

## BLOCKCHAIN – VERS UNE NOUVELLE RÉVOLUTION

## AVIS D'EXPERT

Par **Éric Lévy-Bencheton** | Blockchain Strategist - Keyruset **Frédéric Maserati** | Directeur Conseil - Keyrus Management

La Blockchain est une technologie créée avec le bitcoin, devenue la 8ème monnaie mondiale en termes d'échanges. La Blockchain porte en elle de nouvelles promesses d'innovation dans tous les secteurs, mais aussi de disruption des modèles économiques dominants. S'intéresser aujourd'hui à ses applications possibles, c'est prendre un temps d'avance sur la prochaine étape de la révolution digitale et l'avènement d'une société « horizontale », sans intermédiaires, ni autorité centralisée...

La Blockchain est probablement appelée à révolutionner les transactions et les échanges ; au même titre qu'Internet a permis la communication pair à pair, la Blockchain assurera dans les années à venir les transactions pair à pair avec une logique décentralisée et autonome.

Si un mystère subsiste quant à l'identité réelle des initiateurs du *Bitcoin*, la preuve est faite, après 7 ans d'existence, qu'il est possible de créer et de faire fonctionner dans la durée une monnaie 100% digitale en s'affranchissant du système bancaire et de toute autorité centrale. Ce tour de force a fini par attirer l'attention sur la technologie sous-jacente au *Bitcoin* : la fameuse « chaîne de blocs » ou Blockchain, dont le potentiel de disruption inquiète autant qu'il suscite d'intérêt et d'enthousiasme à travers le monde.

Pour preuve l'accélération des investissements, le nombre incroyable de conférences et d'articles. Engouement grandissant depuis notamment les effets d'annonce des Gouros de l'Internet ou de la Finance aux Etats-Unis, en premier lieu Blythe Masters au board de Digital Asset Holdings, qui a entamé un cycle de conférences sur les applications de la Blockchain au monde de la finance internationale, dont les impacts sont chiffrés en milliards de dollars... c'est peu dire !

Pensé et construit sur les cendres de la crise de 2008, le système porte dans ses gènes une philosophie de la confiance (*the trust machine*)<sup>1</sup>, établie par une collaboration massive entre les membres du réseau, et par des techniques avancées de cryptographie. Confiance qui devait pallier les défauts d'une finance mondiale encore en déroute.

## COMPRENDRE LES PRINCIPES DE LA BLOCKCHAIN

Avec la Blockchain, les informations partagées entre les

membres d'un réseau sont stockées sur chaque nœud de celui-ci (chaque ordinateur), au lieu de dépendre d'un point central. La validation des blocs est assurée par des moyens cryptographiques et par une logique de consensus, 51% des nœuds de la chaîne, devant approuver l'information.

Non seulement ce registre contient à tout moment l'historique complet des transactions mais il est infalsifiable et irrévocable, du fait même des technologies d'encryptions utilisées, et de sa répliquation en de multiples points. Cette description rapide permet de dégager trois apports majeurs de la Blockchain :

- la possibilité de limiter les intermédiaires et les tiers de confiance dans les échanges ;
- la possibilité de garantir la conformité, l'intégrité et la traçabilité d'une transaction ou d'une information sans recourir à une autorité supérieure/centrale ;
- l'absence d'infrastructure dédiée, la puissance de calcul nécessaire étant fournie par les machines des participants (nœuds) et optimisée par des algorithmes.

Nous parlons jusqu'à maintenant de Blockchain, « au singulier » en laissant éventuellement à croire en son unicité. Or il existe de nombreuses Blockchains (celle de la *Bitcoin* en est une) et elles adoptent différents modèles de gouvernance et/ou de partage d'informations : Privé, Public, Mixte, Hybride.

Une Blockchain peut porter des informations « statiques »

<sup>1</sup> <http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>

comme des transactions d'échange de *Bitcoins*, mais peut aussi être le porteur de programmes auto-exécutables, appelés *Smart Contracts* car ils peuvent agir comme des contrats « auto-porteurs » et automatiques.

Nous en voyons apparaître les premiers usages comme par exemple une assurance agricole liée à la météo, dont le *Smart Contract* ira automatiquement chercher la pluviométrie / l'ensoleillement auprès d'une source agréée par avance (météo France par exemple), et paierait le cas échéant l'indemnité convenue de manière automatique entre les parties.

Nous parlerons aussi d'*Autonomous Agent*, un ensemble de *Smart Contracts*, et donc un programme beaucoup plus complexe. Nous y voyons la promesse de nouvelles formes d'entreprises humaines, comme des organisations décentralisées. « The DAO » (*Decentralized Autonomous Organization*)<sup>2</sup> en est un des premiers exemples. La campagne de collecte de fonds réalisée sur Kickstarter pour la DAO s'est élevée à 174 millions de dollars<sup>3</sup>, ce qui en fait le projet de financement participatif le plus important qu'on ait jamais vu. La DAO peut s'apparenter à une société de financement distribuée, où ceux qui lui ont alloué des fonds peuvent décider des projets qu'ils pourront financer via des *Smart contracts* en échange d'un revenu sur ses investissements.

Le 17 juin 2016, The DAO a connu un immense crash suite à une attaque informatique, le « pirate » a réussi à exploiter une faille dans le « smart contract » régissant la DAO, lui permettant de siphonner petit à petit les ethers (*Token ou monnaie d'Ethereum*) détenus par cette dernière. Ce ne sont pas loin de 3,6 millions d'ethers qui ont ainsi été piratés, soit plus de 30% des fonds de la DAO !<sup>4</sup>

Nous y voyons volontiers également l'émergence de nouvelles formes d'intelligences artificielles basées sur les principes de l'IA « plautoïde »<sup>5</sup> comme le montre l'incroyable travail de Primavera de Filippi<sup>6</sup>, chercheuse à la faculté de droit de Harvard.

## POURQUOI LA BLOCKCHAIN EST UNE RÉVOLUTION ?

Certains y voient le moyen de passer à une économie collaborative à grande échelle et à de nouvelles formes d'exercice de la démocratie comme la nouvelle démocratie liquide ou *liquid democracy*<sup>7</sup>. D'autres tablent sur la promesse d'une réduction drastique des coûts de transactions grâce à l'élimination des intermédiaires ; d'autres encore y voient l'opportunité de développer des services inédits et, ce faisant, de prendre des positions dominantes sur des marchés totalement nouveaux ou existants – ce qui n'est pas sans inquiéter les acteurs en place, à juste titre... Même si cette technologie émergente, que presque personne ne comprend, reste absconse pour la plupart des gens, il faut avoir aujourd'hui le bon niveau d'abstraction pour pouvoir en parler, s'y intéresser, et commencer à imaginer les impacts sur les modèles des

organisations d'aujourd'hui et de demain.

Bien que le *Bitcoin* reste, à ce jour, la seule application à très grande échelle de la Blockchain, tous les observateurs s'accordent sur le caractère disruptif de cette technologie. Son irruption pourrait, selon certains, provoquer une rupture de même ampleur que le TCP/IP, le protocole à l'origine d'Internet !

Nous sommes face à la deuxième génération de l'Internet, celle des valeurs et des transactions, là où la première génération a largement été celle de l'information et de la communication réseau. (de l'automatisation de la relation décentralisée à l'automatisation de la transaction décentralisée).

Faut-il pour autant parler de révolution ? Outre qu'il faut beaucoup plus qu'une technologie pour faire une révolution, il est de toute façon trop tôt pour le dire. Cependant, le contexte social et économique est propice et, avec la constitution d'un écosystème très dynamique, les conditions sont réunies pour que les expérimentations se multiplient. Elles dépassent d'ores et déjà largement les moyens de paiement et même la finance, même si c'est dans ce secteur que l'on compte actuellement le plus d'initiatives et d'alliances avec des start-ups/fintechs travaillant sur la Blockchain.

## QUATRE GRANDES CATÉGORIES D'UTILISATION DE LA BLOCKCHAIN.

L'inventaire des initiatives et expérimentations en cours fait apparaître quatre grands domaines d'utilisation de la Blockchain.

**1/ La facilitation des échanges :** les paiements transfrontaliers, les micro-paiements, l'échange de titres non cotés, sont les premiers cas identifiés. Nous évoquons volontiers le cas de la Banque Allemande Fidor, en association avec la start-up Ripple Labs, qui a mis en place des services de paiements et de change, à coûts extrêmement réduits pour ces clients. Deux avantages de la Blockchain sont mis en œuvre : sa rapidité et ses coûts largement optimisés. La Banque Santander prédit à ce propos une économie de 15 à 20 milliards par an pour l'industrie des services financiers, à compter de 2020.

**2/ La notarisation d'actes et de documents :** la Blockchain ayant, comme nous l'avons vu, la capacité à stocker et rendre infalsifiable la preuve d'existence d'un document à une date donnée. L'Université Léonard de Vinci, à La Défense Paris, expérimente ce moyen dématérialisé pour certifier les diplômes qu'elle délivre.

**3/ L'exécution certifiée de workflows :** la Blockchain permettant la publication ainsi que la vérification publique de chaque étape d'un workflow. Qu'il s'agisse d'un processus industriel de contrôle qualité ou bien encore d'un processus de logistique, la logique de *trusted workflow* permet tout simplement de s'assurer que toutes les parties prenantes ont participé au processus,

<sup>2</sup> [https://en.wikipedia.org/wiki/Decentralized\\_autonomous\\_organization](https://en.wikipedia.org/wiki/Decentralized_autonomous_organization)

<sup>3</sup> <https://doahub.org/>

<sup>4</sup> Quand un membre quitte le fond d'investissement, il déclenche une fonction appelée *splitDAO()*. Et cela occasionne 2 problèmes. Le premier est que le membre doit fournir son propre code avec la transaction. Ce code permet de dire à la DAO où il doit transférer les Ethers. C'est une fonction nécessaire qui fait partie également du Bitcoin. Le second problème est que le code d'Ethereum est récursif. Cela signifie que lorsqu'une fonction est lancée, elle peut s'appeler une seconde fois. Et le bug se produit lorsqu'on appelle le *splitDAO()*. Quand l'appel est effectué, il va appeler le code de tous les récipients pour transférer les Ethers. Le code des récipients va ensuite appeler de nouveau *splitDAO()* avant de terminer le processus. Mais avec le bug, cela provoque une répétition du processus en transférant plus d'Ethers. En gros, le *splitDAO()* est déclenché, qui appelle le code du « pirate », qui appelle *splitDAO()*, qui appelle de nouveau le code du « pirate » et ainsi de suite. Plutôt que d'envoyer le montant désiré à celui qui veut quitter le fond d'investissement, le processus devient une boucle infinie en épuisant toutes les pièces du DAO.

<sup>5</sup> <http://theconversation.com/do-plantoids-dream-of-electric-arts-council-grants-52263>

<sup>6</sup> <https://cyber.law.harvard.edu/people/pdefilippi>

<sup>7</sup> <https://discuss.pirateparty.org.au/t/liquid-democracy-on-blockchain-and-in-parliament/527>

de façon certaine, irrévocable, à la connaissance de tous, simplement et facilement, l'information étant partagée en tout point des nœuds du réseau. Des laboratoires pharmaceutiques envisagent, par exemple, d'utiliser la Blockchain pour accélérer le recueil du consentement des patients à chaque nouvelle étape d'un protocole de test et réduire ainsi les coûts et la durée des phases d'essais cliniques, sur de nouvelles molécules.

**4/ Les titres de propriété numériques :** l'inscription sur le registre distribué d'une Blockchain permet d'attester la propriété d'un individu et de garder la trace de toutes les cessions d'un actif matériel ou digital. Avec l'aide de l'ONG Bitland, le gouvernement du Ghana table sur ces propriétés de la Blockchain pour mettre en place à moindre coût un cadastre officiel. Des artistes numériques commencent à l'utiliser pour authentifier leurs œuvres, en contrôler la diffusion et protéger leurs droits. Cette facette de la technologie Blockchain présente une rupture par rapport à la première génération de l'Internet qui a vu les créateurs, les ayants droits, se voir spolier de leurs droits au profit d'acteurs comme Spotify, Apple Music ... sans même évoquer les impacts du piratage.

#### BLOCKCHAIN OF THINGS ET BLOCKCHAIN OF DATA

Afin d'aller plus loin et d'ouvrir de nouvelles perspectives, avec notamment l'Internet des objets (*Internet Of Things* ou IoT) qui figure comme une déferlante inéluctable de nos sociétés numériques, nous pouvons évoquer divers exemples dans le B2C (traqueurs d'activité, domotique...) ou dans le B2B (capteurs de surveillance des voitures de flotte, capteurs de toutes les pièces d'un avion...), où l'IoT nécessite une capacité à effectuer chaque jour des milliards de transactions et de manière automatisée.

L'émergence d'une *Blockchain of Things*, stockant toutes ces transactions, avec des *Smart Contracts*<sup>7</sup> régissant les relations entre ces objets de plus en plus évolués, nous apparaît comme un impératif. En fait, l'IoT donne aux objets la possibilité de réaliser directement, en toute autonomie, des transactions. Cette vision de l'IoT suppose que les objets communiquent et réalisent des transactions entre eux. L'aspect décentralisé de la Blockchain constitue le ciment permettant à ces objets de transacter entre eux, d'en garder la preuve, dans un cadre de référence (*Smart Contract*) préalablement défini, en toute autonomie (IA) et sécurité. L'économie digitale passant de la "plateformisation" (mettre en contact direct des personnes entre elles) à la "Blockchainisation" (mettre en contact direct des « agents » entre eux) correspond à cette révolution numérique en cours

Dans une logique similaire, nous faisons confiance au quotidien à de nombreux organismes, qui stockent et utilisent nos données personnelles. Dans bien des cas, notre consentement éclairé n'est pas vraiment sollicité ni approuvé.

La *Blockchain of Data* pourrait être une solution pour stocker nos informations individuelles, mais surtout gérer (via les mécanismes des *Smart Contracts*) les droits conférés et/ou délégués aux entreprises. Certaines

données pourraient être gratuites sous certaines conditions, d'autres payantes à l'utilisation, enfin une dernière catégorie sur invitation uniquement.

#### SE PRÉPARER AU TSUNAMI DE LA BLOCKCHAIN.

Devant le caractère universel de ces catégories, on comprend que tous les secteurs, publics et privés, sont concernés et seront touchés, d'une manière ou d'une autre, par l'adoption et la diffusion des technologies Blockchain. Le nombre de processus susceptibles d'être impactés est proprement phénoménal. Les banques ne s'y sont pas trompées. Seules ou collectivement, comme au sein de consortium R3<sup>8</sup>, elles explorent et expérimentent les possibilités de la Blockchain avec un double objectif : tirer parti de ses avantages (de sécurité, de coûts et de transparence) et intégrer la logique de point à point dans leur propre modèle pour mieux résister à l'arrivée de nouveaux acteurs utilisant un modèle nativement distribué et désintermédié. Le monde de l'assurance fait de même et s'intéresse notamment aux possibilités offertes par les *Smart Contracts*.

Les premiers fournisseurs de solutions pour constituer des Blockchains publiques ou privées commencent à apparaître. Les start-ups fleurissent et attirent les investisseurs. Il faut donc s'attendre à voir surgir, dans tous les secteurs, des acteurs proposant des services P2P quasiment gratuits. Disruptifs il y a 5 ans avec leurs plate-formes de mise en relation, les fleurons de l'économie dite du partage ne sont pas à l'abri : la start-up israélienne LaZooz.org et son homologue anglais Arcade City entendent bien « uberiser Uber » avec son service de covoiturage décentralisé et autogéré basé sur la Blockchain...

Le seul moyen pour une entreprise de se préparer aux bouleversements annoncés est de s'intéresser dès maintenant à la Blockchain et à son écosystème. La première action est d'identifier les stratégies gagnantes pour accélérer ma transformation et garder ma longueur d'avance. Cela revient à se replonger dans tous les rouages de l'organisation et de sa chaîne de valeur et, en quelque sorte, à faire une mise à plat des modèles existants, avant de les re-penser à l'aune des technologies horizontales, décentralisatrices et sécurisées en mode P2P comme peut l'appeler de ses vœux Michel Bauwens<sup>9</sup>.

L'exercice paraît complexe mais c'est le plus sûr moyen d'identifier précisément où la Blockchain peut apporter quelque chose et commencer à l'expérimenter dans une logique de *Proof of Concept*.

La philosophie de cette démarche d'acculturation et d'expérimentation peut se résumer en une phrase : se « disrupter » soi-même pour ne pas subir la disruption. Internet promettait l'instantanéité, l'immédiateté et la permanence de l'information et de la communication en temps réel. La Blockchain promettra la collaboration, la transparence, la décentralisation, la sécurisation de toutes les transactions au sens large...

E.LB.

F.M.

<sup>7</sup> Ces contrats intelligents sont des programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine. Le concept n'est pas nouveau mais la Blockchain en renforce la sécurité et remplace le tiers de confiance nécessaire auparavant.

<sup>8</sup> Rejoint par plus 40 grandes banques depuis sa création à New York en 2014, le consortium R3CEV développe et expérimente pour l'industrie financière des standards et des solutions basées sur la technologie blockchain.

<sup>9</sup> [http://www.editionslesliensquilibrent.fr/livre-Sauver\\_le\\_monde-9791020901835-1-1-0-1.html](http://www.editionslesliensquilibrent.fr/livre-Sauver_le_monde-9791020901835-1-1-0-1.html)



## A PROPOS DES AUTEURS

**Eric Lévy-Bencheton** accompagne depuis 20 ans ses clients dans leurs transformations Marketing, Sales & Client, accélérées par les technologies du Numérique. Il a développé dans un premier temps une connaissance sectorielle du domaine bancaire, complétée ensuite par des expériences dans les secteurs de la Distribution, des Télécoms, de l'Énergie et du Transport. Dès 2011, Eric commence à accompagner ses clients dans l'exploitation des médias sociaux pour la Relation Client, et publie un des premiers documents de référence sur le sujet (« Social CRM – vers la Relation Client Augmentée »). Il intègre **Keyrus** début 2015, attiré par la capacité de l'entreprise à mettre au service de ses clients les leviers Numériques de la transformation, et à accélérer cette même transformation par l'exploitation de leur capital informationnel. Il y exerce un rôle de Strategic Account Executive, essentiellement pour le monde des services financiers. Auprès de Bruno Teboul, SVP Sciences & Innovation, Eric conduit le développement de nos offres autour de la technologie Blockchain.

**Frédéric Maserati** opère depuis près de 20 ans dans la Banque de Détails et dans le Retail. Il a occupé plusieurs fonctions opérationnelles notamment dans le marketing et le e-business pour le compte de plusieurs grands groupes bancaires. A partir de 2011 en qualité de Senior Manager dans un Grand Cabinet, Frédéric a accompagné de nombreux acteurs de la Banque et de la Distribution sur des problématiques autour des paiements, de la distribution, des nouveaux environnements utilisateurs et du Big Data. Il est aussi intervenu pour de nombreux événements de Place comme le Payforum ou Banque & Innovation, en qualité d'expert Paiement et Innovation. Il intègre **Keyrus** en 2015 comme Directeur Conseil au sein de **Keyrus Management** où il développe plusieurs offres autour de la Blockchain, des Crypto-monnaies, du commerce de demain et de la banque du futur, et des nouvelles approches autour de l'Intelligence Artificielle. Il s'intéresse de plus en plus aux impacts des technologies exponentielles sur les nouveaux modèles d'affaires des banques et des retailers.

## A PROPOS DE KEYRUS

**Keyrus, créateur de valeur à l'ère de la Data et du Digital**

Acteur international du conseil et des technologies, spécialiste de la Data et du Digital, **Keyrus** a pour mission d'aider les entreprises à tirer profit du paradigme de la Donnée et du Numérique pour accroître leur performance, faciliter et accélérer leur transformation et générer de nouveaux leviers de croissance, de compétitivité et de pérennité.

Plaçant l'innovation au cœur de sa stratégie, **Keyrus** développe une proposition de valeur unique sur le marché autour d'une offre novatrice qui s'appuie sur la combinaison de trois expertises majeures et convergentes :

**• Data Intelligence**

Data Science - Big Data Analytics – Business Intelligence – EIM – CPM/EPM

**• Digital Experience**

Innovation & Stratégie Digitale – Marketing Digital & CRM – Commerce Digital – Performance Digitale – User Experience

**• Conseil en Management & Transformation**

Stratégie & Innovation – Transformation Digitale – Pilotage de la Performance – Accompagnement des Projets

Présent dans 15 pays et sur 4 continents, le Groupe **Keyrus** emploie près de 2500 collaborateurs.

**Keyrus** est coté sur le compartiment C de l'Eurolist d'Euronext Paris (Compartiment C/Small caps - Code ISIN : FR0004029411 – Reuters : KEYR.PA – Bloomberg : KEY:FP)

Plus d'informations sur : [www.keyrus.fr](http://www.keyrus.fr)