisé(s) : Trust & Sign
Pays d'implantation : France, Belgique, Portugal, Italie

Mission et offres

Marchés cibles : B2B(2C).
Description du produit/service : La solution Saas, Trust and Sign de Netheos, supprime le papier et utilise l'Intelligence Artificielle pour sécuriser et accélérer la vente en ligne de produits bancaires et assurantiels. Le motion design Trust and Sign (2 min) : www.netheos.com/#videomotion.

Expertise et savoir-faire

Nous nous distinguons en premier lieu par notre savoir faire en IA, nos technologies largement éprouvées et par le niveau d'automatisation de nos solutions. Mais c'est aussi notre orientation business qui fait la différence :

- Lutter contre la fraude sans considérer l'impact sur le business n'est plus admissible aujourd'hui. Et le ratio en ce sens de nos solutions est très bon,
- Il existe beaucoup de solutions de signature électronique mais la nôtre est spécifiquement dédiée à la vente en ligne et à l'acquisition de nouveaux prospects ce qui la rend très efficace dans ce contexte.

Marchés visés

Nos marchés principaux sont ceux de l'assurance et de la banque. Il s'agit de dématérialiser la souscription de produits du type assurance vie, mutuelle, garantie loyer impayé, assurance prêt immobilier, etc. Même si nous avons quelques déploiements avec nos partenaires en Europe, le territoire est aujourd'hui principalement la France.

ONEWEALTHPLACE

Alexandre HARKOUS – Président
01 84 25 30 40 – aharkous@onewealthplace.com

OneWealthPlace est une fintech évoluant dans le domaine de la gestion d'actifs et de fortune, créée en Août 2017. Nous proposons des solutions digitales disruptives et innovantes intégrant intelligence artificielle et blockchain afin d'accompagner les institutions financières dans leurs projets de transformation digitale.

38, Avenue de l'Opéra, 75001 Paris
www.onewealthplace.com
www.linkedin.com/company/onewealthplace

Chiffres-clés

Date de création : août 2017
Effectif en 2018 : 6
Statut juridique : SAS
Projet(s) labellisé(s) : AirFund, décembre 2018
Pays d'implantation : France

Mission et offres

Marchés cibles : à la fois BtoB et BtoBtoC.
Description du produit/service : deux offres avec AirFund, Blockchain privée à permission pour la gestion et dissémination des données pour les fonds avec un registre décentralisée ; Et AirWealth, une solution 100% modulaire, couvrant toute la chaîne de valeur pour la gestion de fortune, gestion sous-mandat et gestion conseillée.

Expertise et savoir-faire

Un board exécutif et un comité consultatif disposant d'une très grande expérience dans les métiers de la banque privée et de l'asset management. Un savoir-faire reconnu des équipes OneWealthPlace dans la conduite et l'implémentation de projets complexes globaux.

Marchés visés

Les typologies de clients concernés sont les banques privées, les sociétés de gestion disposant d'une activité de gestion sous mandat/gestion conseillée, les Conseillers en Gestion de Patrimoine, les Family Office ainsi que les Asset et Fund Managers. Les zones géographiques ciblées, dans un premier temps, sont la France, la zone Benelux et la Suisse.

OZE ENERGIES

Gilles NOZIÈRE – Président
09 61 68 40 08 – gilles.noziere@oze-energies.com

Optimisation du confort et économies d'énergies sans travaux dans les immeubles tertiaires et résidentiels avec une solution IA+IoT en utilisation réelle.

59, avenue de Paris, 94300 Vincennes
www.oze-energies.com
fr.linkedin.com/company/oze-energies

Chiffres-clés

Date de création : 2006
Effectif en 2018 : 15
Statut juridique : SARL
Projet(s) labellisé(s) : Conduite anticipée des équipements de génie climatique des bâtiments tertiaires en fonction des conditions climatiques en vue d'optimisation sans travaux des consommations et du confort des occupants avec une solution à base d'Iot et d'IA.
Pays d'implantation : France et Europe

Mission et offres

Oze-Energies développe et commercialise une solution originale reposant sur l'IA et les objets connectés, Optimzen®, qui booste les performances énergétiques et le confort des immeubles tertiaires ou résidentiels collectifs, sans travaux. Déployée rapidement, avec un temps de retour sur investissement court, la solution permet d'améliorer sensiblement le confort (ressenti et mesuré) tout en réalisant 25% d'économies d'énergie, sans travaux, dans un bâtiment ancien ou neuf, sous tout climat et dans tout environnement règlementaire. Elle valorise un actif immobilier en le rendant plus « smart », traçable économe et conforable, favorise le bien-être de ses occupants et réduit l'empreinte carbone d'un bâtiment. Optimzen® équipe actuellement plus de 3 millions de m^2.

Expertise et savoir-faire

- Optimisation simultanée du confort et de l'énergie sans travaux sur les immeubles existants;
- Traçabilité et optimisation ;
- Smart Building ;
- Gestion fine et continue des performances d'un immeuble (énergie et confort) en condition d'utilisation réelle, avec ou sans travaux d'amélioration;
- Relevé et de traitement de données reposant sur des algorithmes et les objets connectés (IoT);
- Ingénierie en efficacité énergétique.

PAYLEAD

Charles DE GASTINES – CEO
06 80 16 27 82 - c.degastines@paylead.fr

PayLead révolutionne la connaissance clients grâce à l'analyse de la donnée de transaction bancaire.

55, rue La Boétie, 75008 Paris
www.paylead.fr
www.twitter.com/pay_lead

Chiffres-clés

Date de création : 27 juillet 2016
Effectif en 2018 : 10
Statut juridique : SAS
Projet(s) labellisé(s) : ALO® (Account-Linked Offers)
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B.
Description du produit/service : Grâce à son expertise en Intelligence Artificielle, PayLead analyse les flux de paiement et offre des clés de connaissance clients incomparables aux institutions financières et aux commerçants, tout en respectant une politique de « privacy by design ».

Expertise et savoir-faire

PayLead est une Fintech spécialisée dans la connaissance clients. La fintech a pour ambition de mettre la puissance de cette donnée engageante, indépendante du canal d'achat et hautement prédictive au service des banques & des acteurs du retail.

Marchés visés

Banques (traditionnelles, en ligne, néo-banques), assurances, retail.

Solutions/produits innovants

PayLead permet aux banques de devenir des prescripteurs inspirants en offrant à leurs clients des avantages pertinents, différenciants et innovants dont la valeur perçue est évidente pour le consommateur, au travers d'offres commerciales 100 % personnalisées* selon leurs comportements et habitudes d'achats. En parallèle, PayLead permet aux commerçants de s'appuyer sur une segmentation puissante et leur offre ainsi un ciblage plus intelligent et plus performant afin qu'ils puissent adresser efficacement des audiences stratégiques par des offres sur-mesure.

*Des offres de cashback conçues par les marchands partenaires et directement créditées sur les comptes bancaires des clients des banques partenaires touchés par les offres.

+SIMPLE.FR

Anthony JOUANNAU – Directeur Général
06 03 09 21 90 – ajouannau@plussimpe.com

Courtier en ligne pour les TPE/PME.

2, rue Grignan, 13001 Marseille
www.plussimple.fr/#/home
www.linkedin.com/company/-simple-fr

Chiffres-clés

Date de création : avril 2015
Effectif en 2018 : 38
Statut juridique : SAS
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B (TPE/PME).
Description du produit/service : fondé en 2015, +Simple.fr est un courtier en assurance numérique pour les professionnels indépendants et les TPE, à savoir les entreprises ayant moins de vingt salariés. Elle est implantée en France à Paris (siège social), Nancy et Marseille.

Expertise et savoir-faire

La start-up a ainsi conçu une plateforme de souscription et de gestion des assurances qui propose un parcours simplifié 100 % digital et des solutions dédiées par métier. Pour supprimer toutes les lourdeurs administratives et gagner en transparence, +Simple a développé un robot-courtier qui analyse les besoins du client pour lui fournir une offre adaptée à son activité professionnelle. Il est capable aujourd'hui d'analyser environ cinq cents métiers de manière autonome.

Marchés visés

TPE françaises.

Solutions/produits innovants

De plus pour garantir aux entreprises une offre qui correspond à leurs attentes, la société a noué des partenariats avec des assureurs, des courtiers, des banques, des mutuelles ou encore des institutions de prévoyance qui distribuent leurs offres directement via la plateforme de +Simple. À ce jour, la start-up a signé une quinzaine de partenariats.

QARD

Azzeddine Chaibrassou - CEO
+33 6 16 50 83 85 - ac@qardfinance.com

47, rue Marcel Dassault, Boulogne Billancourt
www.qardfinance.com
www.linkedin.com/company/qardfinance

Chiffres-clés

Date de création : 1er février 2018
Effectif en 2018 : 4
Statut juridique : SAS
Projet(s) labellisé(s) : oui
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B, TPE e-commerçantes.
Description du produit/service : financement des TPE via des contrats de dette à court terme pour les besoins en fond de roulement. La prise de décision et la mesure de risque sont effectuées de façon instantanée et basée sur des données financières conventionnelles autant que non conventionnelles telles que des ratios sur la performance des ventes, l'efficacité opérations ou la satisfaction des clients.

Expertise et savoir-faire

- Prise de décision via un modèle de risque ;
- Gestion et exploitation de données massives;
- Deep learning et reinforcement learning pour l'entrainement du modèle.

Marchés visés

Qard vise le marché des TPE et en particulier des TPE e-commerçantes avec un chiffre d'affaires annuel pouvant aller jusqu'à 5 millions.

Solutions/produits innovants

Qard propose des prêts à court terme sans garantie ni caution pour tous les besoins en trésorerie des TPE e-commerçantes. Grace à sa technologie et son savoir-faire Qard peut offrir aux TPE un prêt sur mesure et en moins de 24 heures, prenant en compte de réels indicateurs de performance de l'activité commerciale et non de simple ratio financiers et comptables.

QUANTCUBE TECHNOLOGY

Thanh-Long HUYNH - CEO
01 43 58 48 46 - tlh@q3-technology.com

FinTech spécialisée dans l'analyse en temps réel de données Big Data pour la finance et l'économie.

19, Boulevard Poissonnière, 75002 Paris
www.q3-technology.com

Chiffres-clés

Date de création : juillet 2013
Effectif en 2018 : 25
Statut juridique : SAS
Projet(s) labellisé(s) : FUI 22
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B, institutions financières.
Description du produit/service : le produit phare de QuantCube Technology est la Global Macro Smart Data, c'est-à-dire la croissance économique en temps réel, l'inflation en temps réel, le marché de l'emploi en temps réel. Cette solution permet d'anticiper les changements de tendance et de se positionner sur les marchés financiers. Cette solution est principalement utilisée pour les investissements à moyen terme, pour la prévision des cycles conjoncturels, et pour les investissements à long terme, tels que l'immobilier ou l'infrastructure. La solution est distribuée sous forme SaaS.

Expertise et savoir-faire

QuantCube Technology est constituée d'une équipe de 26 personnes, la plupart d'entre elles ayant des doubles ou triples formations en mathématiques appliquées, intelligence artificielle, statistiques, mais également en économie et en finance. Au sein de cette équipe, il existe plusieurs sous-équipes spécialisées en IA, notamment pour des techniques de NLP en natif pour l'analyse de texte en différentes langues (anglais, français, chinois, arabe, russe…), de deep learning pour la détection, classification et segmentation d'images satellites, et de théorie des graphes pour analyser les liens entre les personnes.

Marchés visés

Les marchés visés sont les grandes places financières : New York, Londres, Paris, Tokyo et Dubaï. Les institutions visées sont les institutions financières tels que les sociétés de gestion, les hedge funds et aussi les institutions publiques – banques centrales ou ministères.

Solutions/produits innovants

L'analyse des données alternatives a des applications orientées investissement sur différents horizons : court terme, moyen-terme et long-terme. Les solutions analytiques permettent par exemple aux sociétés de gestion la mise en place de stratégies d'investissement, mais aussi la création d'indicateurs macroéconomiques en temps réel (estimation de la croissance économique ou de l'inflation par exemple), d'indices de sentiment en temps réel avec l'analyse de l'e-réputation de sociétés, marques ou individus, ou encore le monitoring des principaux champs agricoles à l'échelle mondiale. Pionnière dans cette industrie d'avenir de l'analyse macroéconomique et financière basée sur la combinaison d'Intelligence Artificielle et de données massives hétérogènes, la startup s'est imposée ces dernières années comme le leader du domaine en Europe et ambitionne d'atteindre le même statut à l'échelon mondial.

QUANTICS TECHNOLOGIES

Pascal FOURNIÉ-TAILLANT – Président
+33 6 07 24 86 62
pascal.fournie-taillant@quantics-technologies.com

Depuis 2010, Quantics Technologies développe des solutions pour la gestion quantitative, le trading algorithmique et le Machine Learning.

42, avenue Montaigne, 75008 Paris
www.quantics-technologies.com
www.linkedin.com/company/quantics-technologies

Chiffres-clés

Date de création : 2010
Effectif en 2018 : 5
CA en 2018 : 420 M€
Statut juridique : SAS
Projet(s) labellisé(s) : Qualta
Pays d'implantation : France

Mission et offres

Marchés cibles : clientèle institutionnelle (Asset management, BFI).
Description du produit/service : diffusion via un service Web de signaux d'achat/vente d'instruments financiers basés sur la technologie propriétaire de Machine Learning/IA QUALTA et développement de stratégies d'investissement quantitatives exploitant ces signaux.

Expertise et savoir-faire

Depuis 2010, Quantics Technologies développe des solutions pour la gestion quantitative, le trading algorithmique et le Machine Learning. En 2016, la société a livré uantify, la 1ère version de sa plateforme Web de gestion de portefeuille entièrement automatique. En 2018, elle obtient un 1er brevet significatif en Machine Learning en rendant possible l'industrialisation à grande échelle de la « Détection de Signaux Faibles » qui est au cœur de la solution Qualta, et qui bénéficie d'applications concrètes pour la prédiction des marchés financiers. Deux offres complémentaires destinées à une clientèle institutionnelle (banques, assurances, gérants d'actifs). Quantics Technologies a bénéficié du statut JEI et est éligible au CIR, éligibilité confirmée par une expertise du Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation menée en 2016. Qualta est notre technologie brevetée de Machine Learning (BOPI N°18-46 du 16/11/18), software + hardware, permettant une analyse prédictive de données fondée sur la recherche de règles d'association, dite « Détection de Signaux Faibles ». Il est le fruit de la complémentarité d'expertises de haut niveau en mathématiques appliquées, développement logiciel et électronique. L'idée fondamentale de Qualta est l'accélération de la compréhension de problématiques complexes, rendue disponible à l'industrie via l'optimisation de calculs massifs. Son originalité tient dans son approche agnostique de l'analyse prédictive de données, ainsi que dans une innovation technologique puissante augmentant les vitesses de calcul tout en réduisant le coût environnemental et logistique lié à l'utilisation de fermes de calcul.

Marchés visés

Asset management, BFI.

REAL QUALITY RATING

Olivier MÈGE – Président
07 87 11 84 34 – olivier.mege@realqualityrating.eu

Leader mondial de la mesure de qualité des actifs immobiliers.

49, rue de Ponthieu, 75008 Paris
www.realqualityrating.com

Chiffres-clés

Date de création : octobre 2016
Effectif en 2018 : 6
CA en 2018 : 53 000 euros
Statut juridique : SAS
Projet(s) labellisé(s) : novembre 2017
Pays d'implantation : France

Mission et offres

Marchés cibles : investisseurs et propriétaires occupants.
Description du produit/service : RQR est une start up spécialisée dans la mesure de qualité des actifs immobiliers. Ses services sont destinés à améliorer la précision et l'efficacité des prises de décisions locatives ou d'investissement. Sa diffusion permettra à terme l'avènement d'un marché de l'investissement immobilier plus juste, plus efficace et ainsi une meilleure allocation de l'épargne publique. Son approche est fondée sur l'intelligence collective augmentée (ICA), rencontre du collectif des acteurs économiques, des sciences cognitives et de l'intelligence artificielle. RQR développe ses méthodologies en collaboration avec des chercheurs de Dauphine et du CNRS. Elle a été labellisée Finance Innovation par le Ministère des Finances pour le caractère innovant de son service. Elle est financièrement soutenue par la BPI et par la Communauté européenne.

Expertise et savoir-faire

Systèmes experts permettant l'évaluation de la qualité, de la création de valeur, et de l'obsolescence.

Marchés visés

Immobilier commercial dans les pays développés.

Solutions/produits innovants

Service d'aide à la décision d'investissement ou locative dans les domaines de l'investissement, de l'asset management, et du fund management. Plateforme d'évaluation collaborative permettant de réaliser le scoring des immeubles an amont d'une acquisition et de benchmarker le score obtenu en interne avec l'évaluation du marché, générée par l'algorithme de notation.

SECURE-IC

Hassan TRIQUI – CEO
+33 6 71 45 47 46 – hassan.triqui@secure-ic.com

Secure-IC : The Security Science Company.

ZAC des Champs Blancs, 15, rue Claude Chappe, Bât. B, 35510 Cesson-Sévigné, France
www.secure-ic.com/
www.linkedin.com/company/secure-ic/
www.twitter.com/SecureIC

Chiffres-clés

Date de création : 2010
Effectif en 2018 : 45
Pays d'implantation : France (Rennes, Paris), Singapour, Japon

Mission et offres

Marchés cibles : B2B & B2C.
Description du produit/service : Our mission is to partner with our Clients throughout and beyond the IC design process to provide best-of-breed security expertise, solutions, and technologies, for embedded systems and connected objects: Protect (a rich IP portfolio), Evaluate (tools to evaluate the security of design before & after Silicon), Service & Certify (support from experts along the project to reach the security goals).

Expertise et savoir-faire

Secure-IC has developed security solutions for any electronic embedded system and connected object to protect them against attacks and guarantee at each stage of the design process that the security level reached is optimal. In order to offer its clients best-of-breed technologies and above state-of-the-art protections, Secure-IC, The Security Science Company, is highly committed in its research community to analyze upcoming threats, explore innovative solutions, and support the work of standardization bodies. Our research activities benefit our partners through trainings or closer collaborations on specific topics.

Marchés visés

Banking & Payment, Identity, IoT & Mobility, Media & Entertainment, Government, Trusted Computing, Automotive.

Solutions/produits innovants

Secure-IC proposes to its clients and partners a full range of products and services. Our Protect offer contains a complete set of hardware and software technologies to include into your design in order to make them attack-resilient. The Evaluate offer is a product line dedicated to the security assessment tools. Our Service offer completes these products to provide the necessary help and knowledge for an optimal use.

SERENDPTECH

Émilie THÉBAULT – CEO
06 20 45 16 25 – emilie.thebault@serendptech.com

SerendpTech est une start-up hybride de la RegTech et de la cybersécurité qui sécurise et simplifie le KYC en vérifiant les identités de manière instantanée et mobile.

1, avenue du champ de Mars, 45000 Orléans
www.serendpTech.com

Chiffres-clés

Date de création : juillet 2016
Effectif en 2018 : 11
Statut juridique : SAS
Projet(s) labellisé(s) : Sync'ID
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B2C.
Description du produit/service : applications mobiles qui permettent de fluidifier l'entrée en relation (onboarding) des clients dans le monde physique et dans le full digital. Simplification et sécurisation des obligations de KWC lors de la création de compte en ligne. Facilitation de l'identification et de l'authentification des transactions.

Expertise et savoir-faire

L'équipe est constituée de 3 anciens des ministères de l'intérieur et de la défense, responsable et représentant de la France au sein de la commission européenne et à l'ONU de la sécurité des titres d'identité et de la lutte contre la fraude. Spécialistes de la biométrie et de la lectures des puces et de la cryptologie associée.

Marchés visés

Le marché bancaire et assurantiel, les fintechs, et le retail.

Solutions/produits innovants

Ces applications sont les seules actuellement à proposer un KYC instantané pour plus de 1 milliard de titres dans le monde et à le rendre fluide et sécurisé grâce à des technologie de crypto et lecture des puces des passeports notamment. RGPD compliance, la solution permets de protéger les données des clients.

SHIFT TECHNOLOGY

Jérémy JAWISH – CEO
06 70 15 19 12 - jeremy.jawish@shift-technology.com

Entreprise offrant une solution en mode Saas pour la détection de fraude à l'assurance et l'automatisation de la gestion des sinistres.

14, Rue Gerty Archimède, 75012 Paris
www.shift-technology.com
www.linkedin.com/company/shift-technology

Chiffres-clés

Date de création : 2013
Effectif en 2018 : 80
CA en 2018 : 3 M€
Statut juridique : SAS
Pays d'implantation : France, Singapour, Japon, États-Unis, Espagne, Suisse, Royaume-Uni, Hong Kong

Mission et offres

Marchés cibles : B2B.
Description du produit/service : Nous proposons des solutions aux compagnies d'assurance pour la détection de fraude à l'assurance et l'automatisation de la gestion des sinistres.

Expertise et savoir-faire

Notre expertise se concentre dans l'IA, le Big Data et le Machine Learning ainsi que dans l'expérience métier des équipes sinistres et fraudes de l'assureur.

Marchés visés

Nous visons les compagnies d'assurance du monde entier pour tout type de ligne de business (Auto, Habitation, Santé…).

Solutions/produits innovants

Nous proposons une solution de détection de fraude aux assurances, basée sur l'intelligence artificielle, baptisée FORCE™. FORCE™ est une plate-forme de prise de décision spécialement conçue pour les gestionnaires antifraude qui permet d'accroître la capacité à détecter des comportements frauduleux (fraude opportuniste et crime organisé). Nous avons également une solution d'automatisation de la gestion des sinistres pour les compagnies d'assurance baptisée LUKE™.

SIS

Rémi DEMONT – Président
06 50 28 85 81 – remi.demont@sisnet.fr

SiS développe My SiS-id, première communauté de direction financière de lutte contre la fraude aux virements.

20, Bld E Deruelle
www.sis-id.com

Chiffres-clés

Date de création : 2016
Effectif en 2018 : 10
Statut juridique : SAS
Projet(s) labellisé(s) : oui
Pays d'implantation : France, UK

Mission et offres

Marchés cibles : B2B.
Description du produit/service : SiS développe My SiS-id, première communauté de direction financière de lutter contre la fraude aux virements.

Expertise et savoir-faire

L'innovation tant technologique qu'organisationnelle repose sur le partage très large d'informations assortie d'une exploitation strictement confidentielle et anonymisée. La plateforme, tiers de confiance, sécurise les données bancaires et des paiements par :

- La création d'un référentiel de coordonnées de paiement hautement sécurisé et infalsifiable reposant sur l'utilisation de la technologie blockchain (partenariat avec IBM);
- La mutualisation anonymisée des données de paiement pour qualifier les nouvelles demandes avant leur émission et d'ainsi prévenir les tentatives de fraudes (partenariat avec le LIRIS/CNRS).

Marchés visés

B2B.

Solutions/produits innovants

- Un référentiel des données de paiement sous la responsabilité des destinataires de paiement, authentifiées et sécurisées une fois pour tous les membres du réseau;
- Un scoring des fichiers de paiement …avant leur départ en banque;
- Une police d'assurance couvrant la fraude à d'identité bancaire.

STRATUMN

Richard CAETANO – CEO
richard@stratumn.com

Stratumn a pour mission de restaurer la confiance dans les processus inter-entreprises.

1 bis, cité Paradis
www.Stratumn.com
www.linkedin.com/company/stratumn

Chiffres-clés

Date de création : 2015
Effectif en 2018 : 20
Statut juridique : SAS
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B assurances et banques.
Description du produit/service : notre produit TRACE est une solution de traçabilité et d'optimisation de processus complexes. TRACE combine le chiffrement, la technologie blockchain et une connectivité simplifiée via API pour permettre à plusieurs partenaires de partager un processus en temps réel. Ainsi TRACE supprime les frictions opérationnelles causées par l'absence de confiance au sein de chaînes de valeur complexes.

Expertise et savoir-faire

Stratumn a pour mission de restaurer la confiance dans les processus inter-entreprises. Notre produit TRACE combine un chiffrement de nouvelle génération, la technologie blockchain et une connectivité simplifiée via API pour permettre une traçabilité universelle des processus. Grâce à TRACE, les processus entrent dans un nouveau paradigme où la traçabilité n'est plus réservée à quelques étapes simples, par exemple la signature d'un contrat d'assurance, mais à l'ensemble d'un processus complexe multi-acteur. Nous supprimons les frictions opérationnelles au sein de chaînes de valeur complexes causées par l'absence de confiance. Là où historiquement les acteurs sont obligés de répliquer des centaines de tâches manuelles et de documents, nous créons la confiance dans un même processus, partagé en temps réel :

- plus de réconciliation a posteriori;
- automatisation en toute sécurité de processus complexes avec historique des éléments entrant dans la prise de décision;
- preuve de conformité en temps réel avec piste d'audit certifiant de la réalisation des contrôles règlementaires avec enregistrement des résultats obtenus;
- responsabilisation des acteurs avec signatures digitales et irrépudiabilité des actions.

Marchés visés

Tracabilité, optimisation de processus, conformité, KYI, KYC, KYS, banques et assurances.

Solutions/produits innovants

Avec TRACE, nos clients passent du monde d'une conformité gérée a posteriori à force de contrôles documentaires manuels et fastidieux à un monde où l'exécution même du processus apporte la preuve de sa conformité, accessible et vérifiable de manière indépendante par les auditeurs et les régulateurs. Les applications en cours de déploiement en production chez des leaders européens de la Banque et Assurance sont la gestion documentaire du processus KYC/KYI, l'automatisation de sinistre en Prévoyance, et le suivi de données financières critiques.

TACOTAX

Aldric EMIÉ - co-fondateur & CEO
06 20 34 75 77 – aldric@tacotax.com

Le coach en ligne pour les finances personnelles des particuliers.

112, avenue de Paris, 94306 Vincennes
www.tacotax.fr
www.linkedin.com/company/10292132/admin

Chiffres-clés

Date de création : 2016
Effectif en 2018 : 15
Statut juridique : SAS
Pays d'implantation : France

Mission et offres

Marchés cibles : B2C2B.
Description du produit/service : TacoTax met à disposition des particuliers tous les outils et conseils pertinents de nos experts pour les aider à optimiser leurs situations financières.

Expertise et savoir-faire

Accompagnement fiscal, accompagnement finances personnelles, machine learning.

Marchés visés

Tout le marché des finances personnelles : défiscalisation, gestion de patrimoine, crédits, assurances, etc.

Solutions/produits innovants

Nous avons développé des algorithmes de machine learning qui nous permettent d'adapter les investissements suggérés à nos utilisateurs en fonction de leur situation personnelle. Basés sur les comportements des utilisateurs sur le site (clics, temps passé, demandes de rappel téléphoniques) mais aussi sur le niveau de satisfaction des utilisateurs (via des enquêtes par email) et de nos partenaires (via des sondages mensuels), ces algorithmes sont au cours de notre ambition de rendre accessible et facile les prises de décision patrimoniales.

TESTAMENTO

Virgile DELPORTE - PDG
01 85 09 67 62 – v.delporte@testamento.fr

Plateforme de sensibilisation et d'anticipation successorale.

91, Rue du Faubourg Saint-Honoré, 75008 Paris
www.testamento.fr
www.linkedin.com/company/testamento

Chiffres-clés

Date de création : 2013
Effectif en 2018 : 10 personnes
CA en 2018 : 100 k€
Statut juridique : SAS
Projet(s) labellisé(s) : Plateforme globale d'anticipation successorale
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B2C et B2C.
Description du produit/service : Testamento propose des solutions uniques de transmission et d'optimisation de la succession, au travers de services de sensibilisation (Kit Info Succession), de solutions juridiques (testament, dernières volontés), et de protection de patrimoine.

Expertise et savoir-faire

Chez Testamento, nous pensons que toutes les étapes de la vie doivent être anticipées en toute simplicité, même les moins amusantes. C'est la raison pour laquelle nous avons décidé, avec notre équipe d'experts du droit, du marketing, de la technologie et de l'assurance, de démocratiser les sujets de succession, en les rendant simples, pratiques, et sécurisées.

Marchés visés

Le principal marché de Testamento est le B2B2C. Nous travaillons avec assureurs/banques, mutuelles, courtiers et institutions de prévoyance, qui souhaitent apporter du conseil à leurs clients, augmenter leur connaissance client pour mieux vendre et leur fournir des solutions simples pour faire face à leurs obligations réglementaires (en particulier la DDA et la Loi Eckert). Le marché français est le premier visé, mais Testamento souhaite se déployer dans tous les pays de droit latin dans les prochaines années.

Solutions/produits innovants

Testamento propose 3 grandes catégories de solutions pour le marché de la prévoyance et de la vie :

- Offre 1 : inclusion des services Testamento sur un espace Testamento.fr co-brandé ;
- Offre 2 : logiciels SaaS de gestion de clause bénéficiaire dans le parcours de souscription et en self-care pour les assurés ;
- Offre 3 : solutions d'acquisition et/ou de fidélisation en prévoyance individuelle ou collective.

THE INDEPENDANT CALCULATION AGENT (ICA)

Stéphane RIO - CEO and founder
+33 1 53 65 35 95 - stephane.rio@the-ica.com

Les calculs de risques de marchés réinventés : Pricing & Risk as a Service ou les technologies au service du Pricing & Risk.

112 avenue Kleber, 75116 Paris
www.the-ica.com
www.linkedin.com/company/the-independent-calculation-agent
www.twitter.com/IndepCalcAgent

Chiffres-clés

Date de création : 2015
Effectif en 2018 : 15
Statut juridique : SAS
Projet(s) labellisé(s) : ICA
Pays d'implantation : France, Angleterre, Japon

Mission et offres

Marchés cibles : B2B. Clients : banques, consultants, auditeurs, «buy-side» (clients des banques).
Description du produit/service : Les nouvelles réglementations sur les dérivés imposent aux banques des calculs de plus en plus complexes et une gestion de quantités énormes de données, pour lesquels les systèmes historiques ne sont plus adaptés. ICA propose une solution plus performante, agile et économique, basée sur les technologies du cloud computing et du big data, en «Software as a Service» ou en implémentation spécifique.

Expertise et savoir-faire

Pour atteindre notre objectif, nous avons utilisé les innovations des acteurs du web et des nouvelles technologies (big data, cloud computing, IA…) pour les mettre au service des calculs quantitatifs sur les produits dérivés qui permettent d'obtenir des prix et mesures de risques dans les domaines les plus complexes de la finance de marché (comme xVA, FRTB…). Le résultat est un système qui nous permet de faire ces calculs plus efficacement que les systèmes traditionnels : à la fois en termes de temps de calculs et de coûts. Cette expertise est disponible à travers notre offre de Software as a Service ou d'implémentations spécifiques à partir des modèles des banques.

Marchés visés

- Pour les utilisateurs de produits dérivés : externalisation de la complexité des calculs liés aux nouvelles réglementations ;
- Avec nos technologies du cloud computing, big data et AI appliquées à vos librairies financières, réduisez vos temps et coûts de calculs actuels à une fraction.

Solutions/produits innovants

- Pricing & Risk as a Service : externalisation de toute la chaîne de calculs depuis les modèles financiers jusqu'à la puissance de calculs. L'utilisateur garde la main sur les inputs et calibrations, mais ne se soucie pas de l'implémentation, la maintenance, la puissance de calculs nécessaires ;
- UI et BI, focus 100% business : depuis le report réglementaire ou comptable jusqu'à la capacité de gérer des scénarios «what-if» en temps réel pour optimiser un portefeuille existant, pour optimiser l'exécution d'une nouvelle transaction, pour évaluer le prix donné par une contrepartie («reverse engineering») ;
- Base de données big data capable de manipuler («slide and dice») en quasi-temps réel des centaines de milliards de données sur des ordinateurs classiques (y compris un laptop!) ;
- Utilisation innovante du cloud en séparant les calculs confidentiels (gérés localement ou dans un cloud privé) de ceux qui ne le sont pas (utilisation de l'élasticité du cloud public). Module d'anonymisation pour enlever TOUS les éléments confidentiels.

TIIME

Maxime DIGUE – Co-Fondateur
06 11 21 68 77 – maxime.digue@tiime.fr

Tiime est une suite d'application gratuite pour entreprendre simplement.

15 – 17, rue Auber, 75 009 Paris
www.tiime.fr
www.linkedin.com/company/tiime-app

Chiffres-clés

Date de création : 2016
Effectif en 2018 : 30
CA en 2018 : 1 M€
Statut juridique : SAS
Projet(s) labellisé(s) : oui
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B.
Description du produit/service : Tiime est une suite d'application gratuite répondant à différents besoins des entrepreneurs : créer en ligne son entreprise, facturer facilement, collecter l'ensemble de ses reçus et matcher automatiquement relevés bancaires et factures. Notre mission : simplifier la vie des petites entreprises et leur faire gagner du temps. À ce jour, Tiime a aidé plus de 15 000 entrepreneurs en France.

Expertise et savoir-faire

Utilisation de l'Intelligence Artificielle dans la catégorisation des données bancaires à des fins d'exploitations comptables ou de gestions.

Marchés visés

Tiime s'adresse aux entrepreneurs français, mais l'ouverture à l'international n'est pas exclue.

Solutions/produits innovants

Tiime offre à ses utilisateurs :
- une carte Mastercard et un IBAN français ;
- la création d'entreprise (SARL, SAS) en ligne et gratuite ;
- une application de devis et factures simples ;
- le rapprochement automatique des factures et des relevés bancaires ;
- la collecte et le classement des justificatifs.

TREEZOR

Éric LASSUS – Directeur Général
+33 1 84 19 29 81
eric.lassus@treezor.com – sales@treezor.com

Treezor est une plateforme de Bank-as-a-Service qui propose aux entreprises des services de paiement en marque blanche par API.

94, rue de Villiers, 92300 Levallois-Perret
www.treezor.com
www.linkedin.com/company/treezor/
www.twitter.com/TreezorBanking

Chiffres-clés

Date de création : 2015
Effectif en 2018 : 35
CA en 2018 : 1 100 000 €
Statut juridique : SAS
Projet(s) labellisé(s) : oui
Pays d'implantation : France et Espace économique Européen

Mission et offres

Marchés cibles : B2B2B & B2B2C.
Description du produit/service : Treezor est un EME agréé par l'ACPR, membre Mastercard et SEPA. La plateforme de Bank-as-as-Service, offre aux sociétés des solutions de paiement en marque blanche par API. La plateforme permet de gérer l'ensemble des moyens paiements : cartes, virement, prélèvement… Une solution de paiement complète qui répond aux besoins des projets de néobanque, marketplace, cagnotte, programme carte.

Expertise et savoir-faire

Paiement, Monnaie électronique, Tokenisation, Gestion de la fraude, Digitalisation.

Marchés visés

Treezor s'adresse à toutes les entreprises européennes qui souhaitent se doter de solutions de paiement innovantes et digitalisées pour simplifier les usages. Treezor vise essentiellement les Fintech, Banque, Assureur, Marketplace, Plateformes collaboratives et Retailer/E-commerçant.

Solutions/produits innovants

API, Core-banking, Wallet, IBAN, KYC, Acquisition en ligne par Cartes bancaires, Virement SEPA, Prélèvement SEPA, Émission de carte physique et virtuelle, BIN Sponsorship, Apple Pay, Samsung Pay…

UNIRIS

Sébastien DUPONT-RAOSETA – CEO
06 12 13 55 51 – seb@uniris.io

Votre carte bancaire c'est vous ! Uniris et ses 11 brevets redéfinissent les standards en termes d'inclusion, de sécurité, de respect des données privées, et d'argent programmable (Biométrie, Blockchain, AI).

86, rue de Paris, 91400 Orsay
www.uniris.io
www.linkedin.com/company/uniris

Chiffres-clés

Date de création : février 2017
Effectif en 2018 : 3
Statut juridique : SAS
Pays d'implantation : France, Inde

Mission et offres

Marchés cibles : B2C (ICO) & B2B.
Description du produit/service : Le premier produit est la cryptomonnaie « UCO » pivot d'une Blockchain de nouvelle génération, qui, contrairement à ses ainées permet :

- une réduction vertigineuse de la consommation d'énergie (20 millions de fois moins);
- une validation instantanée & un stockage illimité des transactions ;
- des fonctionnalités « smart-contract » inédites (facilité de programmation, mise à jour, déclenchement automatisé et interactions avec le monde réel).

Expertise et savoir-faire

AI, blockchain, biométrie, cyber sécurité, brevets.

Marchés visés

Le premier marché visé est de celui de la Blockchain (10 milliards d'euros d'ici à 2022) notamment sur 2 axes prioritaires que sont la cyber sécurité (Défense, ONU) et les Services financiers. La branche Services Financiers démarrera Q1 2019 par le lancement de l'ICO avant de s'étendre, à moyen terme, sur des services tels qu'une MarketPlace et bien sûr les paiements par un simple effleurement de doigt ne nécessitant plus aucun équipement personnel.

Solutions/produits innovants

La solution Uniris repose sur 2 innovations technologiques majeures et brevetées (11 brevets FR/US/Chine/Inde). Le premier est constitué d'un dispositif biométrique de nouvelle génération permettant d'authentifier n'importe quelle personne à partir de son réseau veineux des doigts, et ce, de façon aussi sécurisée qu'une carte bancaire, mais sans nécessiter le moindre dispositif, ni de communiquer quelque donnée personnelle que ce soit. Le second est une Blockchain de nouvelle génération, qui, contrairement à ses ainées (Bitcoin, Ethereum …) a résolu les épineux problèmes de la consommation d'énergie, du temps de validation d'une transaction et de la capacité de stockage jusque-là extrêmement limitée, en outre, cette Blockchain dispose de smart-contracts (ou actions programmées décentralisées) beaucoup plus simples et évolués que les standards actuels (p.ex Ethereum/Solidity).

UNKLE

Matthieu LUNEAU - Co-fondateur & CEO
06 27 35 59 14 - matthieu@unkle.fr

Unkle est le nouveau garant souscrit simplement et automatiquement en ligne par un locataire pour booster son dossier et rassurer son propriétaire qui est couvert gratuitement contre les loyers impayés.

112, Avenue de Paris, 94300 Vincennes
www.unkle.fr/
www.linkedin.com/company/unkle-tech

Chiffres-clés

Date de création : 26 juin 2018
Statut juridique : SAS
Projet(s) labellisé(s) : oui
Pays d'implantation : France

Mission et offres

La mission de Unkle est de fluidifier l'accès au logement pour tous les locataires qui ne remplissent pas les conditions de marché pour louer rapidement et facilement un appartement. Aujourd'hui, les conditions de marché sont les suivantes :

- Avoir une situation stable (s'apparentant quasi-systématiquement à un CDI);
- Avoir un garant solide;
- Avoir un historique en France;
- Gagner au moins trois fois le loyer.

Faute de remplir toutes ces conditions, 6 millions de locataires ont (ou auront un jour) du mal à se loger rapidement et facilement en France. Unkle propose aux locataires de devenir leur garant afin de (i) booster leur dossier de location, de (ii) faciliter leurs démarches de recherche immobilière et de (iii) convaincre plus facilement un propriétaire de leur laisser louer son appartement. Avec Unkle, le propriétaire est assuré de continuer à toucher ses loyers tous les mois même si le locataire arrête de le payer. Le locataire paie mensuellement 3,5% du montant du loyer et Unkle touche une commission chaque mois. La garantie Unkle apportée par un locataire pour son propriétaire :

- Une garantie gratuite pour le propriétaire;
- Un remboursement jusqu'à 96 000€de loyers impayés;
- Une couverture de 24 mois d'impayés sur toute la durée du bail;
- Pas de franchise ni délai de carence.

Le locataire se connecte sur www.unkle.fr, rempli un questionnaire, upload ses pièces justificatives et Unkle lui donne une réponse.

Expertise et savoir-faire

Unkle est une Fintech à classer plutôt dans la catégorie Insurtech à la croisée des chemins entre l'assurance et l'immobilier. Unkle est un intermédiaire en assurance et en banques et en services de paiement. Unkle est agréée par l'ORIAS (l'organisme pour le Registre des Intermédiaires en Assurance, Banque et Finance) sous le numéro 18005151. Unkle a développé une une plateforme tech 100% en ligne, une garantie ainsi qu'un scoring innovant et est adossé à un porteur de risque.

Marchés visés

Les clients d'Unkle sont les freelances, les indépendants, professions libérales, jeunes actifs, expatriés, étudiants, colocataires, retraités. Tous ces futurs clients ont pour point commun de ne pas réunir l'ensemble des conditions de marché pour louer facilement un appartement.

UTOCAT

Clément FRANCOMME - CEO
06 37 58 42 80 - clement@utocat.com

Éditeur de logiciel blockchain pour le domaine bancaire et assurantiel.

Euratechnologies Doge B, 4, avenue des Saules, 59160 Lille
www.utocat.com
www.linkedin.com/company/utocat

Chiffres-clés

Date de création : 10 novembre 2014
Effectif en 2018 : 12
CA en 2018 : 412k€
Statut juridique : SAS
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B.
Description du produit/service : Catalizr est un logiciel de gestion numérique des titres non cotés. La solution traite, de la souscription à l'archivage en passant par la signature, les documents nécessaires à un investissement en non coté sous un format numérique. Elle centralise les échanges entre acteurs et propose une gestion simplifiée des OST et des revalorisations.

Expertise et savoir-faire

Nous concevons des solutions permettant d'assurer la transition numérique de nos clients. Nous sommes spécialisés dans la technologie blockchain depuis 4 ans et nous amenons la technologie blockchain dans des usages métiers. Nous assurons également une sécurité numérique maximale dans l'ensemble de nos produits grâce à un usage contrôlé de la technologie.

Marchés visés

Nous évoluons sur le marché bancaire et financier et nous avons, pour principal client, l'ensemble des grandes banques françaises et européennes, les conservateurs ainsi que les entités juridiques traitant les dossiers d'investissements.

Solutions/produits innovants

Catalizr permet de faciliter l'accès à l'investissement dans l'économie réelle. Fini les procédures manuelles et les dossiers administratifs à rallonge, nous proposons de centraliser l'ensemble des processus afin de proposer à l'investisseur une expérience unique d'investissement. Nous garantissons également l'accès à l'ensemble des produits financiers permettant d'optimiser vos investissements tels que le PEA. Nous utilisons la technologie blockchain comme une surcouche sécuritaire supplémentaire en indexant les preuves numériques afin de certifier les procédures.

VARIABL

Simon POIROT – Directeur Opérations, Cofondateur
06 38 68 90 57 – simon@variabl.io

Plateforme de création et d'échange de produits dérivés en cyberactifs programmés et exécutés sur la Blockchain Ethereum pour plus de transparence, sécurité et stabilité. Le projet VariabL est supporté par la société ConsenSys France.

WeWork, 64 rue des Archives, 75003 Paris
www.variabl.io
Twitter @VariabLio

Chiffres-clés

Date de création : 2016
Effectif en 2018 : 8
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B, B2C.
Description du produit/service : VariabL est une plateforme d'échange construite sur la blockchain publique Ethereum, permettant d'entrer dans des contrats dérivés en crypto-actifs. La plateforme est dite « semi-décentralisée » : certaines fonctionnalités sont exécutées directement sur la Blockchain (ie. décentralisées) et d'autres sont gérées en interne (ie. centralisées). Il s'agit du premier marché d'instruments dérivés sur une blockchain publique bénéficiant de toutes ses caractéristiques et avantages, et notamment :

- Un haut niveau de sécurité des transactions, qui sont validées, gérées et exécutées par le biais d'un réseau informatique décentralisé sans nécessité d'intervention d'un intermédiaire ;
- Des transactions effectuées quasi instantanément ;
- Des frais de transaction très faibles ;
- Des « fonds » qui n'ont pas besoin d'être consignés par un intermédiaire, puisque les actifs en jeu sont conservés dans les « smart-contracts » à partir du moment où un ordre est placé, et ce jusqu'à la liquidation. En effet, ce sont les « smart-contracts » et non VariabL qui sont les consignataires des fonds des utilisateurs : seul leur code peut décider de l'issue du contrat et de la répartition des fonds qu'il contient. Ces décisions sont conditionnées par avance et ces conditions sont immuables.
- Pas de possibilité de détournement des fonds ;
- Une compensation et un règlement effectués automatiquement : la plateforme est codée de manière à ce que la compensation et le règlement des transactions s'effectuent automatiquement d'une manière quasi décentralisée selon les conditions prédéfinies dans le code, et qui ne peuvent être modifiées, même par VariabL ;
- Un enregistrement en temps réel de l'historique des transactions dans un registre partagé qui ne peut être falsifié.

Expertise et savoir-faire

Expertise technique :

- développement logiciel et serveurs ;
- blockchain Ethereum et smart-contracts (infrastructure, fonctionnement, évolutions) ;
- technologie « state channels » ;

Expertise financière.

Marchés visés

- À court terme, le marché existant du trading d'actifs numérique (50 millions d'utilisateurs estimés) ;
- À moyen terme, le marché des applications décentralisées – autrement dit, les entreprises développement des solutions utilisant la technologie blockchain. Il s'agit d'un marché très jeune, à la croissance exponentielle ;
- À long terme, les institutions financières traditionnelles souhaitant s'exposer à risque de marché ou couvrir un risque financier.

VIALINK

Philippe SANCHIS – CEO & Directeur Général
philippe.sanchis@vialink.fr

23-25, rue Daviel, 75013 Paris
www.vialink-kyc.com
www.linkedin.com/company/vialink-france

Chiffres-clés

Date de création : 1999
Effectif en 2018 : 40
Projet(s) labellisé(s) : à venir
Pays d'implantation : France, Europe prochainement

Mission et offres

Marchés cibles : B2B, B2B2C.
Description du produit/service : Vialink propose une plateforme en mode API, permettant la reconnaissance et la lecture de documents, mais aussi le contrôle automatisé de dossiers (KYC) en passant par la contractualisation digitale (SIGN). Vérification automatique des documents : basé sur des algorithmes Machine & Deep Learning et sur la connexion à de nombreuses bases de données externes (Infogreffe, PEP, OFAC, BODACC, …), Vialink assure de manière systématique les contrôles sur chaque document de manière unitaire comme croisée. Ces contrôles sont valables tant pour la personne physique que morale, et permettent d'accélérer drastiquement les délais d'entrée en relation. Notre solution de « face matching » (reconnaissance faciale) permet d'ajouter un niveau de contrôle supplémentaire sur les parcours à distance tout en fluidifiant les parcours de souscription. Simplification et sécurisation contractuelle : notre plateforme propose une large gamme de solutions de signatures : de la signature simple à avancée (respectant les normes eIDAS en vigueur), pour les personnes physiques ou morales. KYC + SIGN, une plateforme unique pour répondre à l'ensemble des problématiques de conformité et de parcours clients.

- Assurer un parcours clients sans couture, 100% digitalisé de l'entrée en relation à la signature du dossier;
- Accélérer l'acquisition de nouveaux clients avec en moyenne une hausse de 40% du taux de conversion ;
- Réduire les coûts de traitement back-office et conformité.

Le GROS plus de la solution Vialink est qu'elle est totalement adaptable aux besoins métiers grâce à ses possibilités de paramétrage. Par exemple : l'authentification des éléments d'une carte identité sera décisive pour l'ouverture d'un compte bancaire, alors que l'authentification et la lecture d'un bulletin de salaire le sera pour une agence immobilière dans la location d'un appartement. La plateforme permet de gérer simplement, rapidement et de manière conforme la relation client, de la prise de contact à la signature de l'acte.

WIZI–TYRELL SAS

Julien LOZANO - CEO
06 70 99 75 68 - julien@wizi.eu

WIZI permet de simplifier et d'optimiser le process de gestion locative entre particuliers.

55, rue Alphonse Pluchet, 92220 Bagneux
www.wizi.io

Chiffres-clés

Date de création : 2016
Effectif en 2018 : 6
Statut juridique : SAS
Projet(s) labellisé(s) : oui
Pays d'implantation : France

Mission et offres

Marchés cibles : Actuellement commercialisé en B2C, nous souhaitons développer notre offre à destination du marché B2B.
Description du produit/service : Wizi est une application mobile collaborative qui donne aux locataires ET aux propriétaires les moyens de sécuriser, d'optimiser et de simplifier TOUTES les étapes du cycle de vie d'une location longue durée entre particuliers.

Marchés visés

Le parc immobilier locatif français représente 5 500 000 logements détenus par 2 400 000 propriétaires bailleurs dont les 2/3 louent leur bien en direct. A l'échelle européenne, la tendance est encore plus marquée, 78 % des bailleurs traitent en direct avec les locataires sans passer par une agence immobilière. Mais le propriétaire bailleur, pour rester « maitre » de son bien en traitant directement avec son locataire, doit assurer toutes les tâches de mise en location et de gestion. Sans les compétences et les outils d'un professionnel immobilier il assume les risques de vacance locative, d'impayés et même de non-conformité juridique, car le marché immobilier est très réglementé. De son côté le locataire qui, pour éviter les frais d'agence, s'engage dans une relation directe avec un bailleur prend le risque de visites inutiles ou décevantes, car mal ciblées, d'une contractualisation non conforme, abusive ou illégale et d'un suivi administratif parfois chaotique. Les bailleurs et locataires en sont ainsi réduits, malgré les incertitudes et les risques d'une relation directe non professionnelle, à gérer par eux-mêmes leur processus de location en intégrant laborieusement outils disparates et gestion manuelle.

Solutions/produits innovants

Wizi est une innovation de service qui bouscule le marché en intégrant dans une application unique l'ensemble des moyens permettant d'exploiter un bien immobilier : gestion d'une annonce jusqu'au rapprochement locataire/propriétaire, contractualisation jusqu'à la signature du bail, gestion locative jusqu'au congé du locataire. Wizi est la première solution « tout en un » couvrant l'intégralité du processus de location entre particuliers. La stratégie d'une solution « Mobile first », donc sur smartphones dotés des dernières fonctionnalités (photo, géolocalisation, notifications, agenda …), permet d'exploiter les dernières technologies telles que la signature électronique, le paiement électronique, l'authentification faciale, la visite en réalité virtuelle, la réalité augmentée. Wizi, solution résolument innovante, fait également le pari d'être une solution « ready for future ».

XBRAIN

Gregory RENARD - CEO & Chief AI Officer
+1 650 285 8405 - gregory.renard@xbrain.ai

xBrain est un éditeur de logiciel spécialisé dans l'augmentation de la productivité par l'intelligence artificielle au travers du langage naturel. Satisfaction.AI est sa 1ere solution complète dédiée à l'augmentation de la relation client.

6, Boulevard Haussmann, 75009
www.satisfaction.ai
www.linkedin.com/company/xbrain

Chiffres-clés

Date de création : 2012
Effectif en 2018 : 16
Statut juridique : SAS
Pays d'implantation : France, USA

Mission et offres

Marchés cibles : B2B, B2C.
Description du produit/service : satisfaction.AI est une solution d'augmentation de la qualité et productivité de la relation client par la mise en oeuvre de processus d'intelligence collective entre l'Intelligence Humaine et l'IA.

Expertise et savoir-faire

Intelligence Collective Homme-Machine par Intelligence artificielle, Natural language processing et Machine Learning au service de la relation client.

Marchés visés

Les petites, moyennes et grandes entreprises dans un 1er temps, à travers le monde et pour tout type d'industrie (relation client, banque, assurance, e-commerce…). L'objectif à terme étant de rendre la solution accessible à tous les professionnels.

Solutions/produits innovants

Satisfaction.AI est une solution d'IA de gestion de la conversation dédiée à la relation client et basée sur la complémentarité homme / machine. En plus de vous permettre d'apporter une réponse 24h/24 à vos clients, elle permet une présence sur l'ensemble des canaux de communication : voix, sms, chat, email répondant ainsi à 100% des demandes de vos clients sur leur canal privilégié. satisfaction.AI vous permet aussi de passer très simplement d'un canal à un autre, de la voix au SMS par exemple. Ses interfaces de monitoring vous offrent une vue unifiée de l'ensemble des conversations en cours et permettent à vos collaborateurs de prendre la main si besoin sur des conversations (sur la base de notre solution brevetée d'analyse de l'atmosphère de la conversation et d'indicateurs métiers).

YESACCOUNT

José VAZQUEZ - directeur des Opérations
+33 6 32 24 09 47/+33 1 77 13 17 51 - jv@netsas.com

Solution YesAccount by Netsas, éditeur de logiciel. YesAccount est une plateforme d'automatisation de la tenue comptable et de certification blockchain des pièces, écritures comptables et transactions.

100, rue Lafayette, 75010 Paris
www.yesaccount.fr

Chiffres-clés

Date de création : septembre 2015
Effectif en 2018 : 1 à 2 salariés
CA en 2018 : 350 k€
Statut juridique : SAS
Projet(s) labellisé(s) : YesAccount
Pays d'implantation : France

Mission et offres

Marchés cibles : La solution YesAccount s'adresse en B2B aux professions du chiffre et principalement aux Cabinets d'Expertise Comptable.
Description du produit/service : YesAccount propose un bouquet d'applications permettant de collecter, traiter et exploiter les documents et les données utiles au pilotage de l'entreprise : gérer ses devis et factures d'achats ou de vente, suivre ses encours clients et fournisseurs, gérer ses notes de frais ou ses contrats. Elle permet de produire automatiquement des écritures comptables exploitables par son cabinet d'expertise.

Expertise et savoir-faire

YesAccount permet de produire automatiquement des écritures comptables directement exploitables par son cabinet d'expertise. Le Dirigeant dispose ainsi au fil de l'eau des données d'activité et le cabinet d'une tenue comptable automatisée pour plus de réactivité et de conseil. Ceci de manière transparente, simple et sécurisée.

Marchés visés

YesAccount est commercialisé avec succès par des cabinets d'expertise comptable. Nous voulons accélérer le développement commercial de la solution auprès des TPE françaises ainsi qu'auprès des banques ou une société d'assurance pour apporter un service différentiant à vos clients et disposer de données uniques.

Solutions/produits innovants

La fiabilité des données est une composante clé puisqu'elles sont utilisées pour les déclarations légales telles que la TVA, DNS, IS. Elles ne peuvent pas être altérées ou considérées comme peu fiables. Pour répondre à cette problématique centrale, nous avons fait reposer YesAccount dès sa conception en mai 2015, sur la technologie de blockchain publique. En soumettant l'ensemble des documents, transactions et exports comptables réalisés au fil de l'eau, les données exploitées deviennent alors irrévocables, uniques. Ces informations de grande valeur permettent de créer des services à très forte valeur ajoutée comme des achats groupés ciblés, des prêts interentreprises, des analyses financières en temps réel pour n'en citer que quelques-uns.

YOUSE

Olivier Bazin - Co-Fondateur et Directeur Général Adjoint
06 88 11 57 21 - olivier.bazin@youse.fr

Youse, c'est le garant qui change tout. Plus besoin de CDI avec une sélection unique à partir des relevés bancaires. Plus de retards de paiement ou d'impayés car c'est Youse qui verse le loyer.

4, place Raoul Dautry, 75015 Paris
www.youse.fr
LinkedIn ou autre :
www.linkedin.com/company/yousehome
www.twitter.com/YouseFrance

Chiffres-clés

Date de création : juin 2018
Effectif en 2018 : 8
CA en 2018 : 800 000 €
Statut juridique : SASU
Projet(s) labellisé(s) : labellisé dans la catégorie Immobilier + Prix du public pour la Fintech de l'année 2018.
Pays d'implantation : France

Mission et offres

Youse, c'est le garant qui change tout pour le propriétaire et pour le locataire.
Propriétaires ? Ne manquez plus un seul de vos loyers. En tant que propriétaire, vous avez deux exigences : trouver un locataire solvable, et percevoir vos loyers en temps et en heure. Et si nous avions enfin la solution ? Filiale à 100 % de CNP Assurances, Youse est le garant institutionnel qui sélectionne les locataires en analysant leurs relevés bancaires. Plus qu'un simple garant, Youse est un intermédiaire de paiement automatisé qui vous reverse chaque mois vos loyers à date fixe. Finis les impayés et retards de paiement ! Et en plus, c'est gratuit pour vous : la garantie Youse est intégralement financée par le locataire (3,8 % du loyer charges comprises). Résultat ? Vous sécurisez la rentabilité de votre bien… et vous gardez l'esprit libre ! Alors, prêt à oser Youse ?
Locataires ? Obtenez votre garant et rassurez les propriétaires ! Décrocher un appartement en location est devenu un vrai parcours du combattant. Quand on a pas de CDI, un garant et 3 fois le loyer, difficile de faire accepter son dossier. Et s'il était temps de tout changer ? Filiale de CNP Assurances, Youse apporte aux locataires le garant dont ils ont besoin pour rassurer les propriétaires. Comment ça marche ? Sur simple étude de vos relevés bancaires, Youse sélectionne les locataires les plus fiables et se porte garant. Après signature du bail, Youse reverse chaque mois vos loyers au propriétaires, contre une mensualité de 3,8 % du loyer charges comprises. Pour votre propriétaire, c'est une garantie forte qui inspire confiance. Alors, prêt à oser Youse ?

ZELROS

Christophe BOURGUIGNAT - CEO
06 30 89 92 09 - christophe.bourguignat@zelros.com

AI for Augmented Insurers.

Station F - 5, Parvis Alan Turing, 75013 Paris
www.zelros.com
www.twitter.com/ZelrosAI

Chiffres-clés

Date de création : 2016
Effectif en 2018 : 11
CA en 2018 : 1 M€
Statut juridique : SAS
Pays d'implantation : France

Mission et offres

Marchés cibles : B2B.
Description du produit/service : Solution d'IA pour assureurs : aide à la vente et à la gestion des sinistres. Grâce à notre technologie de machine learning, les assureurs obtiennent des gains de 40 % en moyenne, l'enjeu final étant l'amélioration de l'expérience client.

Expertise et savoir-faire

Machine Learning, Big Data, Intelligence Artificielle, cloud, traitement du langage naturel.

Marchés visés

Notre marché est celui des technologies d'Intelligence Artificielle pour assureurs et bancassureurs. Notre vision est que dans le futur, les assureurs les plus performants feront cohabiter cerveaux biologiques (experts humains) et cerveaux de silicium (intelligence artificielle) : ce sera l'avènement de l'Assureur Augmenté.

Solutions/produits innovants

Solution de collaborateur augmenté pour assureurs. Grâce à notre technologie de machine learning, nous révolutionnons la vente des produits d'assurance et la gestion des sinistres. Plusieurs clients ont déjà choisi notre solution (CNP Assurances, Natixis Assurance, MAIF, AXA…), principalement dans l'assurance habitation, crédit emprunteur, et vie.

Remerciements très particuliers à l'attention de Sarah Lamoudi



Sarah LAMOUDI

Je souhaite remercier tout particulièrement Sarah Lamoudi, expert Blockchain et Intelligence Artificielle pour son exceptionnelle contribution au pilotage et à la réalisation de ce Livre blanc.

En effet, au tout début de l'aventure, Sarah Lamoudi a montré une exceptionnelle motivation pour l'innovation en technologie appliquée à la finance : diplômée de l'École d'ingénieurs Polytech' Paris, titulaire d'un MBA de la Sorbonne et certifiée Fintech du MIT (Cambridge USA), et forte de 12 ans d'expérience en conseil dans de grands cabinets de conseil et stratégie (Capgemini, Accenture, PwC), Sarah a souhaité apporter son expérience au développement de l'écosystème Fintech au sein du Pôle de compétitivité, et la conduite du Livre blanc a représenté une opportunité inédite pour l'innovation dans le secteur financier et les défis de transformation digitale.

Sarah a montré des qualités très précieuses à plusieurs titres : l'identification des experts et des compétences nécessaires au projet sur un plan français et international, l'identification des meilleures tendances en intelligence artificielle, blockchain et quantique. Sarah est très « débrouillarde », curieuse et aime « challenger » les idées avec les meilleurs experts. Elle a su convaincre des experts de premier plan à rejoindre l'aventure.

C'est sur la base de cet état des lieux couplé avec l'état des lieux français que le livre blanc a été lancé au sein du Pôle de compétitivité fin 2017.

Une fois le Comité de pilotage désigné, Sarah a coordonné et piloté l'ensemble des groupes de travail (7 groupes de travail avec plus de 60 réunions) pour faire émerger avec les 200 participants (chercheurs du CNRS/CEA/INRIA, banquiers/assureurs/asset managers, startups/fintechs…) et en collaboration étroite avec les pilotes du Livre blanc et les équipes du Pôle, les domaines d'innovation prioritaires mis en exergue dans le Livre blanc.

Sarah a démontré pendant tout le temps du projet un esprit collaboratif, ainsi qu'une attitude très créative et a réalisé un travail de rigueur (technique/scientifique) avec détermination, en lien étroit avec des experts seniors notamment Juliette Mattioli (PhD, Senior Experte en IA, Thalès), Bertrand Braunschweig (Directeur de la Stratégie IA pour la France, ex-Directeur de INRIA Paris-Saclay), Jean Gebriel Ganascia (Professeur à Sorbonne université), Muriel Faure (Directrice de l'AFG), Philippe Denis (Head of Blockchain Lab, BNP Paribas CIB), Cathy Rosalie-Joly (Avocate associée, Experte réglementation fintech et blockchain, Bird&Bird), Patrick Seifert (Cabinet Chappuis Halder), Pascale Se-

nellart (Directrice de recherche CNRS en quantique)… ainsi que l'ensemble des experts qui sont remerciés très chaleureusement dans ce livre blanc.

Aujourd'hui, Sarah, ayant évolué dans le monde de l'innovation avancée, et forte d'un réseau global d'experts, est sur sa lancée pour mettre à disposition ses compétences au sein de structures (TPE/PME/Grandes entreprises ou fonds d'investissement) en pleine transformation technologique et humaine.

Ma chère Sarah, un grand merci de ma part et de toute l'équipe du Pôle ainsi que ceux qui ont collaboré avec toi.

Joëlle Durieux

Directrice générale
Pôle de compétitivité mondial
FINANCE INNOVATION

Un grand merci à tous les contributeurs

L'intelligence artificielle

- **Juliette MATTIOLI**
  Thales
- **Bertrand BRAUNSCHWEIG**
  INRIA
- **Jean-Gabriel GANASCIA**
  Professeur au Lip6 Sorbonne Université/ COMETS (Comité d'éthique du CNRS)
- **Hamza DIDARALY**
  IA Pour Tous
- **Yannick GAILLARD**
  Chappuis Halder & Co.
- **Patrick SEIFERT**
  Chappuis Halder & Co.

- **Christophe BOURGUIGNAT**
  ZELROS
- **Jean-Guillaume DE MANEVILLE**
  Netixis
- **Christine DAMEME**
  Orange Bank
- **Arnaud DE SERVIGNY**
  Bramham Gardens
- **Olivier DEBEUGNY**
  Lingua Custodia
- **Frédérique FAGES**
  FBF – Fédération Bancaire Française
- **Alice FROIDEVAUX**
  Quant Cube
- **Philippe GUILLAUME**
  Mutex
- **Stéphane HOUIN**
  CGI
- **Augustin HURET**
  MondoBrain
- **Thanh-Long HUYNH**
  Quant Cube
- **Benoît JULLIEN**
  Athling
- **Mouna KHETAB MOUSSAOUI**
  Invivoo
- **Youssef KHOALI**
  Digitalent consulting
- **Gauthier LALANDE**
  Malakoff Médéric
- **Jacques LEVY-VEHEL**
  INRIA
- **Nicolas MÉRIC**
  DreamQuark
- **Laure MERVAILLIE**
  xBrain
- **Éric MIGNOT**
  PlusSimple.fr
- **Laure MINOO MORRA**
  Société Générale
- **Yvon MOYSAN**
  IESEG
- **Bibi NDIAYE**
  BPCE
- **Gilles PAGÈS**
  LPMA Sorbonne Université
- **Guillemette PICARD**
  Allianz
- **Nathalie POUX-GUILLAUME**
  BNP Paribas
- **Laurent PRUD'HON**
  EURO-Information (Crédit Mutuel - CIC)
- **Gregory RENARD**
  xBrain
- **Bertrand RONDEPIERRE**
  Mission Villani pour l'intelligence artificielle
- **Michèle SEBAG**
  Laboratoire de Recherche en Informatique
- **Philippe SERAFIN**
  Sopra Steria
- **Benoît SPOLIDOR**
  Sopra Steria
- **Ludan STOECKLÉ**
  BNP Paribas
- **Thomas VALLI**
  Association Française de la Gestion Financière
- **Hervé VARILLON**
  Crédit Agricole
- **Chloé BEAUMONT**
  MAIF
- **Pejvan BEIGUI**
  EASY MILE
- **François-Xavier BOIS**
  Kernix

- **Francoise BRIAND**
  Dassault Aviation
- **Loïc BRIENT**
  Pôle Digital – BPCE
- **Stéphane BUFFAT**
  Institut Recherche Biomédicale des Armées
- **Jean-Charles CABELGUEN**
  iExec
- **Fabien CELLIER**
  Dascils
- **Georges COLLET**
  Athling
- **Jean-Marc DAVID**
  Renault
- **Olivier DE BELLESCIZE**
  OPCVM 360
- **Christine DUVAL**
  IBM
- **Stéphane FENIAR**
  DataRobot
- **Agathe GUILLOUX**
  Université Evry Paris Saclay
- **Samy JOUSSET**
  Région Île-de-France – Direction des entreprises et de l'emploi
- **Philippe KERIGNARD**
  Bouygues Telecom
- **François LABURTHE**
  Amadeus
- **Philippe LEPEUPLE**
  Intégraales Agora - inCube
- **Achille LERPINIÈRE**
  DGE – Direction Générale des Entreprises
- **Laurent MARCELLIN**
  CashLab
- **Jean-Marc MERCIER**
  MPG Partners
- **Michel MOULINET**
  Winbids
- **Gilles NOZIÈRE**
  OZE-Energie
- **Anass PATEL**
  Groupe570
- **Michel REVEST**
  ex-COVEA - Pôle Finance Innovation
- **Pierre RIOU**
  3WS-EVEA Cognitive
- **Georges UZBELGER**
  IBM
- **Pierre VERGER**
  Immo Neuf
- **Guillaume ANDRÉ**
  Banque de France
- **Véronique AUBERGÉ**
  UGA, CNRS – Laboratoire d'Informatique de Grenoble
- **Nathalie BEAUDEMOULIN**
  Banque de France
- **Olivier BLANDIN**
  Assurance Courtage Conseil Risk Management Associés
- **Stéphane CHAUVIN**
  mydataball
- **Philippe DUBOUCHET**
  Expert people
- **Sylvie FLECKINGER-BOTTER**
  Leader Trust - U-Invest
- **Thierry LE FUR**
  Addlib
- **Marie SOULEZ**
  Lexing Alain Bensoussan Avocats
- **Bertrand ANNETTE**
  Lyncas
- **Frédéric BARDOLLE**
  Algo Transparency
- **Jacques BAUDRON**
  IXTEL
- **Alain BENSOUSSAN**
  Lexing Alain Bensoussan Avocats
- **Pierre BLANC**
  Athling
- **Jean-Hubert DE KERSABIEC**
  Prévention, Sécurité, Santé, Satisfaction au Travail (P3S)
- **Dominique DELEERSNYDER**
  Cercle LAB
- **Jérôme DUPRÉ**
  Agreement Avocat
- **Adrien FACON**
  Secure-IC
- **Mélissa FREUNDLICH**
  Ailancy
- **Yannick GRELOT**
  DEECISION
- **Nicodème KANHONOU**
  Avistem
- **Serge KRYWYK**
  Aevatar
- **Françoise MERCADAL-DELASALLES**
  Crédit du Nord

- **Xavier RIPART**
  Investance Partners
- **Matthieu SÉNÉCHAL**
  Robin'Finance
- **Carolina SPOREA GODVIN**
  GenHybrid
- **Su YANG**
  Banque de France

La Blockchain

- **Muriel FAURE**
  AFG
- **Cathie-Rosalie JOLY**
  Bird & Bird
- **Alexandre STACHTCHENKO**
  Blockchain Partner
- **Alain ROSET**
  La Poste
- **Philippe DENIS**
  BNPP Securities Services
- **Marc ALAURENT**
  BNPP Personal Finance
- **Fatiha GRANDJEAN**
  Risk Management Solutions
- **Olivier SALOMON**
  Allianz
- **Arnaud GRUNTHALER**
  FieldFisher
- **Charles GUILLEMINOT**
  BNP Paribas
- **Stéphane EYRAUD**
  Chappuis Halder & Co.

- **Daniel AUGOT**
  INRIA
- **Muriel BARNEOUD**
  La Poste
- **Sébastien BOURGUIGNON**
  Margo
- **Guillaume BRUYAS**
  TATA Consultancy Services
- **Camille BUSSY**
  Société Générale
- **Fabien CELLIER**
  Dascils
- **Mathis COLIN**
  Consultant independant
- **Sébastien COUTURE**
  Stratumn
- **Rémi D'ALISE**
  Lusiol Project Fintechrisks
- **Noémie DIE**
  Institut Louis Bachelier
- **Alexandre EICH-GOZZI**
  Sopra Steria
- **Roxanne FAURE**
  Caisse des dépôts/LabChain
- **Nadia FILALI**
  Caisse des dépôts/LabChain
- **Francois-Xavier HAY**
  MACIF
- **Michel IVANOVSKY**
  MIPISE
- **Gauthier LALANDE**
  Malakoff Médéric
- **Jean-Marc MERCIER**
  MPG Partners
- **Jihane KHOUZAIMI**
  Fédération Française de l'Assurance (FFA)
- **Astrid MITTELHOCKAMP**
  Dentons
- **Anh NGUYEN**
  Pulsar Connect
- **Céline PASSEDOUET**
  50 Partners
- **Matthieu PATELSKI**
  Sopra Steria
- **Thomas REYNAUD**
  GarantMe
- **Agnès SERERO**
  EY Société d'Avocats
- **Xavier SIMONIN**
  Sopra Steria
- **Séraphin TSETE**
  La Banque Postale
- **Aurore TUAL**
  DGE – Direction générale des Entreprises
- **Cyril VIGNET**
  BPCE
- **Michelle ABRAHAM**
  Cabinet Michelle Abraham
- **Matthieu ALLEAUME**
  Société Générale
- **Thierry BEDOIN**
  Banque de France
- **Laurent BENICHOU**
  AXA
- **Cécile BLONDEAU DALLET**
  CNP Assurances

- **Paul BOUGNOUX**
  Largilliere Finance
- **Thomas BUREAU**
  Psion Finance
- **Gregory CHENUE**
  Crédit Agricole
- **Dominique CHESNEAU**
  Tresoriskconseil
- **Thibaut DE LAJUDIE**
  Ailancy
- **Régis DELAYAT**
  Scor
- **Jean-Louis DELPERIE**
  Exton Consulting
- **Romain DEVAI**
  Ailancy
- **Marc ESCUYER**
  Banque de France
- **Bruno GARÇON**
  Covéa
- **Mathilde GAROTIN**
  Allianz
- **Éric GAUBERT**
  Reinsurance Group of America
- **Christophe LEPITRE**
  OFI Asset management
- **Andres LOPEZ VERNAZA**
  Banque de France
- **Fabienne MARQUET**
  Économiste, vice-présidente X-sursaut
- **Emmanuel MORANDINI**
  April
- **William O'RORKE**
  ORWC Avocats
- **Johann PALYCHATA**
  BNPP
- **Claire PION**
  VariabL
- **Simon POLROT**
  LGO Group
- **Patrick SENICOURT**
  Nota PME
- **Dominique STUCKI**
  Cornet Vincent Ségurel
- **Audrey THOMAS**
  Exton Consulting
- **Stéphane THOMAS**
  Chappuis Halder & Co.
- **Christophe VAN CAUWENBERGHE**
  Paylib Services
- **Azzedine ALKHALFIOUI**
  Barclays
- **Christophe CHEREAU**
  BNP Paribas Personal Finance
- **Jérôme COIRIER**
  BeeAM
- **Dany DUBRAY**
  Celac Finance/Bloowing
- **Serge KRYWYK**
  Aevatar
- **Jean-Marc LEVY DREYFUS**
  Fone4 Technology
- **Henri MOCKA**
  Consultant indépendant
- **Quentin MOREL**
  Enza Management Consulting
- **Anass PATEL**
  Groupe 570 / ConexCap
- **Marie ROBIN**
  Bird & Bird
- **Lionel TOLEDANO**
  Sopra Steria
- **Sajida ZOUARHI**
  ConsenSys

Technologies quantiques

- **Pascale SENELLART**
  Centre de Nanosciences et de Nanotechnologies, CNRS, Université Paris-Sud, Université Paris-Saclay
- **Maud VINET**
  Leti CEA Tech
- **Eleni DIAMANTI**
  Chercheuse CNRS à Sorbonne Université, directrice adjointe du PCQC
- **Adrien FACON**
  Secure-IC
- **Georges UZBELGER**
  IBM France
- **Philippe DULUC**
  Atos
- **Yazid GHIRA**
  Chappuis Halder & Co.
- **Vincent WIENCEK**
  Chappuis Halder & Co.
- **Benoît GENEST**
  Chappuis Halder & Co.

- **Cyril ALLOUCHE**
  Atos
- **Alexia AUFFEVES**
  CNRS
- **Anil CASSAM CHENAI**
  LogicelIs
- **Philippe CATON**
  Covea
- **Alain CHANCÉ**
  Enza Management Consulting
- **Christine DUVAL**
  IBM France
- **Jean-Christophe GOUGEON**
  BPI France
- **Grégoire JAFFRE**
  BPCE
- **Iordanis KERENIDIS**
  CNRS
- **Julien KRYWYK**
  Preditt
- **Clément LEBLANC**
  Société Générale
- **Anthony LEVERRIER**
  INRIA
- **Sami LOUATI**
  BPCE
- **Frédéric MAGNIEZ**
  IRIF
- **UNIVERSITÉ PARIS DIDEROT – PARIS 7**
  LIAFA
- **Jean-Jacques RABEYRIN**
  BNP Paribas
- **Olivier SALOMON**
  Allianz
- **Miklos SANTHA**
  IRIF/CNRS
- **Philippe TESCHER**
  Exton Consulting
- **Jean VANNIMENUS**
  CNRS

Finance Innovation

Pôle de compétitivité mondial



VIVIENNE
INVESTISSEMENT

Vivienne Investissement est une société de gestion de portefeuille innovante créée en 2005 qui met en œuvre un processus d'investissement scientifique et discipliné en s'appuyant sur une approche par intelligence artificielle des marchés.

Membre du Pôle FINANCE INNOVATION,
la société a obtenu le label Bpifrance : Entreprise Innovante.

L'idée phare de Vivienne Investissement ? Mettre l'innovation par la recherche au coeur de la construction et de la gestion du portefeuille :

- En mettant des technologies de pointe telles que l'intelligence artificielle, le Big Data et les méthodes d'apprentissage automatique (Machine Learning) au service de la performance.
- En développant des outils d'analyse financière propriétaire multi-classes d'actifs afin de sélectionner dynamiquement les meilleures stratégies d'investissement.
- En étant toujours à la pointe de la recherche scientifique et financière et en poursuivant sa politique de publication et de conférences.

"Notre ambition est d'apporter à nos clients le meilleur de la recherche. Nous croyons dans l'innovation, qui apporte de la robustesse et permet d'adapter sans cesse notre compréhension des risques et des biais, pour structurer nos processus de gestion. L'idée majeure est de faire parler les données dans l'optique de comprendre les faits."

Laurent Jaffrès, *Président de Vivienne Investissement.*

Vivienne Investissement
Grand Hôtel-Dieu
1 place Pascalon, Bât D
69002 LYON - FRANCE
www.vivienne-investissement.com