Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ambassade de France à Washington
Service pour la Science et la Technologie
4101 Reservoir Road NW, Washington, DC 20007
Tél. : +1 202 944 6246
Mail : info@france-science.org
URL : http://france-science.org

Domaine : Technologies de l'Information et de la Communication, Sécurité
Document : Rapport d'Ambassade / Ambassade de **France, Washington DC**
Titre : Au- delà du *Bitcoin : la révolution par la technologie Blockchain*?
Auteur(s) : Hervé Martin (attache-it@ambascience-usa.org)
Date : Février 2018

Mots-clés :	Blockchain, Sécurité
Résumé :	*En signant le 12 Décembre, le National Defense Authorization Act (NDAA) qui incite les différentes agences gouvernementales à développer des systèmes basés sur le blockchain, le président Donald Trump confirme l'intérêt croissant des Etats-Unis pour cette technologie popularisée par le développement du Bitcoin et qui apparaît comme une innovation de rupture. Cybersécurité, cryptographie sont au cœur de ces technologies qui ont le potentiel pour révolutionner de nombreux domaines. Cette technologie suscite un fort engouement aux Etats-Unis et provoque une dynamique très riche tant en recherche que dans les milieux socio-economiques. Cette note souligne les raisons qui motivent cet intérêt et donne quelques exemples de développement des applications de type Blockchain dans ce pays.*

1. Pourquoi la technologie *blockchain* ?

La technologie *blockchain* se situe au croisement de différentes expertises des sciences du numérique issues notamment de la cryptographie et de la cybersécurité permettant le partage sécurisé et distribué de données via Internet.

Cette technologie a été initialement rendue populaire en 2008 par le développement de crypto-monnaies telle que le *Bitcoin* qui, en s'appuyant sur la technologie *Blockchain*, permettent d'effectuer des transactions de pair à pair sans avoir à recourir à une institution financière ou à tout autre intermédiaire de confiance. Techniquement, la chaine de blocs permet le stockage et la transmission d'informations de façon distribuée (i.e. sans organe de contrôle par un serveur central) en petits paquets, dans des blocs cryptés et reliés entre eux par une chaine. Ainsi, les éléments constitutifs de la transaction (portefeuilles impliqués, nature et montant de la transaction) sont enregistrés dans un registre (*ledger*) stocké dans un des blocs de la *blockchain* et partagé par l'ensemble des membres de la communauté.

Au delà du *Bitcoin*, cette technologie suscite un intérêt pour toute une pléiade d'applications susceptibles de bénéficier de tout ou partie des propriétés ou caractéristiques associées à la technologie du *blockchain* :

• **Authentification** : tous les éléments inscrits dans un bloc sont codés et peuvent être authentifiés de manière unique. Il est en effet possible de représenter de manière quasi-unique un document par une fonction de hachage cryptographique (clé de *Hash*) et de référencer ce document par cette clé sans diffuser le document lui-même. La fonction de hachage associe une image de taille fixe (que l'on appelle la clé) à une donnée de taille arbitraire et a pour propriété essentielle d'être pratiquement impossible à inverser. En enregistrant cette clé dans un bloc, on peut, par exemple, prouver l'appartenance d'un document (texte, musique, film, ...) dans une base de données à un instant donné sans donner l'accès au document lui-même.
• **Pérennité** : les blocs contenant les informations ont a priori une durée de vie illimitée. Il est donc possible de garantir la pérennité d'une information enregistrée dans un bloc, c'est à dire de stocker indéfiniment les informations. Cela peut permettre par exemple de vérifier dans le temps, l'historique d'une série de transactions ou la validité d'un document précédemment enregistré dans un bloc.
• **Décentralisation** : la technologie *blockchain* s'abstrait de toute gestion centralisée par un serveur central. Les différents blocs du *blockchain* sont répliqués et partagés par l'ensemble des participants. La gestion des blocs est donc entièrement décentralisée et l'ajout d'information ne se fait que par consensus. Cette technologie permet donc de modéliser des environnements fortement distribués.
• **Robustesse** : la technologie est basée sur différents mécanismes robustes de copies multiples et de validation (preuve de travail, preuve d'enjeu) qui font que les blocs contenant les informations sont quasi **infalsifiables**. L'ajout d'un nouveau bloc est une opération complexe et coûteuse en temps et il est quasiment impossible de modifier, ou supprimer des informations inscrites dans un bloc. Alors que la cybersécurité devient un enjeu essentiel pour les entreprises, les personnes et les gouvernements, la confiance sur la validité d'une information est un élément essentiel de tout système d'informations pour faire face aux risques de piratages ou autres actes malveillants.
• **Dynamique** : la technologie initiale ne cesse d'évoluer et certaines plateformes telle que Ethereum apparue en 2015 intègrent la possibilité d'associer des programmes simples ou des contrats logiciels (**smart contracts**) à l'intérieur de la transaction. Cette possibilité démultiplie les possibilités d'applications en permettant de coder dans un petit programme les termes d'une transaction. Il devient par exemple possible d'exprimer les conditions d'exécution d'une transaction impliquant différents acteurs, à l'instar des solutions proposées pour le partage d'énergies renouvelables ou des solutions de financement participatif.

2. Quels sont les principaux domaines utilisant cette technologie aux Etas-Unis ?

Beaucoup d'applications nécessitent de partager des données de manière sécurisée avec un certain niveau de confidentialité dans des environnements distribués, robustes et dynamiques. Il n'est donc pas surprenant que la technologie *blockchain* trouve un écho dans de nombreux domaines.

Domaine de la finance

Les premières applications dans la finance ont suscité un intérêt particulier aux Etats-Unis (i) en ce qui concerne la régulation ; (ii) pour les petites et moyennes entreprises ; (iii) pour le secteur de l'assurance ; ou encore (iv) pour les infrastructures de marché. On estime à 1,4 milliards de dollars les sommes investies dans ce domaine en 2016[1].

Concernant la réglementation, l'Etat du Delaware, où beaucoup de sociétés sont fiscalement domiciliées, a lancé en août 2017 le projet "Delaware blockchain initiative" pour le suivi (*tracking*) des mouvements d'actions tandis que l'Etat du Nevada a reconnu légalement en juin 2017 les registres distribués et a empêché leur taxation ainsi que celle des *smart contracts*.

Cette technologie intéresse également les PME/PMI qui font du commerce à l'international dans la mesure où elle permet de limiter voire de supprimer les redondances administratives par le maintien d'un unique registre distribué. La suppression de tiers de confiance pour effectuer les transactions financières permet également d'envisager de s'exonérer de certains frais de commission transfrontalière et de transaction.

Par ailleurs, l'automatisation permise par les contrats logiciels pourrait offrir des opportunités pour le secteur de l'assurance et réassurance. Ainsi, dans une étude de 2016, PriceWaterhouse Coopers estime que cette technologie pourrait abaisser les coûts pour la réassurance de montants de l'ordre de 5 à 10 Mrd USD.

Enfin, le domaine de la compensation (*clearing)* et de la règlement-livraison (*settlement*) pourrait également subir des transformations majeures à la suite d'une adoption large de la technologie *blockchain* par les différents acteurs. Dans un rapport de 2017, Accenture estime à 10 Mrd USD les économies possibles pour les plus grandes banques d'investissement.

Domaine de la cybersécurité

La cybersécurité est un domaine stratégique pour toutes les entreprises et administrations qui utilisent l'Internet pour proposer des services ou objets connectés (IoT). Outre les grandes entreprises du secteur comme IBM, Cisco, Northrop Grumman et Lockheed Martin, de nombreuses start-up développent des solutions fondées sur la technologie *blockchain* pour relever différents défis liés à la cybersécurité.

- Le projet Certcoin du MIT est un excellent exemple de possibilité offerte par le *blockchain* pour permettre à une organisation de garantir des propriétés essentielles comme la confidentialité, l'intégrité et l'authenticité.
- Le projet Blockstack[2] à Princeton propose une solution basée sur la technologie *blockchain* pour redonner aux utilisateurs le contrôle de leurs données.

[1] https://www.cryptocoinsnews.com/pwc-expert-1-4-billion-invested-blockchain-2016/.

[2] http://reason.com/reasontv/2017/06/22/blockstack-bitcoin-blockchain-internet

- La start-up Nebulis[3] propose une solution basée sur la *blockchain* pour gérer les noms de domaine (DNS) et éviter les attaques par déni de service (DoS) comme celle qui a bloqué les accès à Paypal, Netflix et Twitter en octobre 2016.

Dans le domaine public, les différents Départements du gouvernement américain s'intéressent également à cette technologie et ont lancé différentes initiatives.

- Le Département de la sécurité intérieure (Homeland Security - DHS) s'intéresse à la pertinence des propriétés de sécurité et de confidentialité proposées par cette technologie. En 2016, via les programmes SBIR[4], le DHS a ainsi financé 600 000 USD de bourses à des entreprises travaillant sur des applications *blockchain* pour le gouvernement. En 2017, l'entreprise Evernym a reçu 794 000 USD du DHS pour concevoir et développer des systèmes de gestion de clés décentralisés.
- Pour accélérer le développement de systèmes robustes moins sensibles aux cyber attaques, le Département de l'énergie (DOE) s'intéresse aussi au *blockchain*. Un projet de plusieurs millions de dollars a été lancé pour financer un consortium mêlant des industries comme Guardtime et Siemens et des académiques avec Washington State University pour développer des technologies de cybersécurité basées sur la *blockchain*.
- Le Département de la défense (DoD) étudie également l'utilisation de la technologie *blockchain* pour protéger les infrastructures militaires. La DARPA a ainsi octroyé un financement de 1,8 Mio USD à la société Galois pour évaluer la solution *blockchain*.

Les acteurs institutionnels de la recherche américaine tels que la National Science Foundation (NSF) et le National Institute of Standards and Technology (NIST) s'intéressent également de près à cette technologie. La NSF a lancé un programme (*Cybersecurity Innovation for Cyberinfrastructure*) de 8 Mio USD sur la sécurité en s'appuyant notamment sur la technologie *blockchain*. Des équipes du NIST étudient différents aspects de cette technologie (architecture, taxonomie et primitives cryptographiques) et analysent les cas d'utilisation afin d'étudier la pertinence de standards dans ce domaine. Côté universités, le Massachusetts Institute of Technology (MIT), conscient que cette technologie a la potentialité d'impacter la société dans son ensemble, a décidé de promouvoir au sein de son Media Lab une initiative dédiée, nommée "*Digital Currency Initiative*" pour en étudier les risques et les opportunités ainsi que les problématiques éthiques associées[5].

Parmi toutes ces applications, la sécurité de l'internet des objets (internet of Things) est certainement l'un des domaines les plus prometteurs car la très haute distribution des différents appareils connectés nécessite de repenser les politiques de sécurité actuelles et la *blockchain* présente de nombreux avantages[6].

[3] http://www.the-blockchain.com/2016/12/06/blockchain-startup-nebulis-set-prevent-ddos-attacks-dns-servers/
[4] https://www.sbir.gov
[5] http://dci.mit.edu
[6] https://hbr.org/sponsored/2017/10/how-blockchain-will-accelerate-business-performance-and-power-the-smart-economy

Domaine de l'énergie

La technologie *blockchain* possède également quelques atouts pour les systèmes de distribution d'énergie. Elle peut permettre de satisfaire les besoins d'un marché de plus en plus distribué où certains utilisateurs produisent trop alors que d'autres observent des pics de demandes.

Dès 2014, la cryptomonnaie Solarcoin[7] a été créé pour faciliter le développement de l'énergie solaire. Cette tendance continue avec notamment la start-up Sun Exchange qui a levé 1,6 Mio USD pour lancer une plateforme collaborative d'échange d'énergie solaire.

A New York, la start-up LO3 Energy[8] en collaboration avec Siemens a lancé le projet pilote Brooklyn Microgrid qui permet aux habitants du quartier de choisir et partager leur énergie. Un des objectifs des initiateurs du projet est d'offrir une meilleure résilience aux aléas climatiques en installant des batteries pouvant stocker l'énergie produite localement. Ce projet s'inscrit dans la stratégie de New York pour l'énergie baptisée « Reforming The Energy Vision » qui vise une production de 50% de l'énergie à partir de sources renouvelables en 2030.

D'autres start-up américaines se sont lancées sur ce créneau comme à Seattle où Drift a levé 2,1 Mio USD en 2017 et s'appuie sur différentes technologies dont la *blockchain* et l'apprentissage automatique (Machine Learning) pour la vente d'énergie.

La start-up Grid+ a levé 29 Mio USD pour se lancer sur ce marché au Texas. Enfin, la fondation Energy Web Foundation fondée par Grid Singularity et le Rocky Mountain Institute promeut une approche open source basée sur la *blockchain* pour le marché de l'électricité. Cette initiative est soutenue par plusieurs grandes sociétés du domaine (Shell, Statoil, Tepco, ...) et le français ENGIE qui ont attribué 2,5 Mio USD à la fondation. L'objectif est de pouvoir proposer un logiciel libre à l'horizon 2019-2020.

Domaine du suivi et de la localisation (tracking)

Le tracking est le fait de pouvoir suivre et localiser un objet ou une être vivant (personne, animal). La technologie *blockchain* facilite et sécurise le processus de traçabilité en permettant l'horodatage, la localisation et le suivi tout en interdisant à quiconque de modifier ou supprimer des informations.

La technologie *blockchain* reçoit donc logiquement un engouement fort dans le domaine des transports de marchandises ou les technologies d'identification type RFID s'associent naturellement avec la *blockchain*. Aux Etats-Unis, Walmart a mené des expérimentations sur la *blockchain* notamment pour la traçabilité du porc chinois et des mangues mexicaines. Walmart vient de signer avec neuf géants de l'agro-alimentaire un partenariat avec IBM pour développer des services basés sur la *blockchain* et assurer de manière sécurisée la traçabilité des produits.

Plusieurs start-up se sont lancées dans ce créneau dont FACTOM[9] basée à Austin qui développe des solutions *blockchain* sur la conformité, l'identité, la transparence et la sécurité. La société californienne Mojix, spécialiste des technologies RFID, s'est associée avec Microsoft pour développer des solutions associant *blockchain* et RFID.

[7] https://solarcoin.org
[8] https://lo3energy.com

[9] https://www.factom.com

Vers une standardisation

Côté standardisation, l'International Organization for Standardization (ISO) étudie la blockchain avec la mise en place d'un groupe de travail spécifique ISO/TC 30710. L'initiative *Enterprise Ethereum Alliance* montre la volonté de différents acteurs de l'industrie, dont *Microsoft*, à coordonner leurs efforts pour voir l'émergence de solutions ouvertes et interopérables.

3. Conclusion

Ce rapport est loin d'être exhaustif et la technologie *blockchain* touche également beaucoup d'autres domaines tels que l'identité numérique avec le programme ID2020 des Nations Unies et la santé avec le projet MedRec du MIT[11]. La plupart des grandes universités de recherche américaines ont des groupes ou projets spécialisés sur ce sujet comme à Berkeley[12] ou à Harvard avec l'étude des effets du *blockchain* sur l'économie digitale[13].

Le potentiel de la technologie blockchain pour favoriser des innovations de rupture dans nos sociétés est remarquable et devrait inciter de nombreux acteurs (individus, industries, gouvernements) à lancer rapidement des expérimentations avant un large passage à l'échelle de cette technologie.

On observe de nombreuses initiatives en France avec la mise en place d'un groupe de travail spécifique par France stratégie, la publication d'un livre blanc par le MEDEF et de nombreuses expérimentations dans les collectivités locales comme à Lorient et par des start-up dans différents domaines tel que l'énergie avec la start-up Evolution Energie, les systèmes de gouvernance avec la start-up 97 ou la santé avec par exemple Kidner qui cherche à faciliter les dons croisés de reins.

Parmi les critiques souvent faites à cette technologie, on retrouve notamment l'idée que le maintien des registres qui utilisent des méthodes de validation par preuve de travail (*proof-of-work*) est coûteux en énergie. Dans le cas du *Bitcoin*, Morgan Stanley a estimé que le réseau *blockchain* du *Bitcoin* utilisait l'équivalent en électricité de deux millions de foyers américains.

D'autres défis technologiques et scientifiques restent à résoudre pour envisager un développement massif de la technologie. Parmi ces points, certains ont trait à la protection de la vie privée, le droit à l'oubli ou la gestion des incidents dans un environnement *blockchain*.

Il est donc probable que l'utilisation de la technologie *blockchain* se réalise dans un premier temps sur des secteurs particuliers où ces limites ne sont pas rédhibitoires. De manière plus générale, l'engouement actuel aux Etats-Unis démontre le besoin de rétablir la confiance avec moins de centralisation et un meilleur niveau de sécurité et des mécanismes de traçabilité dans le monde du numérique. Cette tendance devrait se poursuivre à l'heure où de nombreux secteurs (transport, communication, santé, énergie, ...) dépendent fortement des Technologies du Numérique. A moyen terme, la technologie blockchain pourrait également avoir un impact important sur les géants du Web (Google, Facebook, Amazon, ...) dont le *business model* est basé sur la centralisation.

[10] https://www.iso.org/committee/6266604.html
[11] http://dci.mit.edu/assets/papers/eckblaw.pdf
[12] http://scet.berkeley.edu/blockchain-lab/
[13] http://www.hbs.edu/faculty/Pages/item.aspx?num=52100