

L'impact de l'émergence de la Blockchain sur l'industrie des paiements



Editions du Club SEPA



L'impact de l'émergence de la Blockchain sur l'industrie des paiements

Introduction

Avec la Blockchain, émergent de nouvelles modalités d'échange de transactions financières ou de valeurs, **sans intermédiaire**, grâce à un principe qui cumule cryptographie, enregistrement dans un registre partagé et authentification dans le cadre d'un consensus distribué sur internet.

Dans la première approche de Blockchain publique, les caractéristiques d'échanges Peer-to-Peer remettaient en cause le modèle d'échange de valeur avec un tiers de confiance. Dans le modèle de Blockchain privée, sur lequel nous reviendrons, cette contrainte peut être levée.

Les principes retenus répondent aux enjeux d'échange économique de plus en plus dématérialisé entre deux acteurs nécessitant une authentification et une irrévocabilité des transactions numériques au travers des médias digitaux.

Définitions et vocabulaire utilisés :

- **La Blockchain** est d'abord une technologie de stockage et de transmission d'informations, ouverte, sécurisée, et fonctionnant sans organe central de contrôle. Solution en open source, elle s'appuie sur des registres (ou Ledger) décentralisés et partagés par une communauté. Cette technologie est aussi appelée **DLT** (Distributed Ledger Technology).
- **Une transaction Blockchain** est une transaction cryptée, irrévocable, dont les données sont enregistrées numériquement dans des blocs. Chaque bloc est chaîné au prochain bloc en utilisant une signature cryptographique.
- Cela permet aux chaînes de bloc d'être utilisées comme un **journal comptable** qui peut être partagé et accessible par n'importe qui à partir du moment où il en a l'autorisation. Ce journal s'appelle « Ledger »
- Il existe des **Blockchains publiques**, ouvertes à tous, et des **Blockchains privées**, dont l'accès et l'utilisation sont limités à un certain nombre d'acteurs.
- **Sidechain** :¹ Blockchain secondaire qui se développe parallèlement à une Blockchain principale, mais qui y est rattachée afin de pouvoir en connaître toutes les informations. Les sidechains permettent d'accroître le volume d'informations pouvant être traitées au sein d'une Blockchain (volume normalement limité), tout en restant sur une même Blockchain principale.
- **Les Smart Contracts** ²sont des contrats dont les termes sont enregistrés en langage informatique au lieu d'un support légal. Ils peuvent être exécutés automatiquement par un système informatique comme par exemple un « Ledger » distribué.

¹ <https://blockchainfrance.net/blockchain-pour-les-nuls/>

² <https://blockchainfrance.net/le-lexique-de-la-blockchain/>

Cas d'Usage de la Blockchain dans le monde de la Finance

Nous sommes au début des cas d'usage de la Blockchain dans le monde financier, mais nous ne maîtrisons pas la vitesse de propagation de l'utilisation de la Blockchain.

En effet la nature immuable, infalsifiable et partagée de la Blockchain a induit des cas d'usages standard dans le monde financier, notamment :

- Les transactions de paiements internationaux,
- La tenue de registres sécurisés,
- La mise en œuvre de pistes d'audit,
- Les Smart Contracts pour des contrats OTC sur les marchés financiers ou des contrats de Trade Finance.
- La connaissance du parcours client dans une banque, ...

De 2014 à maintenant, les premières expériences, plus ou moins fructueuses, ont fait place à des POC plus concrets en 2016, et à des premières applications en Production Opérationnelle courant du deuxième semestre 2017.

- Aux Etats Unis, **le groupe R3** est un groupe de 70 membres, spécialisé dans la technologie Blockchain, et fondé en 2014, à New York.
- D'autres acteurs importants, comme **Hyper Ledger** ou **Ethereum**, regroupent des établissements, qui sont membres simultanément de plusieurs consortiums. Une dynamique permanente s'exerce avec ces acteurs.
- **Un groupe de 8 banques** (Deutsche Bank, HSBC, KBC, Natixis, Rabobank, Société Générale et UniCredit, rejointes en janvier 2017 par Santander), commercialisent une nouvelle offre développée avec IBM, **Digital Trade Chain (DTC)** pour simplifier les traitements Trade Finance des PME et ETI en leur permettant de gérer, suivre et sécuriser leurs transactions domestiques et internationales en open account. En raison de l'expansion et de l'internationalisation de la plateforme en 2017, le consortium a décidé de renommer la plateforme « **we.trade** » marque plus attirante et plus forte que DTC.
- En France, **LaBChain**, lancé par la Caisse des Dépôts, regroupe 25 partenaires en Banque et Assurances. Et la CDC a officialisé, en novembre 2016, son deuxième cas d'usage avec la gestion du collatéral, entrepris avec quatre membres de LaBChain (Crédit Agricole, Natixis Asset Management, CNP et OCTO Technology).
- **Le Crédit Mutuel ARKEA** a déployé en octobre 2017 une application avec la technologie Blockchain pour la mise en relation et la connaissance client.
- **La Banque de France** (projet MADRE pour les ICS) et d'autres établissements ont aussi lancé leurs expériences en 2016. Après une expérimentation de MADRE par plusieurs banques françaises, la Banque de France est passée en Production le 15 décembre 2017, et prévoit le raccordement des 4 1ères banques au 1^{er} semestre 2018.

Mais expliquons le fonctionnement de la Blockchain.

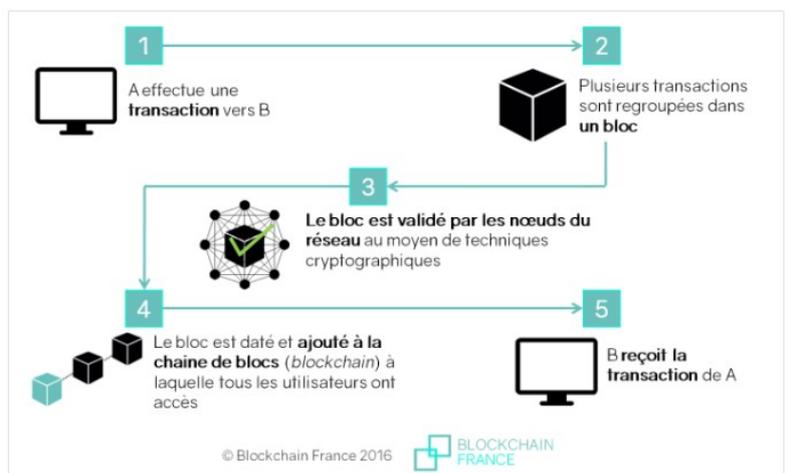
La Blockchain : comment ça marche et comment elle peut être mise en œuvre ?

Les éléments expliqués ci-dessous concernent la Blockchain publique, nous reviendrons par ailleurs sur la Blockchain privée.

Toute Blockchain publique fonctionne nécessairement avec une monnaie ou un token (jeton) programmable. Bitcoin est un exemple de monnaie programmable.

Les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs. Chaque bloc est validé par les “mineurs”, selon des techniques qui dépendent du type de Blockchain. Dans la Blockchain du Bitcoin cette technique est appelée le “Proof-of-Work”, preuve de travail, et est effectuée par la résolution de problèmes algorithmiques.

Une fois le bloc validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que pour l’ensemble du réseau.



Ce processus prend un certain temps selon la Blockchain dont on parle (environ une dizaine de minutes pour Bitcoin, 15 secondes pour Ethereum).

- **Peu de volume et pas (encore) de temps réel** : La Blockchain de par ses contraintes de génération n’adresse pour l’instant que des cas d’usages qui nécessitent peu de volume de transaction et pas de temps réel du fait du temps nécessaire à la génération des Blockchain et de leur traitement.

Il faut cependant indiquer que des études et des tests sont effectués sur des machines à processus beaucoup plus performant, ce qui pourrait lever la contrainte du temps. Ce n’est pas encore opérationnel ni répandu, mais la démarche est lancée.

- L’autre élément à tenir compte est la **notion de valeur probante** de la Blockchain et de valeur juridique. En effet, étant donné que les Blockchains sont générées par un réseau sans organe de centralisation, les principes de confiance et de contrepartie restent à mettre en œuvre.

³ <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>

Blockchain publique et privée

Il faut comprendre ces deux concepts, car ils conditionnent le développement et l'industrialisation du concept d'utilisation de la Blockchain.

Dans la **Blockchain publique**, tous les nœuds du réseau d'échange sont contrôlés par le réseau Peer-to-Peer (« permissionless »). Il n'y a aucune barrière d'entrée, aucune permission à demander pour effectuer une transaction et tous les acteurs sont donc en situation égalitaire dans leur participation au réseau. C'est le cas de la monnaie virtuelle Bitcoin, bien sûr, et de l'Ethereum.

De plus, la technologie Blockchain publique, même si elle évoluera dans le temps, demande à ce jour une très grande puissance de calculs et donc une énergie considérable, d'une part, et d'autre part présente des limites fortes en nombre de transactions par unité de temps.

La **Blockchain privée** est un concept qui se déploie à l'heure actuelle en 2017, même s'il peut apparaître au premier abord comme détournant le principe fondamental d'absence de tiers de confiance. (« permission »)

Deux types de Blockchain privées existent à ce jour :

- Blockchain privée « réduite », ayant les caractéristiques suivantes :
 - Processus de validation limité à une unique organisation
 - Les autorisations de lecture peuvent être publiques ou partiellement limitées, suivant la volonté de l'organisation valideur.
 - La Blockchain devient donc centralisée
 - L'usage est donc limité par rapport à la Blockchain publique
- Blockchain sous contrôle (de consortium), qui représente sans doute l'avenir de l'utilisation de la Blockchain.
 - Un certain nombre de nœuds, présélectionnés, ont la charge d'approuver les transactions.
 - Les valideurs sont donc limités et sélectionnés. Nous revenons indirectement à l'institution (ou l'organisation) en charge du tiers de confiance
 - Le droit de consulter les données est ainsi possible mais réservé aux participants
 - Il tourne sur un réseau privé sur lequel le gérant peut modifier le protocole quand il le souhaite. Personne ne peut y participer sans y être autorisé.

Il est important de constater qu'aujourd'hui, c'est la Blockchain privée qui est le moteur du déploiement de l'utilisation de cette technologie.

L'enjeu de l'interopérabilité

L'interopérabilité des Blockchains entre elles, avec les systèmes informatiques hérités, avec les IoT, les messageries et les réseaux sociaux, est également une clé dans la réussite de l'adoption de cette technologie.

Il existe de multiples déclinaisons de la technologie des Blockchains (Bitcoin, NXT, Ethereum, Eris, Blockstream, ...). A titre d'exemple, dans un monde composé de Blockchains et de systèmes hérités, il sera nécessaire d'apporter une solution à la création d'une vision 360 degré d'un client, de son risque, de l'activité d'une ligne métier ou de toute autre vue consolidée.

Des tentatives de mélange Blockchain privées / Blockchain publiques voient le jour. Par exemple, IBM a conclu un partenariat pour les échanges internationaux transpacifiques avec la société Stellar, qui gère le règlement en monnaie virtuelle.

Autre exemple, comment traite-t-on le cas d'un client cédant la propriété de son contrat démarré sur la Blockchain de sa banque à un client d'une autre banque utilisant une autre technologie de Blockchain ? Faut-il l'envisager ? L'usage métier devra déterminer la technologie choisie.

De manière plus large, une interopérabilité entre acteurs de secteurs différents (financiers / industriels/commerçants) apportera de nouveaux cas d'usages de la Blockchain.

Les enjeux de la Blockchain dans les paiements : une alternative ou une complémentarité

L'effet disruptif de la Blockchain est bien réel à moyen terme. Ses caractéristiques d'échange Peer-to-Peer, d'irrévocabilité et d'authentification, pourraient remettre en cause le modèle bancaire de tiers de confiance dans les échanges bancaires, principe fondamental dans toutes nos architectures et systèmes de paiement.

Le monde financier a pris conscience du risque de désintermédiation et s'organise en conséquence. Plusieurs banques mondiales se sont ainsi regroupées autour de communautés dont le Consortium R3 cité plus haut afin de proposer leur solution.

L'idée est de s'imposer parmi les 6000 Blockchains privées et publiques afin de continuer à gérer les transactions financières mais aussi de l'élargir à l'échange de valeur. Si la Blockchain est nativement open source, la course à son contrôle est lancée.

Au-delà de la maîtrise de la chaîne, les banques ont réalisé que l'utilisation de cette technologie serait source d'économies pour leurs infrastructures par l'automatisation de processus. Dans un rapport de 2015, la Banque Santander a estimé à 15 milliards de dollars par an d'ici 2022, les économies possibles pour le groupe.

De nombreuses institutions financières lancent études et initiatives afin d'explorer les opportunités que cette technologie peut apporter.

Les investissements évalués à 75 Millions de Dollars en 2015 et 400 millions de Dollars en 2019 (Source Aite Group), sont en rapport avec le ROI attendu. Le consortium R3 vient d'ailleurs d'annoncer une levée de fond de 200 millions d'euros.

L'apport du Blockchain dans les paiements est de quatre ordres :

- Maîtrise des risques grâce à une gestion de la liquidité et des risques, plus proche du temps réel.
- Optimisation du cycle de vie des transactions du fait du débouclage effectif des opérations, ce qui élimine les réconciliations et les exceptions
- Simplification de la gestion des réclamations, grâce au caractère irrévocable de la transaction et de sa traçabilité.
- Partage facilité des données dans un même registre

Ces capacités permettent aujourd'hui d'adresser des problématiques liées à l'ouverture de la chaîne de valeur à de nouveaux acteurs et donnent des perspectives sur plusieurs évolutions majeures pour le système de paiement que nous connaissons actuellement : séquestre de fond, archivage centralisé, sécurisé et immuable, transactions irrévocables avec piste d'audit, signature sécurisée induisant trois tendances (l'automatisation de la preuve, l'ouverture des systèmes d'information à des tiers, la remise en question de principe de régulation centralisée par le transfert de valeur de Peer to Peer).

Conclusion : avis du Club SEPA

Dans un premier temps, il est sans doute envisageable que la Blockchain soit mise en place dans le cadre d'échanges financiers internationaux, avec une logique de paiements unitaires, car le tiers de confiance sur ces échanges n'est pas régulé au niveau mondial.

Par ailleurs, en Europe, la Blockchain pourrait répondre en partie aux problématiques de la DSP2 de par son système ouvert, sécurisé et de mise à disposition de données à toute une communauté comme des données bancaires. Mais nous sommes loin des API mises au point pour la DSP2 en ce moment.

La Blockchain bien utilisée peut aussi répondre à certaines contraintes de la GDPR, autre défi à prendre en compte en Europe.

A ce titre cela pourrait pourtant devenir, à terme, un facilitateur du déploiement des transactions SEPA et de mise en concurrence des acteurs dans le contexte de la DSP2.

Plus globalement, c'est la Blockchain privée de consortium qui paraît l'emporter en ce moment, dans le cadre d'applications opérationnelles mises en production. En effet, ce type de Blockchain est plus facile à gérer pour la validation des transactions et la construction d'une offre. Plusieurs acteurs industriels s'y emploient avec des offres grandissantes (IBM, Sopra, ...).

Si certains acteurs pensent à un investissement à 20 ans, d'autres accélèrent le pas, diminuent les contraintes (performances et mise en œuvre opérationnelle), et les cas d'usage se multiplient, aussi bien dans le monde bancaire que dans les autres secteurs. Mais le temps de la maturité est difficile encore à prévoir.

De nouveaux cas d'usage, impliquant des acteurs aussi bien dans le commerce, l'industrie et la finance, vont faire évoluer les modèles économiques et à ce titre, l'utilisation de la Blockchain est réellement disruptive et les banquiers seront bien entendus parties prenantes.