WAVESTONE

LA *BLOCKCHAIN*
COMMENT RÉINVENTER LA CONFIANCE ?

LA *BLOCKCHAIN* : INNOVATION DISRUPTIVE OU SURMÉDIATISÉE ?

Difficile de ne pas avoir déjà lu au moins un article traitant de la *blockchain* et de ses vertus potentielles ! Pourtant, en dehors d'un petit cercle d'experts, le sujet reste aujourd'hui mal maîtrisé. Entre les communiqués de presse qui, sous couvert d'innovation, maquillent des annonces marketing, et les livres blancs abordant de manière très pointue la thématique via de la recherche fondamentale en informatique, statistiques et cryptographie, il est compliqué pour les décisionnaires au sein des grands comptes de se fixer une ligne de conduite.

Pour guider les réflexions, prenons en analogie le milieu de la recherche médicale où l'introduction de nouvelles solutions est extrêmement encadrée. Pour savoir si la technologie est prête, comparons-donc la *blockchain* à un médicament. Les questions qui viennent naturellement à l'esprit sont : quelle pathologie ce médicament prévoit-il de traiter ? Où en sommes-nous des tests ? Et le produit est-il suffisamment mûr pour une autorisation de mise sur le marché ?

Voyons donc ce qu'il en est pour la *blockchain*.

AUTEUR

JONATHAN GÉRARDIN
jonathan.gerardin@wavestone.com

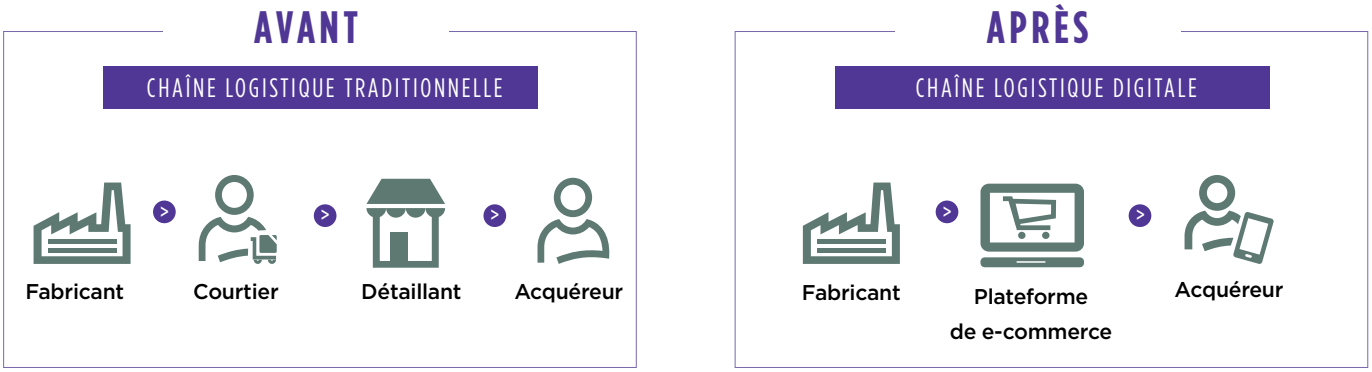
PEUT-ON CRÉER UNE MONNAIE ÉLECTRONIQUE SANS ORGANISME CENTRAL CHARGÉ DE GARANTIR LE SYSTÈME ?

L'essor d'Internet sur ces deux dernières décennies a entraîné d'importants bouleversements économiques, notamment causés par la suppression de certains intermédiaires. Certains secteurs reposant sur des tiers, spécialistes de la commercialisation de produits ou services, ont ainsi été profondément impactés. C'est le cas du tourisme ou encore de la distribution.

Ces fameux « intermédiaires » ont été progressivement remplacés par de nouveaux acteurs hyper-généralistes, fournisseurs de plateformes de commerce basées sur des technologies de pointe, ce qui les a propulsés comme les géants du numérique que nous connaissons : Amazon, Apple, Google et Facebook. Ils ont dès lors prospéré en prenant activement part à une désintermédiation massive qui a engendré une réduction importante des coûts de leurs services, ainsi qu'une accélération et une facilitation des transactions.

Ce processus de désintermédiation a été concentré sur la simplification de la chaîne logistique, en supprimant les intermédiaires entre le fournisseur et le client.

Processus de désintermédiation



Ce phénomène de dématérialisation a considérablement renforcé le rôle d'un de ces intermédiaires. En effet, pour nos achats en ligne, nous faisons appel à un tiers de confiance, chargé de garantir la fiabilité, la sécurité et l'auditabilité du paiement : les établissements de paiement (banques, Paypal, etc.). Leur rôle est d'assurer la bonne exécution des opérations de paiement entre l'acheteur et le vendeur, tout en garantissant la justesse du système dans son ensemble. Dans le cas d'un paiement dématérialisé, en l'absence de monnaie fiduciaire, les montants peuvent, d'un point de vue purement technique, être dupliqués aussi facilement que l'on duplique un fichier électronique. Certaines précautions doivent donc être mises en œuvre pour que la confiance dans notre système d'échange monétaire demeure intacte.

Le sujet de la « dépense double » («*double spending*») est une problématique informatique classique, rendue populaire par la généralisation des moyens de paiement dématérialisés. L'enjeu étant de permettre des transactions aussi rapides et fluides que celles que nous réalisons avec de la « monnaie physique ».

Depuis les années 80 et la popularisation de la carte bancaire, personne n'avait été en mesure de trouver de solution à cette problématique, sans avoir recours à un intermédiaire, tiers de confiance, chargé de vérifier et de procéder aux opérations de paiement.

Avec les années 2000 et l'explosion du commerce électronique, le problème avait finalement fini par être considéré comme insoluble, jusqu'au 31 octobre 2008, date de publication **du livre blanc « *Bitcoin: a Peer-to-Peer Electronic Cash System*[1] » dans lequel Satoshi NAKAMOTO** présente sa solution de monnaie électronique et démontre que le problème de « dépense double » peut être résolu sans le recours à un tiers de confiance.

Pour reprendre notre analogie médicale, la « dépense double » est la pathologie que se propose de traiter Bitcoin (qui est en soit la première implémentation d'une blockchain).

1- Bitcoin P2P e-cash paper - Cryptography mailing list - Satoshi NAKAMOTO - 31 octobre 2008 - http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

BLOCKCHAIN : UNE VIABILITÉ TECHNIQUE DÉMONTRÉE AU QUOTIDIEN À TRAVERS BITCOIN

La *blockchain* est un registre de transactions, non répudiables, fonctionnant sans autorité centrale.

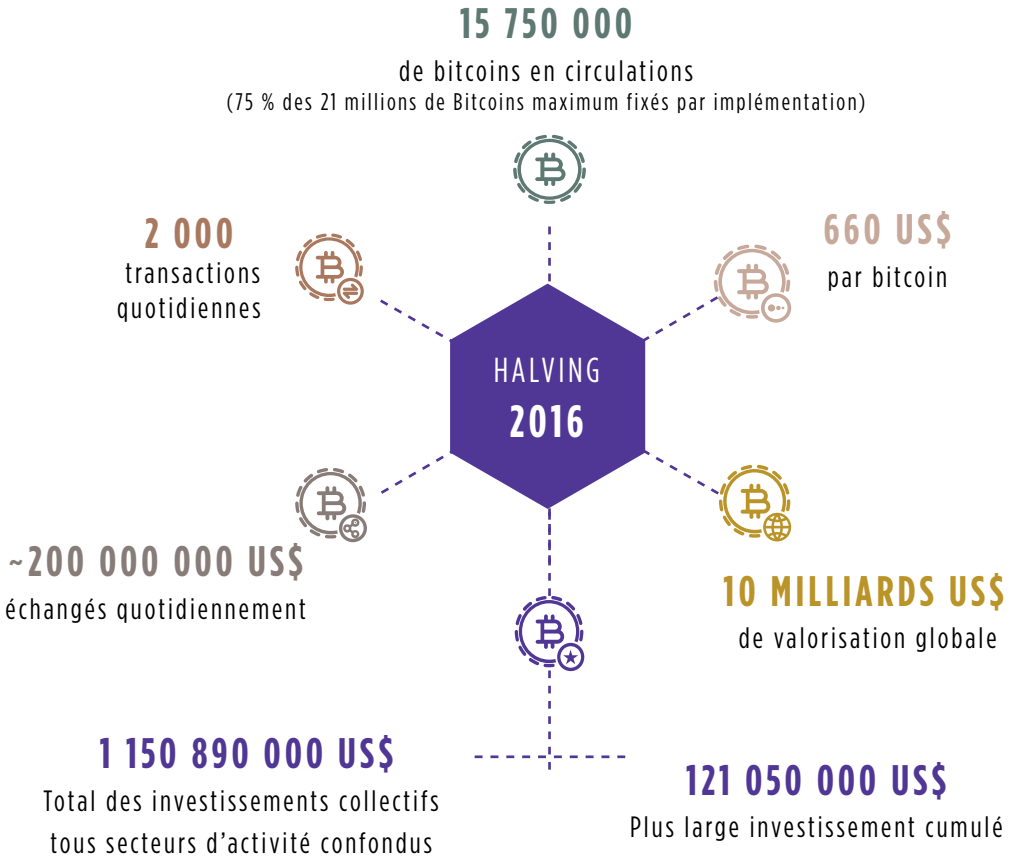
En 8 ans, Bitcoin a prouvé la robustesse du système proposé par Satoshi et sa *blockchain* n'a jamais cessé de croître. Le modèle est donc loin d'être une simple proposition théorique : elle s'impose aujourd'hui comme **un système opérationnel de gestion de transactions électroniques, distribué mondialement, basé sur un système ne reposant pas sur la confiance en une autorité centrale.** En quelque sorte, on peut considérer que le médicament est efficace, *in vivo*, et que la phase de tests à grande échelle a bien été réussie.

Pour mieux comprendre le chemin parcouru depuis, Bitcoin au 09/07/2016[2] c'était :

> Le **09/07/2016** est une date symbolique pour le Bitcoin. La récompense associée au minage d'un nouveau block (opération de validation d'un groupe de transactions) est réduite de moitié tous les 210 000 blocks, on parle de **Halving**. À cette occasion la rétribution est passée de 25 bitcoins à 12 bitcoins. Le prochain se produira le 26 juin 2020, et réduira à 6 bitcoins la récompense associée au minage d'un nouveau bloc valide.

Et bien que la *blockchain* ne soit rien de plus initialement que la solution technique permettant le fonctionnement de Bitcoin, c'est en fait véritablement un système alternatif au recours à une autorité centrale pour garantir l'enregistrement de transactions de tout type. Par rapport aux systèmes traditionnels, **la *blockchain* promet d'offrir une plus grande efficacité de traitement, davantage de fluidité et des coûts de fonctionnement réduits**. Ces bénéfices étant, du reste, envisageables grâce à la suppression des « tiers de confiance » (désintermédiation).

Bitcoin au 09/07/2016



2- Source : Bitcoin Magazine Halving Infographic - https://bitcoinmagazine.com/articles/the-halving-then-now-a-bitcoin-magazine-infographic-1468082535

LA *BLOCKCHAIN* EST-ELLE UNE INNOVATION DISRUPTIVE, EN DEHORS DES MONNAIES ÉLECTRONIQUES ?

Comme dans chaque cycle industriel, une innovation s'accompagne d'un écosystème d'entreprises, ou d'organisations, d'entrepreneurs, souhaitant transformer le progrès technique en de nouveaux produits ou services. **Pour la *blockchain*, tous les secteurs dont le produit, ou le service, reposent sur la confiance sont potentiellement éligibles à transformation**. Le nombre d'acteurs n'a eu de cesse de proliférer, qu'il s'agisse de plateformes « généralistes » dont le service de base est la confiance («*Trust as a Service*»), que de spécialistes adressant chacun leur sujet de niche.

Mais **jusqu'à présent la recherche d'application** où la *blockchain* pourrait offrir des avantages par rapport à des solutions plus classiques, **n'a pas fait apparaître de domaine évident, en dehors des monnaies électroniques, que la solution serait en mesure de révolutionner.**

Pour un médicament, on pourrait dire que la reproductibilité des effets bénéfiques de la blockchain reste encore à démontrer. En l'attente d'une telle démonstration, l'autorisation de mise sur le marché serait suspendue, et le médicament ne pourrait quitter les expérimentations de laboratoire.

COMMENT PASSER DE L'INNOVATION TECHNOLOGIQUE À UNE UTILISATION INDUSTRIELLE MAÎTRISÉE ?

Les principes techniques fondamentaux de la *blockchain* sont matures et le modèle dispose d'une valeur certaine. Pourtant, **le chemin reste important pour trouver les bons cas d'usage et transformer le progrès technique en de nouveaux produits ou services innovants accessibles à tous.**

Les actualités récentes mettent en lumière les difficultés auxquelles se heurtent actuellement les pionniers du marché. Les *blockchains* les plus populaires ayant pour usage principal celui de monnaie

Aperçu de l'écosystème *Blockchain*

1 GÉNÉRALISTES

PLATEFORMES DE « *TRUST AS A SERVICE* » Ethereum, Rootstock, Tendermint, Lisk, Eris...

2 SPÉCIALISTES DE NICHE

SERVICES FINANCIERS

Paiement, prêt, gestion de patrimoine, financement participatif

Blade, BitNet, BitPay, Ripple, BitBond, BTCpop, LoanBase, AlphaPoint, KolBanx, WelFund, Harvestr...

IDENTITÉ

Authy, BlockSeer, NetKi, OneName, ShoCard...

ASSURANCE ET MICRO-ASSURANCE

Augur, EverLedger, WeKeep, Consuelo, Riskebiz...

NOTARIAT, PROPRIÉTÉ INTELLECTUELLE ET BREVETS

BitProof, CoinSpark, Mamoru, Proof of Existence, Stampery...

électronique, celles-ci font naturellement l'objet de convoitises importantes. La sécurité nécessite plus que jamais l'intervention de spécialistes pour se protéger.

- En mars 2016, *Shapeshift*, une plateforme de change de monnaies électroniques (comme pour un bureau de change, la plateforme permet d'échanger entres elles Bitcoin, Ether, Litecoin, et autres), a été **victime d'un piratage réalisé par l'un de ses propres administrateurs système**[3]. Le piratage a entraîné le vol de 230 000$, l'interruption de la plateforme pour un mois, ainsi que la reconstruction dans l'urgence des infrastructures.

  Les procédures de sécurité de base de l'entreprise ont dû être renforcées suite à l'incident, en particulier en ce qui concerne les procédures de communication sécurisée entre les employés, ainsi que les moyens d'accès aux serveurs hébergeant la plateforme.

- En juin 2016, « *The DAO* » active sur la *blockchain* Ethereum a été victime d'un piratage d'un montant de 3,6 millions d'Ether. « *The DAO* » est le nom d'une *Decentralized Autonomous Organization*, c'est-à-dire une organisation dont les statuts (règles, gouvernance, et moyens de décision) sont implémentés à l'aide de *smart contracts* (extensions logicielles permettant de réaliser des opérations sur la *blockchain*, selon des conditions définies dans un contrat). L'objectif d'une DAO est d'éliminer le recours à des documents, et aux personnes, en vue de créer une structure fonctionnant de manière décentralisée.

« *The DAO* » pouvait être considérée comme une organisation de gestion de fonds d'investissement pour différents projets, dont le fonctionnement était basé uniquement sur des *smart contracts*.

L'un des *smart contracts* de « *The DAO* » s'est trouvé être vulnérable à **une faille de sécurité liée à une erreur d'implémentation** [4], faille qui a ensuite été exploitée.

Ce piratage a eu pour conséquence immédiate un effondrement de la cotation de l'Ether, passant sa valeur de 21,5$ à moins de 13$ en quelques heures. Malgré cette baisse de cotation, le montant dérobé représentait toujours plus de 60 millions de US$. Fin juillet, après plusieurs semaines de discussions, la communauté d'Ethereum a réalisé un *hard fork* (opération entraînant la création d'une nouvelle *blockchain* basée sur un historique déjà existant, mais en modifiant certaines des règles de fonctionnement) en vue de récupérer les fonds dérobés.

Il est important de souligner que la faille de sécurité exploitée n'était pas liée à l'implémentation de la *blockchain* Ethereum, mais uniquement à un *smart contract*, conçu par une société tierce. La conception de *smart contracts* et leur développement sont des activités qui doivent être considérées comme critiques et ceux-ci systématiquement soumis à l'audit de spécialistes.

Au final, c'est la décision du *hard fork* par la communauté d'Ethereum qui, aura le plus d'impact à long terme. Cet évènement aura démontré que l'historique et les règles applicables à une *blockchain*, censés être inaltérables, peuvent être modifiés de manière volontaire, si suffisamment de mineurs décident d'associer leurs ressources à la décision (détail important, à l'issue d'un *hard fork*, deux *blockchains* coexistent en parallèle, et la participation à l'une ou l'autre relève du choix de chacun des participants).

3- https://info.shapeshift.io/blog/2016/04/19/timeline-shapeshift-hacking-incident
4-http://www.securityinsider-solucom.fr/2016/06/ethereum-x-dao-retours-sur-lattaque-de_30.html

LES ENJEUX DE LA *BLOCKCHAIN* POUR LES GRANDS COMPTES NE SONT PAS QUE TECHNIQUES

Sous un angle moins sensationnaliste, d'importantes questions restent à aborder pour que la *blockchain* puisse être utilisée efficacement et simplement en dehors d'une population restreinte de *start-ups* spécialisées et enclines à la prise de risques.

La **transparence** intégrale des *blockchains* les plus populaires peut être un obstacle que certaines structures ou organisations jugeront insurmontable. En dehors des réseaux publics, des *blockchains* peuvent être déclinées via des modèles plus restrictifs : soit complètement privées, soit par une délégation de la gestion à des représentants de confiance. Chacune de ces déclinaisons se fait nécessairement sur la base d'un compromis vis-à-vis de la sécurité, ou de la décentralisation, en recréant un nouveau statut de tiers de confiance. Néanmoins, ces *blockchains* privées, ou semi-privées, semblent constituer de bonnes solutions pour partager des informations entre plusieurs organisations. La confiance préalable entre les participants et la *blockchain* (principe et difficulté des opérations de validation des transactions, nombre de transactions par seconde., ...).

Le recours et l'usage d'un service par de multiples parties implique tôt ou tard des divergences entre les parties prenantes. Bien que la *blockchain* impose techniquement par son protocole les règles de son fonctionnement, celle-ci peut être confrontée à des situations trop complexes pour être gérées uniquement par algorithme. L'exemple de l'exploitation d'une faille de sécurité sur « *The DAO* », ou encore les discussions autour de l'évolution du protocole de *Bitcoin* pour augmenter le nombre de transactions possibles par seconde sur cette *blockchain*, sont des exemples qui illustrent la **nécessité de gouvernance**. En l'absence de tels mécanismes, la fragmentation du marché actuel continuera à produire des *blockchains* optimisées pour un usage spécifique et non interopérables les unes avec les autres. Le temps qu'une *blockchain* généraliste dominante soit en mesure de conquérir le marché, le recours à des intermédiaires sera nécessaire pour faire le lien entre les différentes *blockchains*. L'objectif premier de simplification par la désintermédiation est donc un objectif à long terme, dépendant de la standardisation ainsi que de la consolidation de l'écosystème.

Dans la continuité de notre comparaison au monde médical, l'analyse bénéfices/risques de la *blockchain* par rapport aux solutions traditionnelles peut sembler plutôt négative, au regard des éléments exposés. Les expérimentations mettent en lumière un ensemble de freins que la recherche s'applique à adresser.

OBSERVATEUR OU ENTREPRENEUR : QUELLE POSTURE ADOPTER ?

Pour résumer : les principes techniques fondamentaux de la *blockchain* ont démontré leurs capacités à fonctionner à grande échelle, pour **un usage de type monnaie électronique**. Certaines des limites intrinsèques à la *blockchain* ont également montré leurs effets : limite du nombre de transactions par seconde, consommation énergétique, latence... Une partie des expérimentations actuelles vise à identifier des solutions de contournement à ces limites, sans que l'on puisse véritablement présager des résultats. Les autres investissements alimentent un écosystème de *start-ups* chaque jour plus important. **L'objectif étant d'identifier des cas d'usages où la *blockchain* pourrait démontrer des apports concrets, en rupture vis-à-vis des solutions traditionnelles**. C'est sur ce second domaine que les incertitudes sont les plus fortes mais c'est là également que résident le plus d'espoirs et d'attentes, à l'origine de toutes les spéculations.

Pour un CIO, un CTO, ou un Responsable de l'innovation au sein d'un grand compte, trois lignes de conduite sont possibles. Choisir l'une d'entre elles dépend d'un cocktail de paramètres propre à chaque structure :

- Le niveau de maîtrise du management et des opérationnels sur la *blockchain*, et plus globalement sur la capacité à faire le lien entre des sujets métiers et des sujets technologiques ;
- La culture vis-à-vis de l'innovation : l'appétence au risque et les moyens attribués aux activités de R&D ;
- Les ambitions de l'organisation sur son marché : innovateur ou plutôt casanier.

La **première approche** envisageable est la mise en place d'une **veille active**, à la fois sur les plans **métier et technique**, sur son marché, mais également au niveau du **cadre règlementaire**.

En France, en 2016, l'Etat a commencé à fixer un cadre règlementaire aux entreprises et aux institutions. En juin 2016, a eu lieu la première lecture de la loi Sapin II qui devait permettre l'utilisation dans certains cas et sur ordonnance de la *blockchain*. En mars 2016, Emmanuel Macron, alors Ministre de l'économie, de l'industrie et du numérique en France, annonçait une adaptation de la réglementation afin de permettre l'expérimentation de la *blockchain* sur le marché des bons de caisse. Le champ d'application pourrait ensuite être étendu aux titres non cotés.

La **deuxième approche** est celle d'une **expérimentation autour d'un usage décliné d'une monnaie électronique** (voir page ci-contre). Les cas d'applications peuvent être dérivés des usages de la monnaie fiduciaire, de manière dématérialisée, tels que : la création de marchés d'échanges, de registres de transaction, ou encore des déplacements automatiques de fonds, entre plusieurs organisations sans autorité centrale.

- Les solutions sont facilement accessibles pour la réalisation de prototypes de ce type. **La principale difficulté réside dans l'identification d'une problématique métier se prêtant bien à ce type d'opérations**.

Sans surprise, les banques centrales, les régulateurs et de grands groupes bancaires

se sont naturellement emparés du sujet et mènent des expérimentations depuis plusieurs mois :

- **Les membres de la sphère financière** sont les plus actifs et s'organisent pour mutualiser leurs moyens : via le consortium international R3 auquel participent Société Générale, BNP Paribas et Natixis, ou encore le laboratoire d'innovation lancé par la Caisse des dépôts[5] et regroupant AXA, BNP Paribas, *Blockchain* Solutions, le groupe BPCE, Cellabz, le CNAM, CNP Assurances, le Crédit Agricole, Croissance Plus, Paymium, et le Pôle de compétitivité Finance innovation.
- **La Banque de France mène ses expérimentations à travers un projet opérationnel interbancaire**[6] pour échanger et partager des informations, des données avec les différents acteurs du système financier. Le premier domaine d'emploi concerne le partage d'un référentiel de Place, le fichier des Identifiants Créanciers SEPA (ICS).

Enfin, la **troisième approche**, la plus complexe, est celle d'une **expérimentation de la *blockchain*** en tant **que solution technique d'un nouveau mode de fonctionnement**, ou d'un nouveau service.

Pour être en mesure d'identifier un tel cas d'usage, nécessairement innovant, notre conviction est qu'il faut :

- Mettre en œuvre une démarche d'innovation participative impliquant à la fois des responsables métiers et techniques;
- Disposer d'une fine compréhension à la fois des architectures traditionnelles, mais également des mécanismes internes de fonctionnement de la *blockchain*, afin de s'assurer de l'apport réel de la solution.

Tout l'enjeu est de **trouver le bon mécanisme de contrôle, décentralisé, avant l'enregistrement de nouvelles transactions, ou données, au registre.**

ÉCLAIRAGE

POURQUOI LES MONNAIES ÉLECTRONIQUES OFFRENT-ELLES UN CAS D'USAGE ADAPTÉ À L'UTILISATION DE LA *BLOCKCHAIN* ?

Indépendamment des circonstances de création de la première *blockchain* et de son adhérence naturelle avec Bitcoin, les monnaies électroniques offrent certaines caractéristiques qui permettent à la *blockchain* d'offrir une robustesse particulière pour ce domaine d'application.

Pour qu'un échange de monnaie électronique puisse être considéré comme valide, il faut que l'émetteur dispose de la somme qu'il souhaite voir créditée. Le caractère public du registre de l'ensemble des transactions permet à tous les participants le contrôle, autonome, de la validité d'un échange. Chaque nouvelle transaction enregistrée dans la *blockchain* a donc été validée, et reste vérifiable, par tous, de manière transparente et décentralisée.

Pour une monnaie électronique : le mécanisme de contrôle de la validité d'une transaction se base sur les seules données présentes dans la *blockchain*.

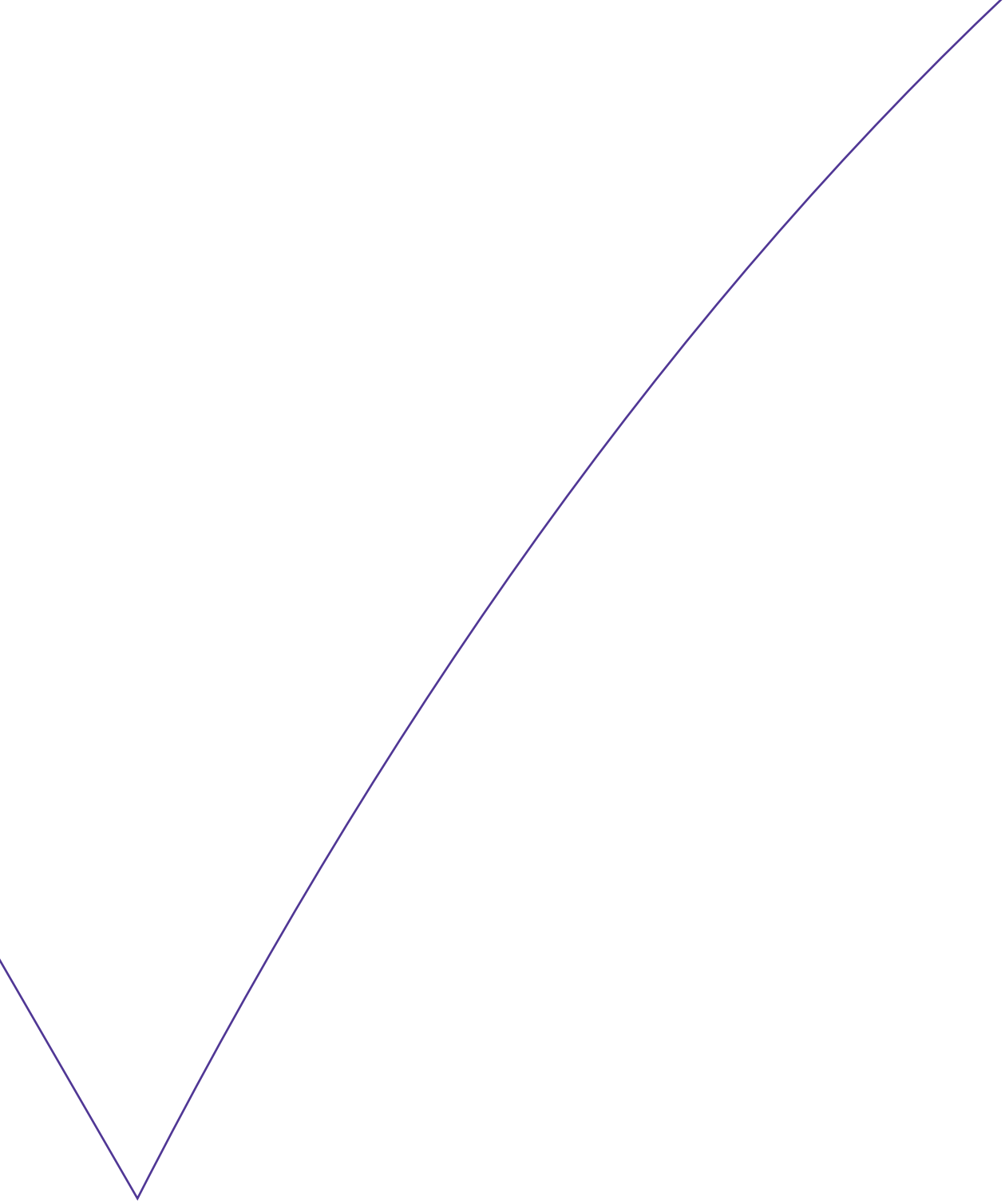
Pour conclure notre parabole médicale : si la Blockchain était un médicament, au regard des éléments partagés, l'Agence Nationale de Sécurité du Médicament et des produits de santé pourrait conclure :

- Que la blockchain est une solution visant à adresser la pathologie de la « dépense double », créée par l'apparition des monnaies électroniques et dont le traitement actuel le plus efficace est celui du recours à un « tiers de confiance » (établissements de paiement : banques, Paypal, etc.).
- Pour cette pathologie le médicament est efficace, in vivo. Les résultats ont été démontré par une phase de tests à grande échelle réussie : Bitcoin.
- Pour d'autres pathologies proches affectant des transactions entre individus, la reproductibilité des effets bénéfiques de la blockchain reste encore à démontrer. Pour ces affections, l'analyse bénéfices/risques du recours à la blockchain par rapport à l'utilisation d'un simple « tiers de confiance » peut sembler pour le moment plutôt négative.

Pour toutes ces raisons le médicament ne peut être considéré à l'heure actuelle comme éligible à une autorisation de mise sur le marché et doit encore faire l'objet d'analyses et d'études complémentaires. Toutefois son utilisation par des spécialistes est autorisée pour traiter certains symptômes causés par le recours aux « tiers de confiance » associé à l'usage de monnaies électroniques.

Cette publication sera complétée par une autre plus technique, à destination d'architectes, responsables d'étude, ou de R&D souhaitant approfondir le sujet en vue de réaliser des expérimentations au sein de leur organisation, ou encore d'évaluer finement les bénéfices/risques du recours à la blockchain par rapport à d'autres solutions traditionnelles.

5- http://www.caissedesdepots.fr/lancement-dune-initiative-de-place-sur-la-blockchain-avec-11-partenaires
6- https://www.banque-france.fr/sites/default/files/medias/documents/communique-de-presse_2016-12-15_la-banque-de-france-mene-une-experimentation-de-blockchain-interbancaire.pdf



WAVESTONE

www.wavestone.com

Wavestone est un cabinet de conseil, issu du rapprochement de Solucom et des activités européennes de Kurt Salmon (hors consulting dans les secteurs retail & consumer goods). Il figure parmi les leaders indépendants du conseil en Europe.

La mission de Wavestone est d'éclairer et guider ses clients dans leurs décisions les plus stratégiques en s'appuyant sur une triple expertise fonctionnelle, sectorielle et technologique.