PROTECTION DE L'ENTREPRISE NUMÉRIQUE

IRT-SYSTEMX

Cybersécurité

La blockchain :

Quelques considérations autour de sa sécurité

Programme « Internet de Confiance »

VERSION	NOM	DATE	Modification
ISX-IC-EIC-sec-blockchain-v1	Philippe WOLF	04/04/2018	Version initiale
ISX-IC-EIC-sec-blockchain-v2	Philippe WOLF	23/04/2018	révisions
ISX-IC-EIC-sec-blockchain-v3	Philippe WOLF	24/07/2018	compléments

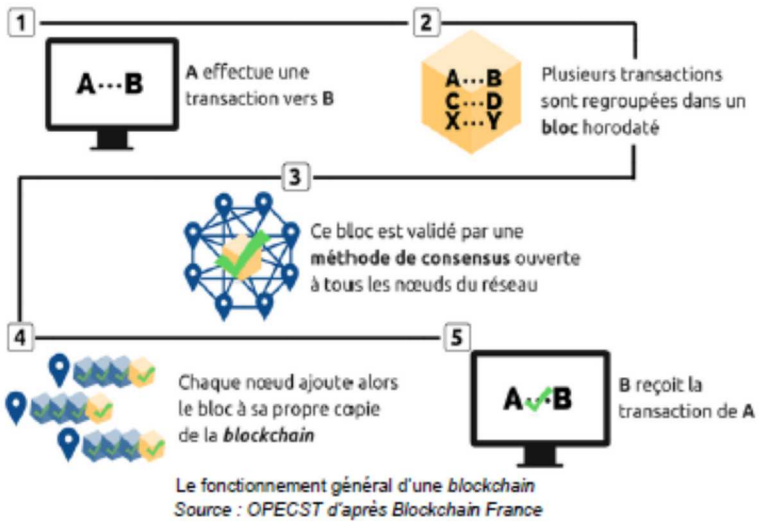
Sommaire

Ce document propose quelques considérations sur **l'usage de la technologie blockchain en cybersécurité** et par conséquence aussi sur **sa sécurité intrinsèque**. Son objectif est de :

1. Comprendre, au-delà du buzz médiatique, où se situe sa nouveauté ;
2. dépasser l'usage premier pour la crypto-monnaie ;
3. appréhender la sécurité de la blockchain. Comme toute technologie de sécurité, elle est attaquée dans toutes ses dimensions ;
4. souligner quelques risques inhérents à toute technologie numérique ;
5. proposer quelques applications possibles à la cybersécurité et sa gestion ;
6. se préoccuper, si possible, d'un minage plus écologique ;
7. distinguer quelques pistes pour ses évolutions futures.

Il ne s'agit, en aucun cas, d'un cours sur la blockchain. Des documents innombrables (articles, présentations, films, livres) sont accessibles librement. Nous essayons d'en lister quelques-uns. Notre analyse n'exploite que des documents publics dont nous donnons systématiquement les liens.

Une bonne synthèse en français est disponible sous la forme d'une fiche parlementaire[1] dont les références constituent, par ailleurs, l'information principale.



Le fonctionnement général d'une *blockchain*
Source : OPECST d'après Blockchain France

Un autre rapport en anglais de la MITRE Corporation[2] (organisation US à but non lucratif travaillant pour l'intérêt public) fait une très bonne synthèse des technologies en jeu. Mais il ne répond pas aux objectifs qu'il s'est fixé de comparer les meilleures solutions adaptées à des usages gouvernementaux qui restent vagues. Sa conclusion est, de ce fait, prudente :

> *Si l'on se tourne davantage vers les blockchains à autorisations (ou privées) pour moderniser les applications traditionnelles, plusieurs exigences doivent être prises en compte. Par exemple, la protection des données personnelles et la confidentialité sur la chaîne de blocs, l'évolutivité des*

[1] Voir http://www.senat.fr/fileadmin/Fichiers/Images/opecst/quatre_pages/OPECST_2018_0020_note_blockchain.pdf

[2] Mitre - Blockchain Technology for Government, https://www.mitre.org/sites/default/files/publications/blockchain-technology-for-government-18-1069.pdf

transactions et la connectivité blockchain-à-blockchain. Alors que des recherches actives sont en cours dans ces domaines dans plusieurs communautés open-source, les blockchains privées doivent évoluer pour répondre pleinement aux besoins des utilisateurs gouvernementaux.

Le traitement médiatique de la blockchain souffre d'une incompréhension générale des mécanismes cryptographiques mis en jeu[3]. Là aussi, les explications simplificatrices font florès. Il s'agit cependant de ne pas négliger l'effort de compréhension mathématique nécessaire pour en apprécier les limites et ne pas prêter à la blockchain des vertus inatteignables. Le numérique demeure encore, même avec l'IA triomphante, un artefact de la « vie réelle ».

Tous les exemples et illustrations seront pris sur les 2 chaînes les plus actives du moment :

Naissance	Monnaie	Créateur	Hachage	Signature	langage(s)	Minage	Remarques
2009	Bitcoin	Satoshi Nakamoto Pseudo collectif… Nick Szabo ?	SHA-256	ECDSA Elliptic Curve Digital Signature Algorithm courbe secp256k1	C++	PoW	La première crypto-monnaie décentralisée. La plus populaire avec la plus grande capitalisation.
2015	Ether ou "Ethereum"	Vitalik Buterin	Ethash (plus ASIC résistant?) Keccak-256 -512 différent de SHA3	ECDSA SECP-256k1	C++, Go	PoW	Support des smart contracts (langage Turing-complet)

Le site https://en.wikipedia.org/wiki/List_of_cryptocurrencies avec d'autres[4], liste la floraison des solutions en développement. Peu d'entre elles dépasseront le stade de la « pompe à phynances » du père Ubu. La bulle des startups Blockchain éclatera doucement…

Il s'agira de suivre plus particulièrement l'initiative *hyperledger* de la fondation linux qui produit aujourd'hui beaucoup de papier mais encore peu de services concrets (liens forts avec *ethereum*)[5].

Les questions monétaires ne seront pas abordées ici : en octobre 2017, le marché du Bitcoin représente 41 milliards de $ et l'ensemble des crypto-monnaies 80 milliards de dollars. Ce qui est absolument minuscule à côté de la masse gigantesque que représente l'ensemble des monnaies et des actifs en circulation, 83 600 milliards de dollars. Mais le boursicotage s'en est emparé ce qui explique les fluctuations actuelles et probablement futures des cours.

[3] Exemple, parmi mille, dans http://www.itespresso.fr/blockchains-rgpd-186906.html : « à toutes les transactions enregistrées sont associées des clés publiques (hashs), chiffrées dans l'absolu, mais susceptibles, par recoupements, de permettre des identifications indirectes. »

[4] Voir aussi https://cryptomining24.net/list-of-cryptocurrencies/ ou https://en.bitcoin.it/wiki/Comparison_of_cryptocurrencies

[5] Voir https://www.hyperledger.org/projects

19/04/2018	Bitcoin	Ethereum	Ripple	Bitcoin Cash	Litecoin	Monero
Total	16 973 322 BTC	98 910 988 ETH	39 122 794 968 XRP	17 068 504 BCH	56 154 283 LTC	15 944 927 XMR
Valeur	1 BTC = $ 8 200.3	1 ETH = $ 533.16	1 XRP = $ 0.723	1 BCH = $ 892.81	1 LTC = $ 140.87	1 XMR = $ 232.21
Capitalisation	$139 186 383 731	$52 734 932 795	$28 292 395 057	$15 238 892 092	$7 910 175 541	$3 702 532 274
Transactions par heure	8599	29724	30897	788	1226	276
Transactions par seconde	2,39	8,26	8,58	0,22	0,34	0,08

Principales crypto-monnaies convertibles (https://bitinfocharts.com/)

Quelques autres données sur ces 2 chaînes :

- Bitcoin
  - https://blockchain.info/fr/charts)
- Ethereum
  - https://www.coindesk.com/bitcoin-miners-ethereum/
  - https://github.com/ethereum/go-ethereum/
- Comparaison des cours
  - https://www.coingecko.com/fr
- La réponse d'ethereum aux « mythes »
  - https://en.bitcoin.it/wiki/Myths
  - https://www.ethereum-france.com/comprendre-la-blockchain-ethereum-article-1-bitcoin-premiere-implementation-de-la-blockchain-12/
  - https://www.ethereum-france.com/comprendre-la-blockchain-ethereum-introduction/
- Les industriels dans hyperledger
  - https://www.hyperledger.org/members

L'ensemble des données sur les chaînes publiques sont accessibles principalement à travers des sites dont on ne comprend pas toujours les liens respectifs ni la finalité.

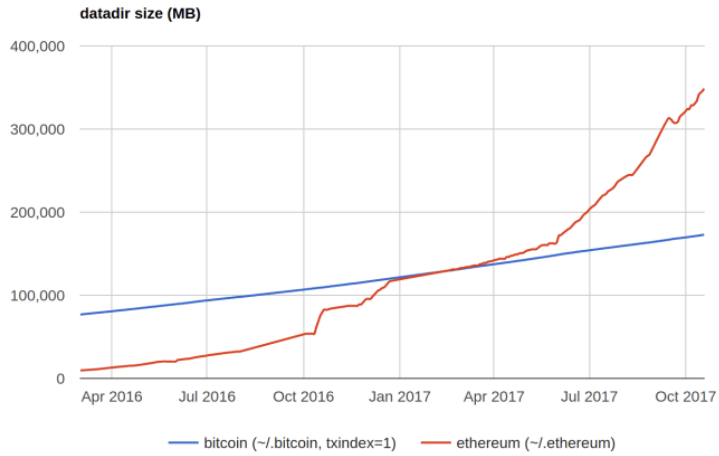
Il n'existe pas de programmes locaux autonomes, libres et faciles d'accès capables de traiter intelligemment la sauvegarde locale de la blockchain. Tout fonctionne par API ou en ligne.

Les logiciels locaux de gestion de portefeuille sont assez pauvres en fonctionnalités : exemple *armory* (un des programmes Bitcoin les plus robustes).

La taille actuelle de la blockchain Bitcoin (190 Goctets) ne facilite pas son exploration. La plupart des études que nous citerons exploitent des outils académiques *ad hoc* dont l'accès n'est guère partagé. La transparence n'est pas encore à la portée de tous.

Les chaînes de blocs grandissent à des rythmes différents. Pour ethereum, il existe 3 modes de synchronisation. Dans le mode Fast Sync, elle fait 65 GB le 16 avril 2018[6].

[6] Voir https://etherscan.io/chart2/chaindatasizefast



La crainte d'une chaîne ethereum bientôt à 1 TB trouve des réponses dans des traitements de synchronisation qui ne nécessitent pas une copie locale de la chaîne complète[7].

La taille future des blockchain bloquera très vite les capacités locales de traitement. Des nœuds dédiés seront nécessaires.

Les chaînes de blocs peuvent également être encombrées par des données ludiques.

[7] Voir https://dev.to/5chdn/the-ethereum-blockchain-size-will-not-exceed-1tb-anytime-soon-58a

Table des matières

Généralités

Le Livre Blanc Blockchain du Pôle Systematic[8] synthétise les éléments essentiels.

L'approche Blockchain repose sur trois principes fondateurs :

- *Toutes les transactions sont enregistrées dans un référentiel de confiance réparti (grand livre distribué) contrôlé par « le public ».*
- *Le contrôle vient de l'hypothèse que les bons sont plus « puissants » que les mauvais (en Bitcoin, le « pouvoir » est la puissance de calcul des « mineurs »).*
- *La confiance vient du fait que le contenu du référentiel est publiquement validé par « le public lui-même », et que cela évite à tout le monde de tout valider.*

Trois concepts structurants :

- *les devises cryptées,*
- *les Smart-Contrats,*
- *DAO (data access object). Un* ***objet d'accès aux données*** *est un patron de conception (c'est-à-dire un modèle pour concevoir une solution) utilisé dans les architectures logicielles objet.*

4 domaines d'application :

- *la finance (traitement des flux de transaction, gestion d'actifs, conformité, etc.) ;*
- *le secteur public avec amélioration de la transparence (fiscalité, protection sociale, lutte contre la corruption) et réduction des coûts ;*
- *le secteur juridique (vérification des contrats et des droits de propriété, exécution automatique des contrats, etc.) ;*
- *l'Internet des objets (équipement d'interopérabilité, etc.).*

Le Groupe de Travail « *Confiance numérique et Sécurité* », met en garde contre une confiance aveugle dans sa sécurité

La technologie Blockchain est généralement considérée comme une technologie intrinsèquement sécurisée. Cependant, il n'existe aucune preuve formelle que les trois propriétés de sécurité classiques (confidentialité, intégrité et disponibilité) sont appliquées par les technologies Blockchain. La technologie Blockchain, dans sa version bitcoin, offre de grandes fonctionnalités de disponibilité et de confidentialité mais une intégrité fragile. En effet, alors que les transactions sont immuables une fois validées dans la Blockchain (ne prenant pas en compte l'attaque à double dépense), la véracité de chaque transaction au sein des blocs ne dépend que de ceux qui contrôlent les clés privées de ces comptes; clés utilisées pour signer des transactions. Cette limitation n'est pas évidente puisque les clients sont installés dans des appareils personnels tels que les téléphones intelligents ou les ordinateurs portables (donc surveillés pendant tout le temps), mais également dans l'IoT, les appareils non gérés et non supervisés exposés à des vols de clés ou à des vols d'informations.

[8] Blockchain : Myth or Reality ?, https://systematic-paris-region.org/wp-content/uploads/2017/07/Systematic-LB-Blockchain-HD.pdf

Commentaire :

Aujourd'hui, le prix à payer de la décentralisation, c'est que la possession de cryptomonnaie ou d'un compte d'accès repose souvent sur la maîtrise de clé(s) privée(s) d'accès à un portefeuille logiciel par les clients[9]. La fragilité intrinsèque est dans l'incapacité, comme pour les mots de passe, pour les usagers à se discipliner pour appliquer quotidiennement de bonnes pratiques de gestion de leurs secrets numériques[10]. L'usager ne protège pas suffisamment ses clés ou n'a pas les outils pour le faire (en particulier sur smartphone). La carte à puces avec son code porteur s'était généralisée autour de ce constat de carence.

L'utilisation de « token matériels » pour un usage en milieu industriel de la blockchain est une question essentielle. On en revient toujours à **l'authentification**, comme fonction de sécurité initiale et principale. Les échecs répétés de la signature numérique sont d'abord liés à des facteurs humains…

On peut également s'interroger sur la sécurité réelle d'un portefeuille matériel de cryptomonnaies (clé USB), marché qui a du mal à se développer probablement par la difficulté de mise en œuvre et l'absence de certification de sécurité.

[9] Même si des acteurs privés proposent déjà de gérer vos clés.

[10] Comme http://www.cnewsmatin.fr/monde/2017-12-05/il-jette-sa-cle-usb-avec-90-millions-de-dollars-en-bitcoin-dessus-770428

7 mythes

La blockchain entretient de nombreux mythes. En voici quelques-uns (traduction approximative de l'article ci-après). Nous les reprendrons dans certains chapitres.

Références : https://www.entrepreneur.com/article/309896

Mythe 1: C'est très évolutif,

Les déploiements de blockchain ne sont pas vraiment évolutifs par rapport aux méthodes de transaction conventionnelles (basées sur un serveur central) et les temps de transaction sont actuellement lents (pour bitcoin, quelques transactions par seconde). Ils ne sont évolutifs que pour certains types de transactions, de petites charges utiles et jusqu'à certaines limites. Vous ne pouvez pas simplement empiler des informations sur la blockchain. *Voir chapitre cas d'usages*.

Mythe 2: C'est sécurisé.

Alors que la blockchain est basée sur des standards cryptographiques, les méthodes pour assurer la confidentialité sont entièrement en dehors des normes et des implémentations de la blockchain. L'intégration de Blockchain n'est vraiment comprise et vérifiable que par des experts en cryptographie. Mais, c'est la responsabilité de chaque exécutant d'assurer la sécurité, de sorte que cela est géré en grande partie comme dans le vieux monde de la gestion des transactions financières. *Voir chapitre attaques.*

Mythe 3: C'est digne de confiance.

Blockchain assure l'intégrité des transactions et des informations, sinon rien de ce qui est stocké dans la blockchain n'est intrinsèquement digne de confiance. Vous devez assurer la fiabilité en vous assurant que les parties qui stockent des faits dans la blockchain sont dignes de confiance et que les faits sont véridiques - tout comme vous le feriez en dehors de la blockchain. Un modèle de gouvernance permet à plusieurs parties de prendre la responsabilité conjointe d'une infrastructure, tandis qu'un accès sécurisé est nécessaire pour stocker les faits dans la chaîne de blocs. *Voir chapitre blockchains privées ?*

Mythe 4: Vous pouvez mettre n'importe quoi dans la blockchain.

Blockchain est un protocole exprimé en code et n'est pas défini en termes de standard. Il n'y a pas d'organisme de normalisation pour fournir des règles ou des directives d'application sanctionnées.

Généralement, vous ne pouvez traiter que de petites charges utiles, et vous avez toujours besoin de normes convenues entre tous les participants pour que chacun puisse comprendre ce qui est stocké. Dans la plupart des cas, vous verrez un schéma de suppositions selon lesquelles blockchain est une solution au niveau de l'application, qui permettra l'interopérabilité entre les produits qui ne sont pas encore réels, et que les principales plateformes d'aujourd'hui domineront demain. *Voir chapitre cas d'usages.*

Mythe 5: Vous pouvez exprimer n'importe quoi dans un contrat intelligent.

Bien que cela soit techniquement vrai, en pratique, la blockchain se limite à des cas d'utilisation simples et bien compris. Les contrats intelligents sont essentiellement des fusées (un seul lancement…). Par conception, une fois publié, vous ne pouvez pas réviser ou corriger les bugs. Ils impliquent des interactions remarquablement complexes et des conséquences irrévocables. La DAO

(Organisation Autonome Décentralisée), une société d'investissement basée sur l'Ethereum, est un exemple qui a coûté aux participants des dizaines de millions de dollars en quelques heures. Sa résolution a failli briser la communauté. Vous devez vraiment trouver les bons cas d'utilisation et ne pas supposer qu'ils vont tous être en sécurité. *Voir chapitre Smartcontrats*.

Mythe 6: Si vous n'aimez pas une blockchain publique, rendez-vous dans le privé.

Les blockchains privées ne sont pas la réponse à la vie privée ou à l'accès restreint à l'information. En fait, vous pouvez argumenter que les blockchains privées ne devraient même pas être sur la table en tant qu'option. Néanmoins, les chaînes de blocs d'entreprise peuvent ne pas réaliser tous les avantages inhérents à la technologie blockchain et les chaînes de blocs développées en privé peuvent manquer de la communauté et de l'examen académique nécessaire pour assurer leurs propriétés. *Voir chapitre blockchains privées ?*

Mythe 7: "Nous avons créé une nouvelle blockchain avec la caractéristique X."

Les produits blockchain communautaires peuvent bifurquer à gauche et à droite par la décision d'acteurs privés qui les améliorent de diverses manières. Mais, les grandes communautés composées d'adopteurs, d'utilisateurs, d'universitaires et d'exécutants sont la seule force assurant les propriétés cryptographiques de la mise en œuvre. Seules les blockchains open source avec les communautés les plus importantes et les bases *install-plus-adoption* persisteront. Le reste peut être considéré comme des expériences de laboratoire et 99,9% d'entre eux mourront horriblement. *Voir chapitre blockchains privées ?*

Algorithmes

Il existe plusieurs technologies cryptographiques qui constituent l'essence de Bitcoin mais aussi Ethereum (avec quelques subtilités) et tous les autres. Nous reprenons, en citation, quelques explications disponibles en ligne.

Cryptographie asymétrique

La première est la cryptographie à clé publique. Chaque portefeuille est associé à la clé publique de son propriétaire actuel. Lorsque vous envoyez des bitcoins à quelqu'un, vous créez un message (transaction), attachant la clé publique du nouveau propriétaire à cette quantité de pièces, et vous le signez avec votre clé privée. Lorsque cette transaction est diffusée sur le réseau bitcoin, tout le monde sait que le nouveau propriétaire de ces pièces est le propriétaire de la nouvelle clé. Votre signature sur le message vérifie pour tout le monde que le message est authentique. L'historique complet des transactions est conservé par tout le monde, donc tout le monde peut vérifier qui est le propriétaire actuel d'un groupe de portefeuilles particulier et tracer ses transactions (voir chapitre traçabilité).

Bitcoin et Ethereum utilisent l'algorithme ECDSA (Elliptic Curve Digital Signature Algorithm) et travaillent sur la même courbe elliptique secp256k1.

Commentaire :

Secp256k1 est une courbe elliptique recommandée par Certicom dans une publication de 2000 (http://www.secg.org/SEC2-Ver-1.0.pdf)

The elliptic curve domain parameters over $\mathbb{F}_p$ associated with a Koblitz curve `secp256k1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

$= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$

The curve E: $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ is defined by:

a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

b = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007

The base point G in compressed form is:

G = 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

and in uncompressed form is:

G = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

Finally the order n of G and the cofactor are:

n = FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

h = 01

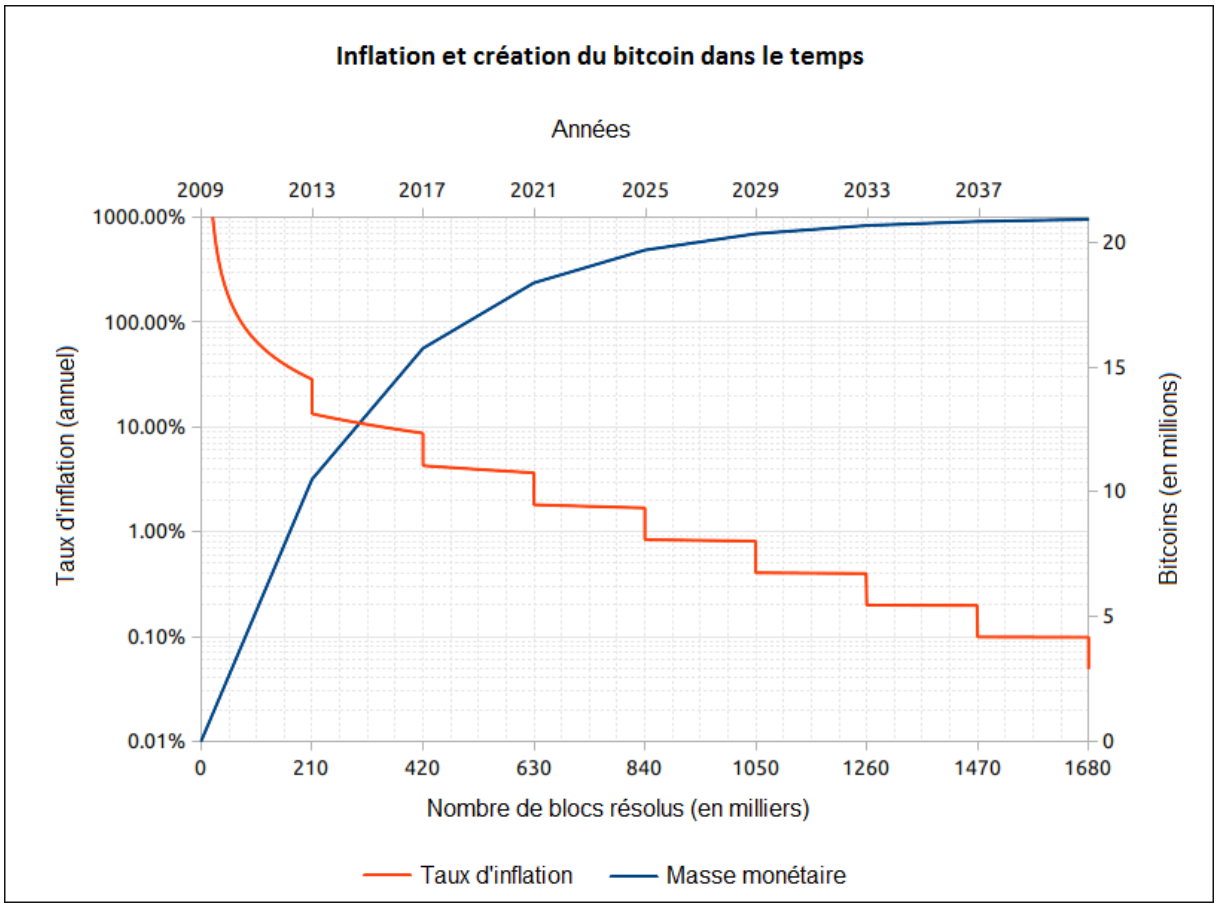
Très curieusement, la NSA semble abandonner en 2015 les courbes elliptiques pour des raisons floues (trop fort ou trop faible ?). Une analyse ici émet des hypothèses : https://eprint.iacr.org/2015/1018.pdf

“ elliptic curve cryptography is not the long term solution many once hoped it would be. Thus, we have been obligated to update our strategy.”

Cela alimente trois des quinze prédictions d’Adi Shamir (le S de l’algorithme RSA) en 2016 lors d’un congrès sur la cryptologie financière :

13. Bitcoin disparaîtra mais laissera un héritage.
14. Blockchain sera *hype*, mais ne réussira que dans des circonstances limitées.
15. Un flux sans fin de nouveaux mécanismes de paiement sera présenté lors des futures conférences *Financial Crypto*.

La fragilité future, mais à échéance imprévisible, de l’algorithme de signature ne sera vraisemblablement pas le facteur décisif qui fera mourir Bitcoin. Le plafonnement de la masse monétaire du Bitcoin (21 millions de bitcoin), fixée dès sa conception, nécessitera au minimum une évolution majeure (fork dans le jargon)[11].



[11] Pour une analyse plus poussée autour des primitives cryptographiques, On Bitcoin Security in the Presence of Broken Crypto Primitives, February 19, 2016, https://eprint.iacr.org/2016/167.pdf

Hachage cryptographiques

La seconde est une fonction de hachage cryptographique[12] (sans clés : erreur classique des commentateurs) qui prend essentiellement des données d'entrée qui peuvent être de pratiquement n'importe quelle taille, et les transforme, de façon effectivement impossible à inverser ou à prévoir, en une chaîne relativement compacte (dans le cas de SHA-256, le hachage est de 32 octets). Faire le moindre changement dans les données d'entrée change son hachage ou condensat de façon imprévisible, donc personne ne peut créer un bloc de données différent qui donne exactement le même hachage. De cette façon, les blocs Bitcoin sont identifiés par leur condensat, ce qui sert le double objectif de l'identification ainsi que de la vérification de l'intégrité.

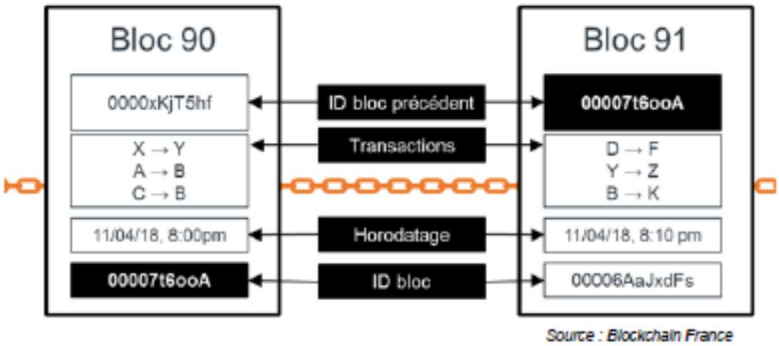
Commentaire :

Personne ne doute aujourd'hui de la solidité de SHA-256 pour de longues années, même si son successeur SHA3 a déjà été retenu par NIST/NSA. Ethereum en implémente d'ailleurs une variante préliminaire différente du choix définitif qui est intervenu après sa naissance. Une collision de SHA1 (160 bits) avait été révélée le 23 février 2017 (http://shattered.io/)

Blockchain

Le troisième ingrédient est la chaîne de blocs partagée par tous même si sa taille infiniment croissante en complique l'analyse (les traitements continus portent sur les derniers blocs). Là non plus, il ne s'agit pas d'une nouveauté.

En informatique et en cryptographie, un **arbre de Merkle** ou **arbre de hachage** est une structure de données contenant un résumé d'information d'un volume de données, généralement grand (comme un fichier). Les arbres de hachage ont été inventés par Ralph Merkle en 1979.



Source : Blockchain France

Cette base de données (le livre de compte ou *ledger*) est spécifiée ainsi :

- Pour bitcoin, pas de spécification formelle, mais la réalisation informatique constitue la référence[13]
- Ethereum a bénéficié d'un effort de formalisation mathématique plus élevé (et abscons) mais là encore ce sont les programmes qui font référence[14] *On y reviendra sur les smartcontrats*.

[12] Voir, par exemple, http://www.fil.univ-lille1.fr/~bouillaguet/PAC/poly/ch3.pdf

[13] Voir https://bitcoin.org/en/developer-reference

Commentaire :

L'évolution de la blockchain et des traitements qu'elle autorise se font par consensus de la communauté. Cela pose des problèmes en cas d'attaques. *Voir chapitre attaques*.

Une divergence peut faire naître de nouvelles branches, phénomène qu'on a pu observer dans le monde des *operating systems* (OS) libres[15]. Mais le marché a horreur de ces instabilités. On distingue :

- Un *soft fork* (embranchement mou) est une modification rétro-compatible du protocole de la blockchain. Les anciens blocs validés restent compatibles avec les nouvelles règles, plus strictes. Si la majorité des participants du réseau adopte les modifications, la mise à jour devient effective. Les nœuds qui ne se plient pas au nouveau protocole sont exclus : leurs blocs ne sont plus en mesure d'être validés par les autres participants. Dans le cas du Bitcoin par exemple, de nombreux soft forks ont été réalisés avec succès.
- Un *hard fork* (embranchement dur) est une modification majeure du protocole, dont les nouvelles règles ne sont pas compatibles avec les précédentes. Son intérêt est de pouvoir réviser n'importe quel aspect du code de la blockchain. Cependant, en l'absence de consensus entre les participants au réseau, le hard fork peut provoquer une scission entre les différents acteurs. Si une minorité de nœuds décide de ne pas suivre les nouvelles règles proposées, ils peuvent être à l'origine d'une blockchain différente dont le protocole reste incompatible avec les autres. Le Bitcoin Cash et l'ETC (Ethereum Classic) sont des hard forks célèbres. *Voir chapitre smartcontrats*.

Minage

L'enregistrement complet des transactions est conservé dans la chaîne de blocs, qui est une séquence d'enregistrements appelée blocs. Tous les ordinateurs du réseau (nœuds et souvent clients) ont une copie de la chaîne de blocs, qu'ils gardent à jour en passant de nouveaux blocs les uns aux autres (architecture résiliente pair à pair). Chaque bloc contient un groupe de transactions qui ont été envoyées depuis le bloc précédent. Afin de préserver l'intégrité de la chaîne de blocs, chaque bloc de la chaîne confirme l'intégrité de la chaîne précédente, jusqu'à la première, le bloc de la genèse. L'insertion d'enregistrement est coûteuse, car chaque bloc doit répondre à certaines exigences qui rendent difficile la génération d'un bloc valide. De cette façon, aucune partie ne peut écraser les enregistrements précédents en forçant simplement la chaîne.

La fonction de hachage sert de base à la loterie du minage. Pour rendre difficile la génération de bitcoins, la fonction de coût hashcash est utilisée. hashcash est la première fonction de coût ou de preuve de travail sécurisée et efficace. La beauté de hashcash est qu'il est non-interactif et n'a pas de clés secrètes qui doivent être gérées par un serveur central ou un tiers de confiance; hashcash est par conséquent entièrement distribué et infiniment évolutif.

Le minage consiste donc, moyennant récompense financière à être pour un mineur le premier à trouver, à partir de son secret et du bloc à valider, un condensat se terminant par un nombre de

[14] Le yellow paper initial est très difficile d'accès : https://ethereum.github.io/yellowpaper/paper.pdf

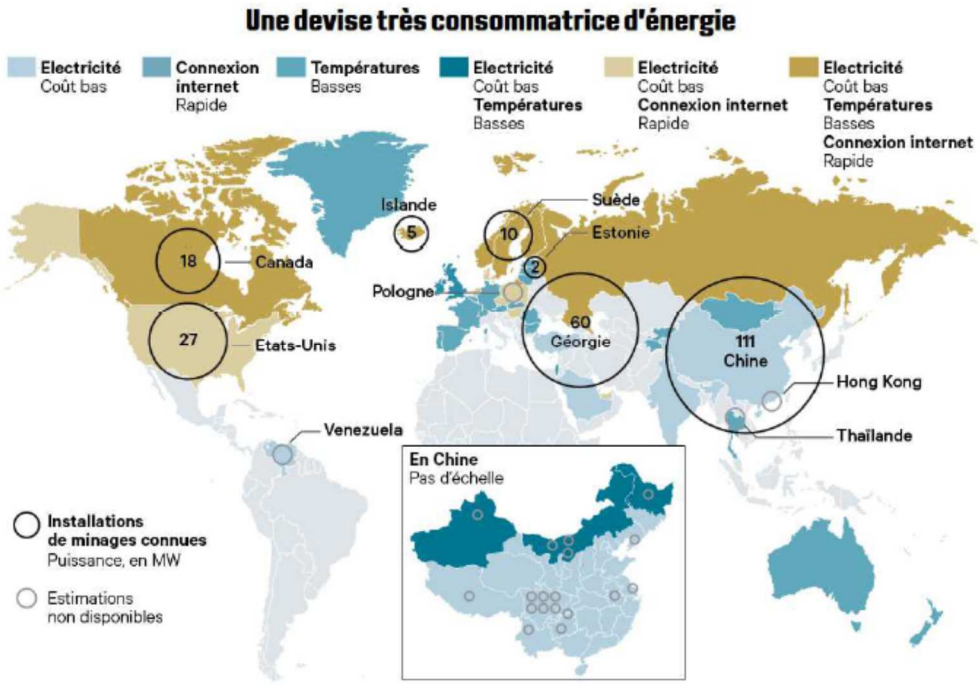
[15] A Repository with 44 Years of Unix Evolution, https://www2.dmst.aueb.gr/dds/pubs/conf/2015-MSR-Unix-History/html/Spi15c.pdf

zéros qui peut être ajusté en fonction de la puissance globale des mineurs (souvent en augmentation en fonction du cours de la cryptomonnaie) et du délai recherché pour la validation de nouveaux blocs (10 minutes pour le Bitcoin, moins pour ethereum mais le mécanisme est différent). La fonction essentielle est de gérer des conflits de type double-dépense.

Dans le cas d'une validation conjointe de deux blocs différents créant deux chaînes parallèles, la règle de la plus longue suite permet rapidement d'assurer l'unicité de la blockchain partagée. Une analyse de cette *Longest Chain Rule* montre, par ailleurs, quelques faiblesses structurelles[16] :

Cette règle de Satoshi peut être considérée comme une tentative précoce et imparfaite de résoudre le problème de double dépense. Plus généralement, d'une certaine manière, c'est aussi une autre façon de tenter de résoudre une version de longue date du « Problème des généraux Byzantins » qui est également résolu par le vote et a été étudié par les informaticiens depuis 1982. On sait que ce genre de problèmes est très difficile à résoudre en pratique.

La crainte d'une collusion de 51% des mineurs (majorité dépassée aujourd'hui par la seule Chine), nécessaire à une atteinte sur son intégrité peut être écartée devant l'industrialisation du métier (concurrence entre acteurs) et sa course à l'armement.



Minage fin 2017

Le seul mécanisme vraiment nouveau de la blockchain est donc le minage collaboratif qui permet l'élimination du contrôle central et/ou du tiers de confiance. Il s'agit d'une avancée majeure qui nécessite cependant un examen lucide (*voir chapitre minage*).

[16] Voir Nicolas T. Courtois, https://arxiv.org/pdf/1405.0534.pdf

J.5. **Mining.** In order to mine a valid block, one repeatedly chooses a random nonce $\mathbf{n}_{rand} \in \mathbb{B}_8$ and calculates the PoW function until

$$\mathtt{PoW}(H_{\mathbb{H}}, \mathbf{n}_{rand}, \mathbf{d})[1] \leqslant \frac{2^{256}}{H_d} \quad . \tag{252}$$

H_d being the current difficulty of the block.

Formalisation du minage PoW de Ethereum

L'idée des smartcontrats date elle de 1997 (http://ojphi.org/ojs/index.php/fm/article/view/548/469).

Enfin, la réussite des protocoles pair-à-pair est tributaire de la qualité de codage des programmeurs pionniers.

Blockchain privée ?

Deux écoles s'affrontent :

- Ceux qui dénient à une technologie non publique, le terme de blockchain.
  - Propriétés jugées indispensables : minage public, décentralisation, blockchain ouverte et partagée, codes libres, liberté d'ouverture de comptes, règles de consensus communautaire.
- Ceux qui soit utilisent une infrastructure communautaire ouverte pour des usages privés, soit utilisent ses fonctions dans un cadre centralisé et/ou propriétaire.
  - Dans les blockchains privées, le propriétaire de la blockchain est une entité unique ou une entreprise qui peut remplacer / supprimer des commandes sur une blockchain si nécessaire. C'est pourquoi dans son vrai sens, il n'est pas décentralisé et peut donc être appelé un registre ou une base de données distribuée avec de la cryptographie pour le sécuriser.

Un article d'IBM[17] souhaite conserver certaines caractéristiques communes aux blockchain publiques et privées :

- Les deux sont des réseaux **pair à pair** décentralisés, dans lesquels chaque participant conserve une réplique d'un registre partagé de signatures numériques uniquement.
- Les deux maintiennent les réplications en synchronisation, grâce à un protocole appelé **consensus**.
- Les deux fournissent certaines garanties sur l'immutabilité du **grand livre comptable (ledger)**, même lorsque certains participants sont fautifs ou malveillants.

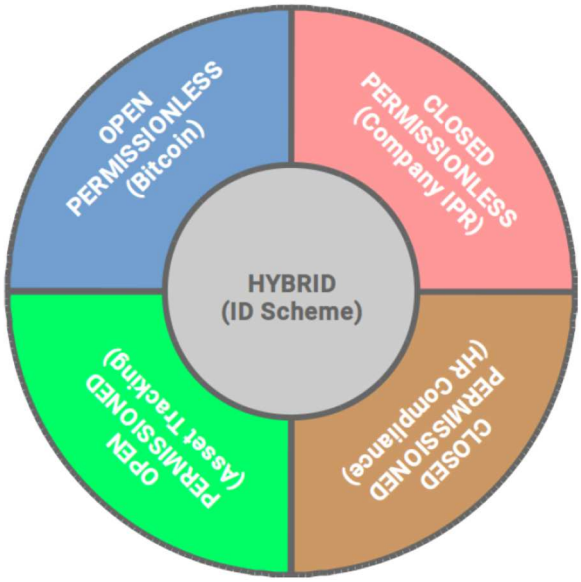
Ce qui les différencie :

- qui est autorisé à participer au réseau (dans le jargon américain, on parle souvent de blockchain à autorisations), exécuter le protocole de consensus et maintenir le ledger partagé.
  - Un réseau blockchain public est complètement ouvert et n'importe qui peut rejoindre et participer au réseau. Le réseau a généralement un mécanisme incitatif pour encourager plus de participants à rejoindre le réseau.
  - Un réseau blockchain privé nécessite une invitation et doit être validé soit par le démarreur du réseau, soit par un ensemble de règles mises en place par le démarreur du réseau. Cela place des restrictions sur qui est autorisé à participer au réseau, et seulement dans certaines transactions. Le mécanisme de contrôle d'accès pourrait varier : les participants existants pourraient décider des futurs entrants ; une autorité de régulation pourrait délivrer des licences de participation ; ou un consortium pourrait prendre les décisions à la place. Une fois qu'une entité a rejoint le réseau, elle jouera un rôle dans le maintien de la chaîne de blocs de manière décentralisée.
- Le minage n'est pas nécessaire sous sa forme PoW. *Voir chapitre minage*.

[17] Voir https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

- il s'agit de parvenir à un consensus sans dépenser énormément d'énergie, de temps et d'argent.

Un autre inconvénient reste l'ouverture de la blockchain publique, qui implique peu ou pas de confidentialité pour les transactions et ne supporte qu'une faible notion de sécurité. Ces deux caractéristiques sont des considérations importantes pour les cas d'utilisation en entreprise. Pour apporter des modifications aux blockchains privées, il faut des privilèges et des accès spéciaux.



5 types de Blockchain

Commentaire

Il est tentant de se détourner de la seule nouveauté que constitue le minage. Mais cela réduit fortement le caractère infalsifiable, immuable et partagé.

Aujourd'hui, quand le défi de la montée en charge (scalabilité) n'est pas la caractéristique majeure du service à remplir (c'est souvent le cas, en dehors des transactions purement financières ou du contrôle d'accès), la meilleure solution consiste à greffer (principe du *parasitisme de couvée*) sa blockchain privée avec ses mécanismes propres de sécurité (confidentialité, intégrité) à une blockchain ouverte et disponible (résilience) par des mécanismes qui ne sont pas si faciles à maîtriser et qui font, en outre, le pari de la pérennité de la solution ouverte. *Voir chapitre attaques*.

Exemple d'une offre d'assurance sur les retards d'avion par AXA :

https://www.axa.com/fr/newsroom/actualites/axa-se-lance-sur-la-blockchain-avec-fizzy

https://fizzy.axa/

Le contrat est là : https://fizzy.axa/api/conditions-generales.pdf

Les smartcontrats Fizzy sont publics[18] avec le discours suivant :

[18] Pour une analyse juridique, voir http://www.iredic.fr/2017/11/17/le-smart-contract-contrat-non-identifie/
Les contrats sont disponibles via : https://etherscan.io/address/0xe083515d1541f2a9fd0ca03f189f5d321c73b872#code

« Lors de la souscription à distance d'un Contrat FIZZY, ses éléments essentiels (vol garanti, retard garanti et indemnité) sont traduits par notre plateforme sous la forme d'un code informatique pour former un « smartcontract », c'est-à-dire un programme qui va solliciter de manière autonome les informations nécessaires à son exécution (au cas d'espèce, l' heure d'arrivée du vol garanti pour déterminer s'il y a eu un sinistre) et exécuter automatiquement les actions contractuellement induites par celles-ci.

Pour garantir l'autonomie et l'indépendance de ce smartcontract, celui-ci est en outre intégré dans un des registres publics décentralisés les plus populaires et sécurisés : la « Blockchain Ethereum».

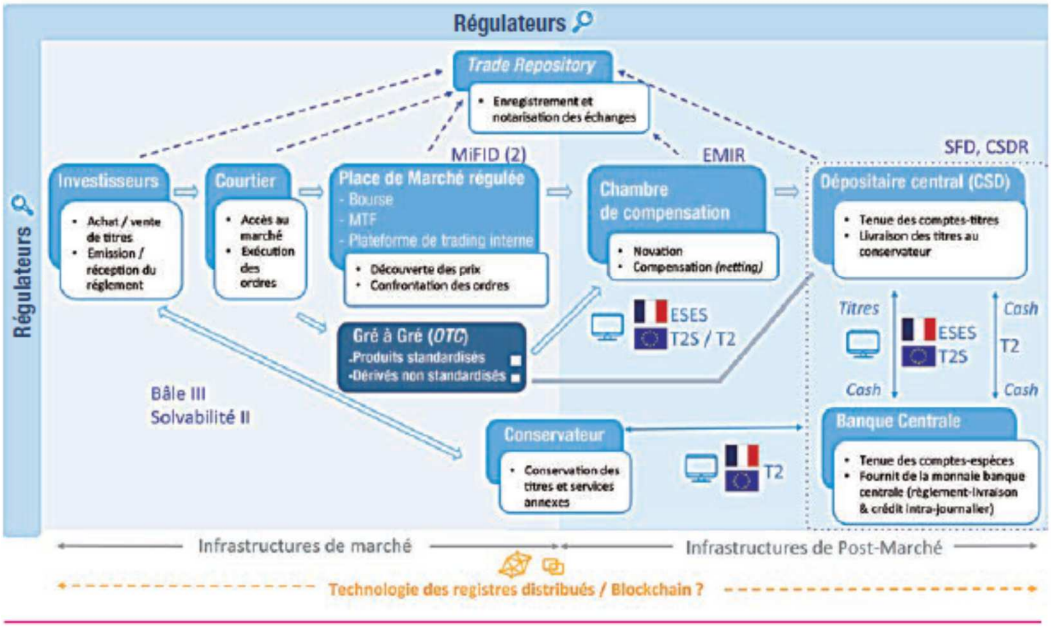
Il en résulte que, dès lors qu'est reçue l'information relative au retard de votre vol via le fournisseur de données aériennes Flightstats, notre plateforme initie de manière autonome et indépendante le processus de paiement de votre indemnité en cas de retard garanti. »

Une offre américaine antérieure du même type existe :

https://github.com/etherisc/flightDelay

Pour une analyse plus poussée : voir page 24 ou 25 d'une étude économico-sociale[19].

Figure 3 : Quel niveau d'intégration pour la DLT au sein de l'infrastructure des marchés financiers ?



Ce schéma, proposé par cette étude, d'intégration dans le marché régulé gomme certains des avantages de la blockchain, en sauvegardant l'organisation et l'orthodoxie historique. L'utilisation d'une BlockChain nécessiterait pourtant de revoir les schémas d'organisation traditionnels vers du communautaire, du décentralisé et du contrôle consensuel (à l'exemple de ce qu'on nomme l'uberisation de l'économie). On pourra alors vraiment parler de « disruption destructrice ».

[19] Blockchain et autres registres distribués : quel avenir pour les marchés financiers ?, https://bitcoin.fr/wp-content/uploads/2016/07/Blockchain-et-autres-registres-distribu%C3%A9s-quel-avenir-pour-les-march%C3%A9s-financiers-Klara-Sok-Alexis-Colomb.pdf

Attaques

Analyse de sécurité

Dans la mise en place d'une blockchain, une analyse des choix de sécurité doit être effectuée pour les différentes technologies, acteurs et cas d'usages selon l'ensemble des axes suivants :

- Conformité RGPD si applicable (droit à l'oubli, respect de la vie privée) ;
- Anonymat, pseudonymat ;
- Contrôlabilité des actions illicites (malware, transactions frauduleuses, …) ;
- Transparence versus protection des smarts contracts ;
- Attaques sur le minage ;
- Attaques sur les smartcontrats ;
- Lien monde réel / monde numérique ;
- Relation IA et Blockchain dans le cadre des analyses prédictives ;
- Preuve numérique ;
- Autres : certification, e-réputation.

Ces considérations doivent compléter un cadre d'analyse de performances plus classique[20].

Il faut cependant garder à l'esprit que le vrai juge de paix de la solidité de la blockchain (ici Bitcoin) est sa résilience à l'épreuve du réel comme le souligne Jean-Paul Delahaye :

Personne avant lui n'avait imaginé un système robuste réalisant cette gestion infalsifiable d'un fichier de comptes. Le scepticisme sur la robustesse de la nouvelle monnaie, assez fort au départ, tend à s'atténuer. Le fait que la monnaie ait résisté plus de cinq ans malgré les attaques qu'elle a eu à subir est une preuve par l'expérience que le protocole tient. C'est l'une des explications de la valeur actuelle du Bitcoin.

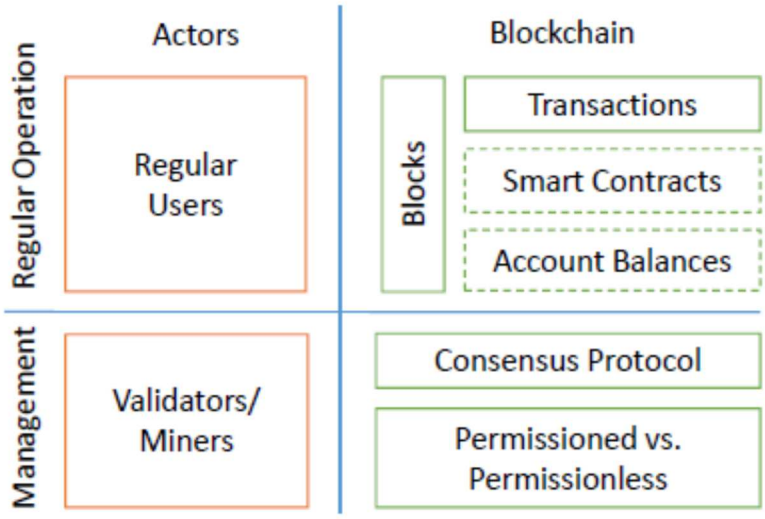


Figure 1: Generic Blockchain Architecture. Dashed lines indicate that the component is optional

[20] Voir par exemple : a general framework for blockchain analytics, https://arxiv.org/pdf/1707.01021.pdf

Analyse Globale

Elle peut être résumée dans le tableau suivant[21] :

Table 1. SWOT analysis of the adoption of blockchain.

	Positive	Negative
Internal	**Strengths**	**Weaknesses**
	- Fast and low-cost money transfers - No need for intermediaries - Automation (by means of smart contracts) - Accessible worldwide - Transparency - Platform for data analytics - No data loss/modification/falsification - Non-repudiation	- Scalability - Low performance - Energy consumption - Reduced users' privacy - Autonomous code is "candy for hackers" - Need to rely to external oracles - No intermediary to contact in case of loss of users' credentials - Volatility of cryptocurrencies - Still in an early stage (no "winning" blockchain, need of programming skills to read code, blockchain concepts difficult to be mastered) - Same results achieved with well-mastered technologies
External	**Opportunities**	**Threats**
	- Competitive advantage (if efforts to reduce/hide the complexity behind blockchain are successful, or in case of diffusion of IoT) - Possibility to address new markets (e.g., supporting car and house sharing, disk storage rental, etc.) - Availability of a huge amount of heterogeneous data, pushed in the blockchain by different actors	- Could be perceived as unsecure/unreliable - Low adoption from external actors means lack of information - Governments could consider blockchain and smart contracts "dangerous" - Medium-long term investment - Not suitable for all existing processes - Customers would still consider personal interaction important

Analyse des protocoles

Les protocoles de sécurité réseaux et en particulier ceux du pair-à-pair nécessitent des analyses de sécurité approfondies par la communauté ouverte. Ainsi le protocole principal de sécurisation de l'Internet TLS (ex SSL) a connu de multiples variantes et mises à jour et bénéficie d'une scrutation continue[22].

La tendance actuelle, notamment dans le foisonnement des crypto-monnaies alternatives, est à partir des protocoles historiques (BitCoin et Ethereum) de développer des variantes qui complexifient les mécanismes et parfois les fragilisent. Pour ne citer qu'un exemple :

20 avril 2018 (ANSSI)

MONDE - Trois vulnérabilités affectant plusieurs cryptomonnaies ont été découvertes

Une équipe de quatre chercheurs des universités de Saarland et de Friedrich-Alexander-Universität Nürnberg-Erlangen a découvert trois vulnérabilités affectant le protocole Zerocoin et la librairie

[21] Blockchain and smart contracts for insurance: is the technology mature enough ?, http://www.mdpi.com:8080/1999-5903/10/2/20/pdf

[22] Thèse ici http://www.theses.fr/2016TELE0014.pdf

logicielle libzerocoin qui est utilisée pour la fabrication de cryptomonnaies au travers de ce protocole. Les cryptomonnaies impactées sont le SmartCash, le Zoin, le Zcoin, le Hexxcoin et le PIVX. En pratique, la vulnérabilité affectant le protocole Zerocoin permet à des attaquants de suspendre une transaction légitime et mener pour leur compte une transaction avant la requête légitime. Concernant les deux vulnérabilités impactant la librairie libzerocoin, la première prendrait la forme d'un bogue d'inflation qui permettrait à des attaquants de générer de nouvelles unités de cryptomonnaies alors que la seconde affecte le processus de signature de transaction[23].

Droit à l'oubli

Le premier principe général qui doit s'appliquer est celui de la rémanence sur Internet : toute donnée publiée en clair sur Internet a une durée de vie non prédictible (sauf obsolescence des supports, faillite des hébergeurs) et souvent très longue (sauvegardes multiples dans le Cloud, effet Streisand, copies privées, etc.). La blockchain par ses mécanismes cryptographiques actuels et sa viralité (stockage sur l'ensemble des nœuds et potentiellement même chez l'usager) assure une durée de vie potentiellement infinie aux transactions qu'elle notarise.

A contrario, une façon simple d'effacer une information, c'est de la chiffrer et de perdre la clé. L'arrivée de la cryptographie homomorphe permettra, d'ailleurs dans quelques années, de travailler sur des données chiffrées[24] sans pour autant éliminer la gestion de secrets (la cryptographie sans clés n'existe pas ; pour fabriquer des secrets, il faut du secret).

Une réponse, non technique, nécessite sur la blockchain[25] :

- De ne pas y stocker de données personnelles ;
- D'y pseudonymiser ces données personnelles ;
- D'y chiffrer les données mais cela nécessite une gestion des clés ailleurs ;
- De stocker les données dans une autre base de données chiffrée et privée. On pourrait alors stocker sur la blockchain publique les clés de déchiffrement elles-mêmes chiffrées par les clés publiques des personnes autorisées à y accéder.

µchain[26] propose une chaîne mutable (modifiable) à base de transactions modifiables et nulles, de méta-transactions avec contrôle d'accès et de deux schémas de gestions de clés. Pour cacher les enregistrements de données obsolètes, il faut soit du chiffrement simple géré par les validateurs, soit du chiffrement avec partage de secrets et fenêtres temporelles bien plus complexe à mettre en œuvre. L'article parle d'un prototype utilisant le code partagé *Hyperledger Fabric* qui ne semble pas accessible pour le moment.

[23] Voir https://www.chaac.tf.fau.de/files/2018/04/attack-cryptocur.pdf

[24] Voir https://hal.inria.fr/IRT-SYSTEMX/hal-01435505v1

[25] Voir http://www.chainfrog.com/wp-content/uploads/2017/08/gdpr.pdf

[26] Voir https://eprint.iacr.org/2017/106.pdf

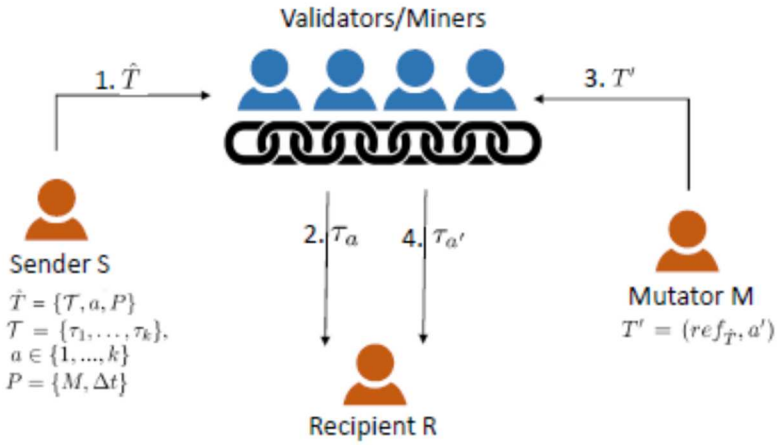


Figure 4: Transaction Mutation

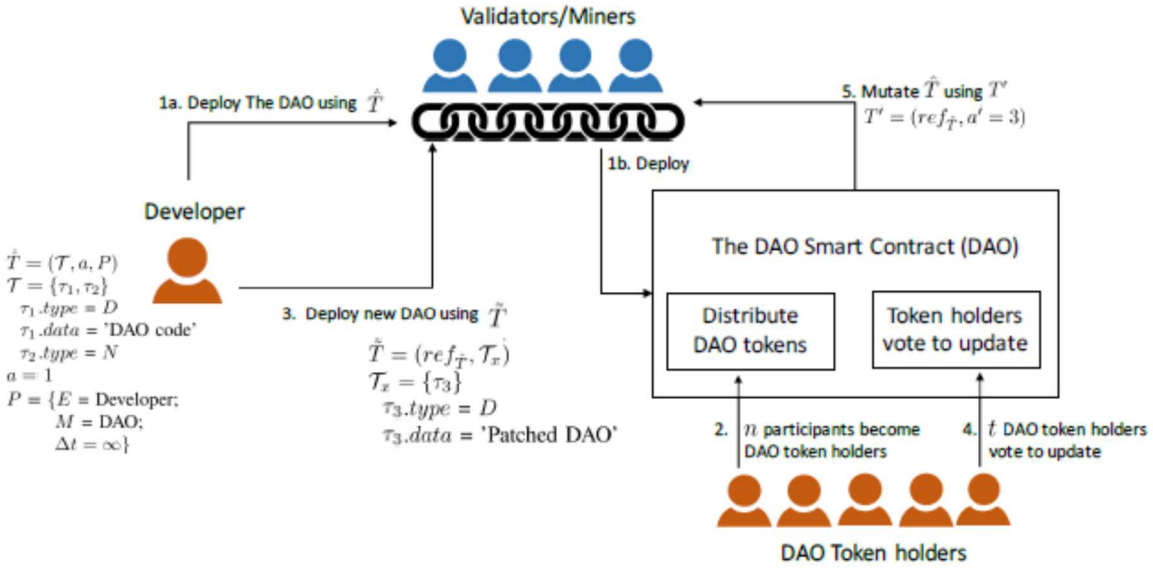


Figure 6: Patching the vulnerability of the DAO Smart Contract

Pseudonymat

L'anonymat (une fonction de sécurité au sens des Critère Communs[27]) est une fonction très difficile à assurer sur Internet. Certains criminels y consacrent beaucoup d'énergie (relais, vpn, messageries dites sécurisées).

Dans notre enquête sur des victimes de cyberattaques réussies (TPE, PME), nous avons pu observer des techniques plutôt rudimentaires. Pour la remise des rançons, après attaque réussie par rançongiciel, le maître-chanteur communique d'abord des adresses de courriels successives puis souvent des comptes Bitcoin créés pour l'occasion qui servent de relais avant blanchiment classique de l'argent converti en monnaie classique. L'impunité relève alors de trois facteurs :

- extra-territorialité et manque de volonté de déclencher des procédures judiciaires complexes ;

[27] Class FPR: Privacy dans https://www.commoncriteriaportal.org/files/ccfiles/ccpart2v21.pdf

- complexité des échanges d'informations sur la cybercriminalité entre pays ;
- existence de « paradis numériques ».

Pourtant, la blockchain permet, avant conversion, un suivi de l'argent sale. Ainsi, en traçant les comptes Bitcoin, les attaquants à l'origine de la propagation du rançongiciel SamSam aux USA auraient gagné près de 850 000 dollars, notamment dans le secteur hospitalier[28].

Des études[29] sur les paiements de rançons suite à des infections par rançongiciels sont possibles à partir des données publiques.

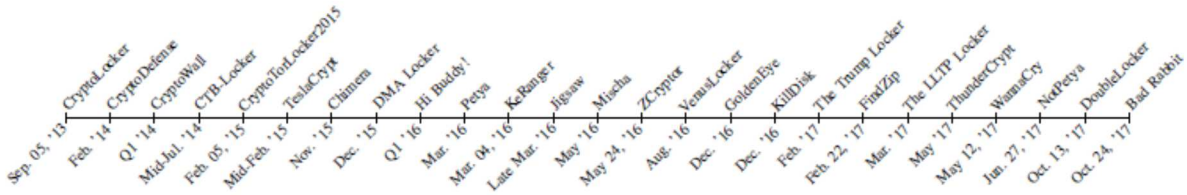


Figure 3: Occurrence of Bitcoin ransomware

Ransom	Time period	Payments	BTC	USD value
$300	May 12, '17 - Oct. 02, '17	192	32.3430	58,416.62
$600		46	14.8313	27,660.14
Total		**238**	**47.1743**	**86,076.76**

Table XVII: Summary of ransoms paid to WannaCry

#	Address	Source(s)
1	1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX	[29, 71]

Table A.7: NotPetya

#	Address	Source(s)
1	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94	[33, 78]
2	12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	
3	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn	

Table A.9: WannaCry

#	Address	Source(s)
1	15fbyNgDnqYQR5vSHJ8PTAEJbKy4dwNBCZ	[96]
2	12YHmaLEAbWx3o3p6BvegG9WH47EYs8t1V	[97]
3	15MHczWfcYxt3P3NwYqCthaNiieGP8RY9d	[98]
4	3NQoq5MVPfEMw12gB4a2c1G61mRZyMymsB	[99]
5	12vfQqmMxiDvZdzYHndfURupmcjjs8uSpY	[100]
6	1FLjcTFpz9MhwLdZ4xm9onpAnUGfRbGdXg	[101]
7	1Cj37Iw5uHwfye6SrdIzHzSMhUekp3jM63	[102]
8	1Q5B5udzDLpNJbpedGpyGMLVU5DR5dTqx6	[103]
9	13VEVaJUMdJyQ7tiPfBaVNKjj2dS9ahU1z	[104]
10	1HxkJ3vz2tvpcHgdt9yyY4XivdY9jKkcZH	[105]
11	1LBhCecBmT23hybSUYyFW1YYqtTJcvFui2	
12	1H8BX1JsLk9YCoNeBahYbgWo5ZqEn752ey	
13	1L9GdBW65Rt6e8UY69bnWNWomsppFFFR2X	[106]
14	1ESe1nekuFJcEWycb1JtCz9KneNEm8yjg3	
15	1EVNFaX7HktWfud6fPueoMJ2Xw4UfYGY5Y	
16	1CcAYfsKNNFPq7AKkbKQzRKw2kqjrqUeN9	
17	18jCCAR2QZf6uZTnu4769ZknPtXjbmh1mw	
18	1EH3yoQciVcWUufa4NWJvftyvvFxjbFLtQ	
19	1F5RJzWN1g38wD9XbcspcxaYDU5hKpdvm8	

Table A.15: Jigsaw

Jigsaw est un rançongiciel créé en 2016 avec compte à rebours.

[28] Voir https://www.csoonline.com/article/3263693/security/samsam-ransomware-attacks-have-earned-nearly-850-000.html

[29] La plus complète est ici : On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective, https://arxiv.org/pdf/1804.01341.pdf

Ransomware	Overall			Ransom		
	Payments	BTC	USD Value	Payments	BTC	USD value
CryptoLocker	51,766	133,045.9961	42,292,191.17	804	1403.7548	449,274.97
CryptoDefense	128	138.3223	70,113.41	108	126.6960	63,859.49
CryptoWall	51,278	87,897.8510	45,370,589.00	3,730	5,351.2329	2,220,909.12
DMA Locker	298	1,433.3463	580,763.95	117	339.4591	178,162.77
NotPetya	70	4.1787	10,284.42	33	4.0576	9,835.86
KeRanger	13	10.0044	4,175.35	10	9.9990	4,173.12
WannaCry	341	53.2906	99,549.05	238	47.1743	86,076.76

Table XVIII: Overview of overall payments and ransom payments to different ransomware

Notre propre analyse ne permet pas de classer Wannacry et Notpetya dans les rançongiciels ordinaires. Les codes malveillants ont parfois intérêt à se maquiller sous la forme la plus active du moment. Cette analyse semble confirmée par les tableaux ci-dessus.

Pour en revenir à l'anonymat, Bitcoin et Ethereum proposent plutôt, sans réalisation explicite, du pseudonymat. La création d'un portefeuille révèle peu d'informations d'identification hors de l'adresse IP (sauf utilisation d'un Tor-Browser).

Certaines crypto-monnaies, comme Monero, garantiraient un meilleur anonymat[30] sans atteindre toutefois à l'efficacité de la criminalité financière ordinaire traditionnelle. L'usage de techniques de signature en oignon (analogue au routage en oignon du réseau Tor) ou de preuve à divulgation nulle de connaissance constitue une piste à explorer.

Mais ce n'est pas si simple que cela. Extrait de la veille ANSSI (29 mars 2018).

La cryptomonnaie Monero présente des vulnérabilités qui permettrait de tracer partiellement les transactions

Des chercheurs de plusieurs universités américaines ont publié une étude à propos de deux vulnérabilités dans le fonctionnement de la monnaie virtuelle Monero. Dans le processus par lequel Monero masque la source d'un paiement, sont insérés dans la chaîne de blocs, en tant que leurres appelés "mixins", des échantillons d'informations d'autres paiements. La première vulnérabilité remonte à la première année d'existence de la cryptomonnaie, alors qu'il était possible pour les utilisateurs de ne pas utiliser les mixins, rendant les transactions non-anonymes. Ces transactions peuvent la suite pu être utilisées en tant que "mixins" qui, une fois identifiés dans un nouveau paiement, peuvent être isolés pour l'identification des autres éléments ; et ainsi de suite pour les transactions suivantes. Une seconde vulnérabilité réside dans la possible identification du datage des leurres et transactions effectives contenus dans une information de paiement. En effet, il serait possible de récupérer ces éléments de datage pour identifier l'origine d'un paiement en isolant l'élément le plus récent. Monero aurait déjà effectué des mises à jour pour la correction de ces vulnérabilités mais elles n'auraient pas complètement résolu le problème.

Des opérations de « pump end dump » traditionnellement activées sur le boursicotage à hautes fréquences commencent à toucher les crytpo-monnaies, facilitées par leur grande volatilité[31].

[30] Voir https://coinsutra.com/anonymous-cryptocurrencies/ Monero utilise des méthodes cryptographiques complexes telles que les signatures Ring, RingCT, Kovri et Stealth pour protéger la vie privée de ses utilisateurs…

[31] Voir : https://www.crypto-france.com/groupes-telegram-pump-and-dump-crypto-monnaies/

Traçabilité

La traçabilité totale des transactions offre des fonctions de sécurité tout à fait inédites, comme vu ci-dessus pour les rançongiciels. Ainsi, chaque incident de sécurité répertorié (rendu public) permettrait d'imbiber la chaîne de blocs par une *teinture* de la crypto monnaie impliquée (pourcentage d'un bitcoin relevant d'un acte délictueux). L'ensemble des transactions ultérieures étant tracée, il est alors possible de propager ce taux de malveillance. Cela permettrait à un utilisateur honnête de refuser de la mauvaise monnaie ou, à un contrôleur, de suivre jusqu'à sa conversion en « vraie monnaie » l'arbre de l'usage malveillant et les comptes créés.

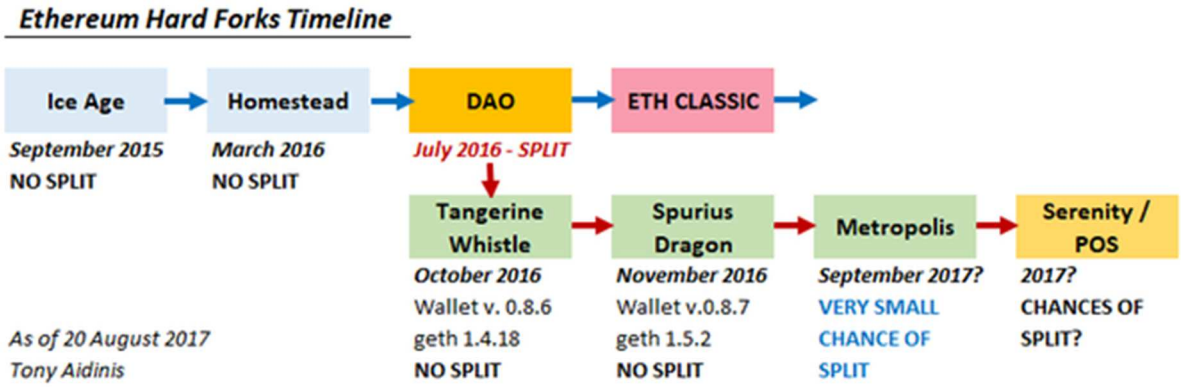
Un article récent[32] propose un tel mécanisme de marquage très facilement intégrable au Bitcoin grâce à un algorithme simple basé sur la règle du *first-in-first-out*.

Que se passerait il si les lois existantes étaient effectivement appliquées aux riches et aux puissants ? Les réformateurs sociaux réclament souvent de nouvelles règles, mais ignorent les énormes changements qui pourraient se produire si nos règles existantes étaient appliquées de la même manière à tous. Et dans le nouveau monde de l'initial coin offering et de la crypto-monnaie en action, les riches et les puissants sont les échanges de bitcoins.

Il s'agit là d'une piste sérieuse qui peut être étendue à d'autres valeurs que la crypto-monnaie (mesure de la confiance, de l'obsolescence, de la fragilité, etc.).

Attaques sur les smartcontrats

Le traumatisme initial est arrivé avec le bogue d'appel récursif The DAO[33]. *Voir chapitre smartcontrats*.



Attaques sur le minage

Depuis une année et fortement lié à la hausse de la valeur du Bitcoin, se développe, à côté du vol de crypto-monnaie[34] (vol de clés par les techniques classiques de l'hameçonnage, du cheval de Troie, de la fuite interne, du vol physique ou d'arnaques de type *Bitcoin Ponzi Scheme*, etc.) des attaques

[32] Making Bitcoin Legal, https://www.cl.cam.ac.uk/~rja14/Papers/making-bitcoin-legal.pdf

[33] Voir https://theethereum.wiki/w/index.php/The_DAO_Refunds

[34] Exemple de la faillite de Mt. Gox, https://www.wired.com/2014/02/bitcoins-mt-gox-implodes-2/?cid=co19086554

consistant, comme le déni de service distribué à base de BotNet, à faire miner des machines compromises pour essayer de gagner le jackpot du mineur chanceux.

Une analyse a été menée sur le minage par des extensions de navigateurs web[35].

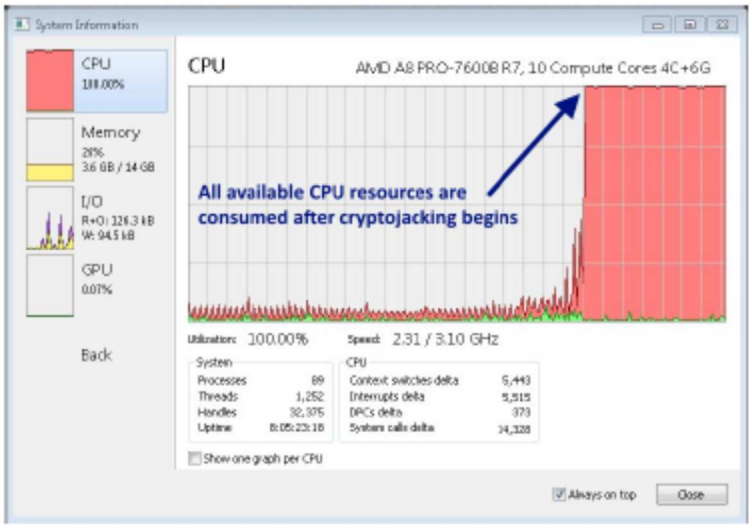


Figure 9. Comparison of CPU usage of browser without and with browser mining enabled.

Quelques exemples récents (veille de l'ANSSI).

18 avril 2018

Avast détecte un nouvel extracteur de cryptomonnaie hébergé sur GitHub

Les chercheurs d'Avast ont découvert un nouvel extracteur de cryptomonnaie ciblant Monero, disponible librement sur la plateforme de développement GitHub. Les vecteurs d'infection utilisés sont des fausses publicités présentes sur des sites Internet infectés, invitant les victimes à télécharger des mises à jour Flash Player ou des jeux pour adultes. L'extracteur est difficile à détecter, car il utilise au maximum 50 % de la puissance du processeur de la victime, laissant ainsi des capacités suffisantes aux tâches prioritaires. Pour des raisons financières, la fonctionnalité d'extraction a été couplée à une extension Google Chrome malveillante injectant de fausses annonces et cliquant sur des publicités en arrière plan. Ces informations ont été transmises à GitHub et Google Chrome, qui travaillent sur des solutions.

16 avril 2018

La plateforme d'échange Coinsecure victime d'un siphonnage de cryptomonnaie possiblement orchestré par l'un de ses employés

Cette plateforme indienne qui compte plus de 200 000 utilisateurs a déclaré avoir été victime d'un siphonnage de 438 bitcoins, soit l'équivalent de 3 millions de dollars. Ces bitcoins étaient stockés dans un portefeuille virtuel protégé par un mot de passe et ont été transférés vers une adresse inconnue de Coinsecure. La plateforme accuse l'un de ses cadres d'être à l'origine de ce vol et a précisé qu'elle indemniserait les clients victimes des pertes subies.

[35] A first look at browser-based cryptojacking, https://arxiv.org/pdf/1803.02887.pdf

6 avril 2018

Plusieurs applications Android malveillantes de minage de cryptomonnaie ont été découvertes dans le magasin de Google

Les chercheurs en sécurité de Kaspersky Lab ont découvert de nombreuses applications mobiles malveillantes de minage de cryptomonnaie Monero qui sont distribués au travers du magasin d'applications Google Play Store. Ces applications prenaient la forme de jeux vidéos, d'applications de diffusion de sports ou de réseaux privés virtuels. Certains de ces applications ont été téléchargées plus de 100 000 fois. Néanmoins, la société de sécurité a prévenu Google qui les a supprimées depuis.

5 avril 2018

Palo Alto découvre un nouveau maliciel de minage de cryptomonnaie en vente dans l'Internet sombre

Les chercheurs en sécurité de Palo Alto ont découvert un nouveau maliciel de minage de cryptomonnaie baptisé Rarog qui utilise des tactiques proches des réseaux de machines zombies. Il charge ainsi des maliciels puis les exécute et est capable de mener des dénis de service distribués. Il présente la particularité de se mettre à jour automatiquement et de pouvoir installer de nouvelles bibliothèques dynamiques sur les machines compromises. L'équipe de chercheur l'a relié à 161 serveurs de commande et de contrôle et confirmé 166 000 compromissions, principalement aux Philippines, en Russie et en Indonésie. Il est actuellement en vente sur les forums criminels russophones pour 104 dollars américains

Contenus illicites

Il s'agit ici d'inscrire dans la blockchain un contenu illicite dans le but de la rendre illégale dans l'ensemble des pays ayant une législation sérieuse sur la cybercriminalité. C'est à la portée de tous.

Une première étude quantitative[36] sur la blockchain du Bitcoin répertorie les contenus illicites suivants :

- Violations de droits d'auteur : liens vers des données piratées, des clés privées.
- Programmes malveillants avec le risque d'activation des antivirus ; rien de significatif à ce stade.
- Violation de la vie privée.
- Contenus politiquement sensibles comme des données du Wikileaks Cablegate.
- Contenus illégaux et répréhensibles, comme la pédopornographie ; phénomène très marginal pour le moment.

Cet article répertorie 1,4% de transactions non-monétaires sur Bitcoin (sur 251 millions de transactions).

[36] A quantitative analysis of the impact of arbitrary blockchain content on bitcoin, http://fc18.ifca.ai/preproceedings/6.pdf

File Type	Via Service? yes	no	Overall Portion	File Type	Via Service? yes	no	Overall Portion
Text	1353	54	87.07 %	Archive	4	0	0.25 %
Images	144	2	9.03 %	Audio	2	0	0.12 %
HTML	45	0	2.78 %	PDF	2	0	0.12 %
Source Code	7	3	0.62 %	**Total**	1557	59	100.0 %

Table 2: Distribution of blockchain file types according to our content-insertion-service and suspicious-transactions detectors.

Gestion de crise

On peut imaginer que si des vidages de comptes étaient opérés en trop grand nombre, la communauté Bitcoin arrêterait toutes les transactions et tenterait de réparer le protocole et de rétablir les comptes dans un état antérieur à la détection de la fraude. De telles situations obligeant à une intervention des équipes de développement du Bitcoin se sont déjà produites deux fois. Une première fois, en août 2010, à la suite de la découverte d'un bug qui avait permis la création de 184 millions de Bitcoins frauduleux qui furent immédiatement annulés. Une seconde fois en mars 2013, à la suite d'une duplication de la Blockchain[37]. Au total, même dans les cas extrêmes de mise en cause du protocole Bitcoin, il est possible d'en limiter les conséquences et d'éviter l'écroulement total du système. Lors de ces rares événements, le principe de décentralisation du Bitcoin cesse temporairement d'être respecté, et une équipe restreinte de développeurs reprend la main et opère des choix qui ne sont pas inscrits d'avance dans le protocole. Ces choix sont faits publiquement et à la suite d'accords entre les développeurs, mais il s'agit quand même d'écarts temporaires inquiétants à la doctrine de base.

Pour les blockchains privées, ce sera plus simple mais il faudra quand même établir des règles et s'y tenir.

[37] Voir http://en.wikipedia.org/wiki/History_of_Bitcoin

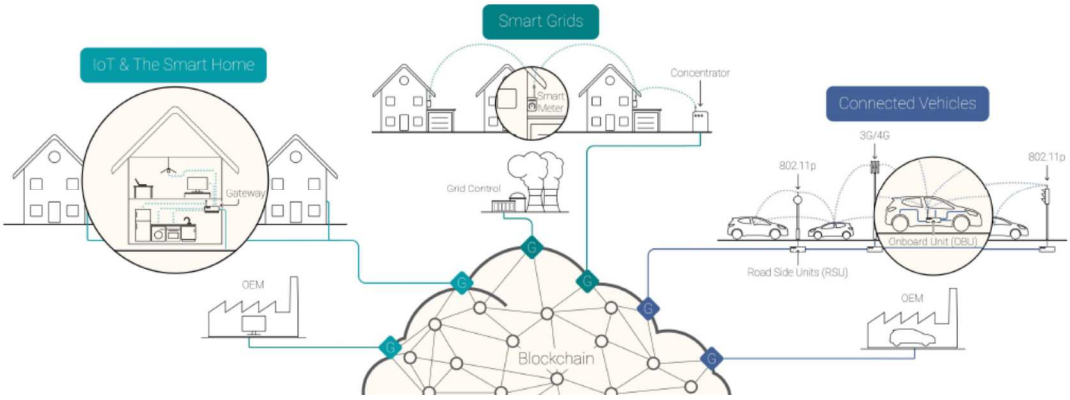
Cas d'usages

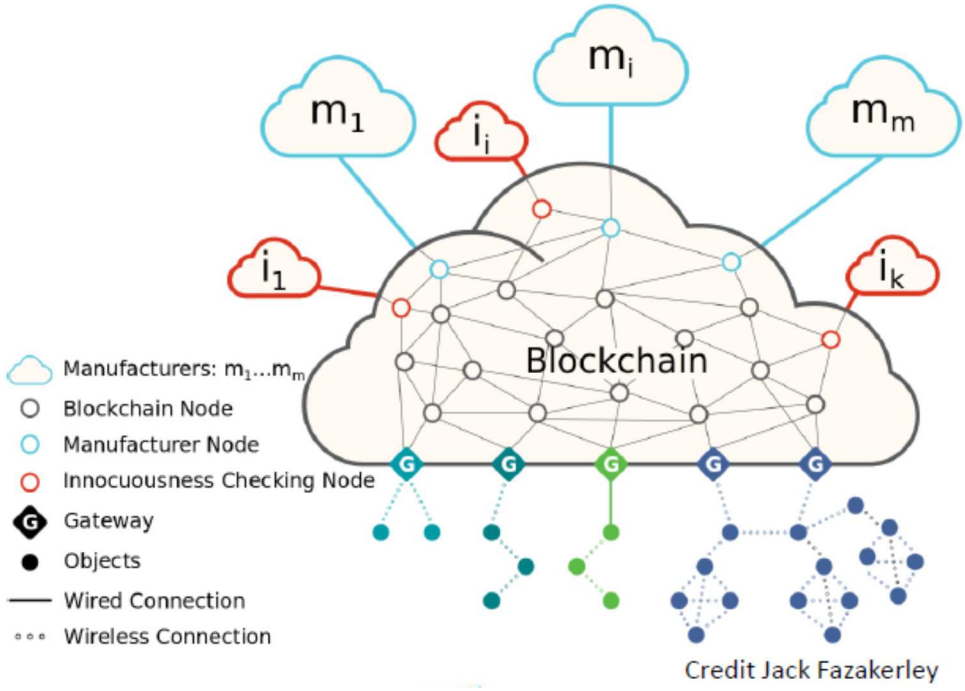
Les idées fleurissent en dehors de la finance : santé, énergie, transport, assurance... Quelques rares projets s'intéressent à la cyber-sécurité elle-même.

Maquettage EIC

Pour EIC, il s'agit principalement de notariser des événements de sécurité sur des infrastructures massives, hyper connectées et non centralisées.

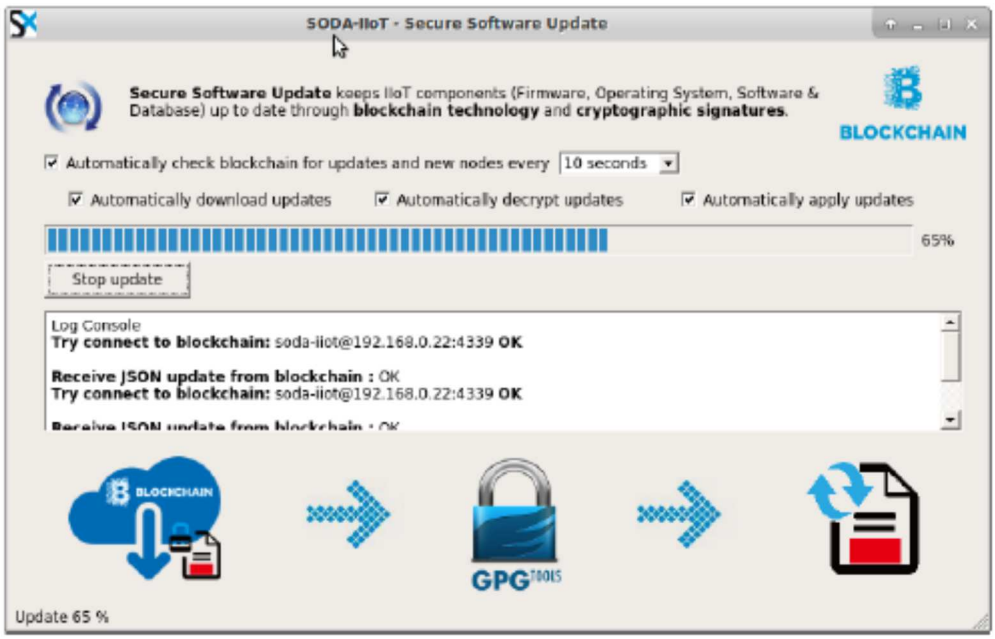
Premier exemple : SODA-IIOT, maintien en condition de sécurité d'une flotte de véhicules (simulation par raspberry)[38]. Le maquettage a été fait sur la solution libre multichain[39].

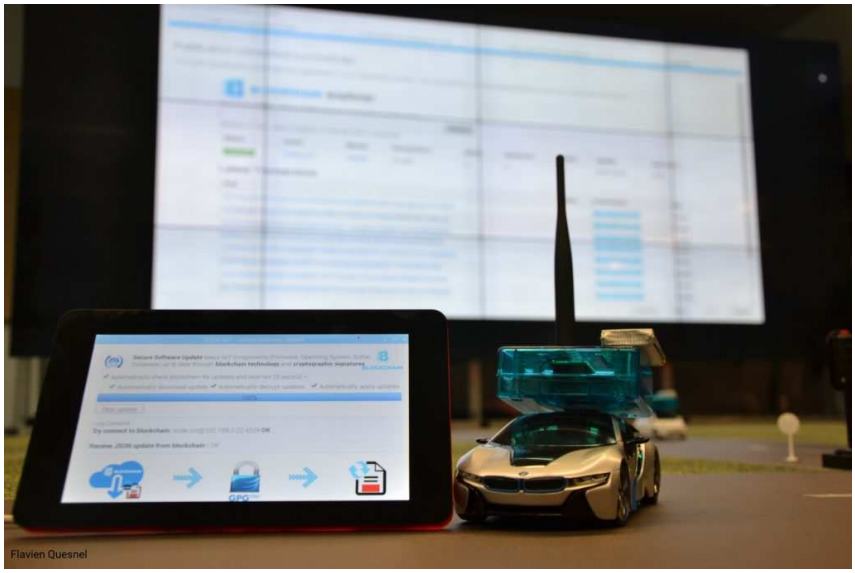




[38] Renaud Sirdey, Aymen Boudguiga, Nabil Bouzerna, Flavien Quesnel, Louis Granboulan, Alexis Olivereau, Anthony Roger, Towards better availability and accountability for IoT updates by means of a Blockchain, IEEE Security & Privacy on the Blockchain (IEEE S&B 2017) an IEEE EuroS&P 2017 AND Eurocrypt 2017 affiliated workshop, avril 2017, https://hal.archives-ouvertes.fr/hal-01516350/document

[39] Voir https://www.multichain.com/





Application à la cybersécurité

Autre exemple, thèse de Mme Dramé-Maigne (Gemalto)[40] :

Deux pistes de recherche seront ensuite explorées dans la thèse de doctorat. L'une d'elles consiste à proposer des solutions visant à simplifier la définition des règles de contrôle d'accès dans le cadre de l'Internet des objets. L'idée est de simplifier et optimiser la définition de ces règles en passant par exemple par plusieurs niveaux d'abstraction à la manière de RBAC. L'autre piste consiste à clairement identifier les risques de sécurité posés par la centralisation de la gestion des règles d'autorisation qui positionne le serveur d'autorisation comme un point d'attaque central, et à proposer des solutions pour réduire ces risques. Pour cela on explorera l'intérêt de méthodes récemment apparues dans la littérature, et consistant à répliquer l'information à protéger un grand nombre de fois pour éliminer le

[40] Voir http://www.adum.fr/as/ed/voirpropositionT.pl?site=PSaclay&matricule_prop=10135

risque d'attaque du système par concentration des attaques sur un point unique. On pourra par exemple s'appuyer sur le principe des BlockChain qui permettent d'assurer l'intégrité de certaines transactions (e.g. Bitcoin) dans un contexte totalement distribué.

La boîte à idées est largement ouverte[41]. On trouve des applications au forensique (autopsie numérique)[42].

The KSI blockchain overcomes two major weaknesses of traditional blockchains, making it usable at industrial scale.

- ***Scalability**: One of the most significant challenges with traditional blockchain approaches is scalability – they scale at O(n) complexity i.e. they grow linearly with the number of transactions. In contrast the KSI blockchain scales at O(t) complexity – it grows linearly with time and independently from the number of transactions.*

- ***Settlement time**: In contrast to the widely distributed crypto-currency approach, the number of participants in KSI blockchain distributed consensus protocol is limited. By limiting the number of participants it becomes possible to achieve consensus synchronously, eliminating the need for Proof of Work and ensuring settlement can occur within one second.*

Il s'agit là d'une tentative, répandue, de supprimer le consensus dans ce qui s'appelle encore une blockchain. La même solution propose un autre usage qui est la cyber-sécurisation des centrales nucléaires UK[43] sans précisions sur ce qui va être tracé et traité.

Autres usages

D'autres usages sont évoqués :

- utilisation de la blockchain pour garantir les échanges de factures entre opérateurs économiques et/ou entités publiques ;
- création et mise en œuvre de smart contracts dans le cadre des contractualisations entre les parties prenantes (entreprises et/ou entités publiques).

Il va de soi que la qualité du passage du monde physique au monde numérique est primordiale. Le minage, s'il y a, lève des ambiguïtés fortement liées au cas d'usage. Le smart contrat, qui devrait simplifier et sécuriser les logiques d'engagement réciproques, rajoute une certaine dynamicité mais ce sont des programmes avec leurs faiblesses...

Les propositions d'emploi de la blockchain pour du contrôle international restent encore au stade des idées. Exemple : proposé par un think-tank indien[44], le contrôle des matières radioactives comme l'uranium. Se pose, ici et ailleurs, la question de la sincérité des données inscrites, mais aussi la

---

[41] Exemples : http://www.information-age.com/technology/security/123460713/how-blockchains-are-redefining-cyber-security

[42] https://www.nist.gov/sites/default/files/documents/2016/11/22/improving_cyber_forensics_and_cybersecurity_through_block_chain_technology_with_truth_based_systems.zatyko.digevid.pdf

[43] https://www.cryptocoinsnews.com/blockchain-cybersecurity-solutions-will-be-used-to-secure-uk-nuclear-plants/

[44] Observer Research Foundation - Preventing Proliferation: Tracking Uranium on the Blockchain, https://www.orfonline.org/wp-content/uploads/2018/04/ORF_Issue_Brief_235_Blockchain-Uranium.pdf

volonté de mise en commun de ces données qui nécessite des accords de partage et des régulations transfrontières. D'autres technologies de sécurité sont invoquées (RFID, NFC) ce qui indique que l'étude de sécurité de ce système de systèmes devra dépasser le cadre strict de la blockchain.

Assurance

Les objectifs d'une alliance entre assureurs et réassureurs suisses[45] autour de l'initiative B3i *Blockchain Insurance Industry* ne sont pas aujourd'hui rendus publics.

Des chercheurs doutent de sa maturité[46]. La communication reste très conceptuelle[47] et au niveau du slogan :

Executives skeptical of the hype should recognize how blockchain's enablement of increased trust and transparency speaks to the heart of the insurance business.

Des startups (comme https://www.utocat.com/fr/) proposent des solutions pour l'assurance mais sans diffuser la moindre information publique sur une technologie dite de confiance.

[45] Aegon, Allianz, Munich Re, Swiss Re and Zurich, https://www.allianz.com/en/press/news/commitment/sponsorship/161018-insurers-and-reinsurers-launch-blockchain-initiative-b3i/

[46] Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?, http://www.mdpi.com:8080/1999-5903/10/2/20/pdf

[47] http://www.ey.com/Publication/vwLUAssets/EY-blockhain-in-insurance/$FILE/EY-blockhain-in-insurance.pdf

Minage

C'est l'avancée principale qui donne lieu à de multiples publications. Il ne s'agit pas à proprement parler d'une avancée mathématique comme en produit la cryptologie tous les dix ans (cryptographie homomorphe en 2009, par exemple), mais d'une mise en pratique et d'une évaluation grandeur nature d'un algorithme pair-à-pair qu'autorise le développement des réseaux (fibre optique).

Nous ne donnons ici que quelques pistes sans lancer un débat sociétal sur la décentralisation dans un pays jacobin. Fondamentalement, la validation par la communauté est plus complexe que le vote majoritaire car elle doit apporter la confiance dans un monde numérique où les malhonnêtes restent largement impunis aujourd'hui. De plus l'immuabilité de la blockchain pose le problème de la correction des erreurs et des évolutions représentées par les *forks* (on retrouve le dilemme *safety/security : patch or not ?*).

Fonctions

Le minage poursuit trois objectifs principaux :

- protéger la chaîne de blocs contre toute manipulation ;
- permettre la création contrôlée de nouvelles pièces dans le cas particulier des cryptomonnaies ;
- inciter les pairs à gérer en commun la blockchain, criminels compris.

Pour les usages non monétaires, le second objectif peut créer d'autres valeurs ou critères mais, fondamentalement, il semble difficile de faire abstraction de valeurs d'échange dans les transactions.

Le minage est implanté par des mécanismes de type challenge sous la forme d'un problème de recherche informatique avec les caractéristiques suivantes :

- difficile à résoudre
- facile à vérifier
- à difficulté réglable
- à gagnant imprévisible

Une loterie ou un jeu prouvablement équitable…

Proof-of-Work (PoW)

La preuve de calcul est considérée très vite comme la seule solution au problème des généraux byzantins (publié en 1982)[48].

Des généraux de l'armée byzantine campent autour d'une cité ennemie. Ils ne peuvent communiquer qu'à l'aide de messagers et doivent établir un plan de bataille commun, faute de quoi la défaite sera inévitable. Cependant un certain nombre de ces messagers peuvent s'avérer être des traîtres, qui essayeront donc de semer la confusion parmi les autres. Le problème est donc de trouver un algorithme pour s'assurer que les généraux loyaux arrivent tout de même à se mettre d'accord sur un plan de bataille.

[48] Proof That Proof-of-Work is the Only Solution to the Byzantine Generals' Problem, https://gist.github.com/oleganza/8cc921e48f396515c6d6

Il a été démontré qu'en utilisant uniquement des messages oraux, ce problème des généraux byzantins peut être résolu, si et seulement si plus des deux tiers des généraux (messagers) sont loyaux. Ainsi un seul traître peut confondre deux généraux loyaux. De plus, le problème peut être résolu pour un nombre quelconque de messagers renégats si les messages sont écrits (et non falsifiables).

D'autres arguments plus économiques ont été développés[49].

Le minage traditionnel du bitcoin du type proof-of-work (CPU based) s'est transformé en artillerie lourde[50].

Il s'agit de transformer de l'énergie consommée en une valeur monnayable (bitcoin, gas). Les optimistes constatent que la moitié de l'énergie de la machinerie informatique est dépensée en vain. Mais la récompense liée au minage échappe de plus en plus à l'individu. Il faut passer par des tiers (rarement de confiance) et qui peuvent acquérir une position monopolistique.

Ethereum[51] propose d'estomper cette course à la puissance CPU avec sa fonction Ethash.

One plague of the Bitcoin world is ASICs. These are specialised pieces of compute hardware that exist only to do a single task. In Bitcoin's case the task is the SHA256 hash function. While ASICs exist for a proof-of-work function, both goals are placed in jeopardy. Because of this, a proof-of-work function that is ASIC-resistant (i.e. difficult to implement in specialized compute hardware) has been identified as the proverbial silver bullet.

Two directions exist for ASIC resistance; firstly make it sequential memory-hard, i.e. engineer the function such that the determination of the nonce requires a lot of memory and bandwidth such that the memory cannot be used in parallel to discover multiple nonces simultaneously. The second is to make the type of computation it would need to do general-purpose; the meaning of \specialised hardware" for a general-purpose task set is, naturally, general purpose hardware and as such commodity desktop computers are likely to be pretty close to \specialised hardware" for the task. For Ethereum 1.0 we have chosen the first path.

L'analyse est incomplète : je ne vois pas pourquoi une architecture dédiée à ce calcul à base de FPGA (circuits programmables) ne pourrait pas paralléliser ou au minimum accélérer les calculs.

Enfin, des analyses autour de la théorie de la complexité (Bennett et Kolmogorov)[52] proposent de rendre les preuves de travail utiles à quelque chose (extraire de l'or ?) :

- recherche de nombres premiers (Primecoin, le pionnier, semble avoir disparu) ;
- déterminer le repliement des protéines ?
- autres grid-calculs ?

[49] Nothing is Cheaper than Proof of Work, http://www.truthcoin.info/blog/pow-cheapest/

[50] https://en.bitcoin.it/wiki/Mining_hardware_comparison et https://en.bitcoin.it/wiki/Mining_rig

[51] Voir http://gavwood.com/paper.pdf

[52] Les preuves de travail, http://cristal.univ-lille.fr/~jdelahay/pls/2014/245.pdf

Proof-of-Stake (PoS)

Ethereum retarde constamment le basculement vers ce minage proposé par son inventeur. Il fait l'objet de critiques[53] et n'a pas encore subi l'épreuve du feu[54].

Ceci étant dit, en ce qui concerne l'augmentation du nombre d'ethers, le postulat de départ est faux : il n'y aura pas génération de 15 millions d'ethers chaque année. Ce taux d'émission correspond à celui qui est en cours aujourd'hui, avec le minage en Proof of Work. Avec la validation des blocs en Proof-of-Stake, qui définit un taux de rendement par inflation, le taux d'accroissement du nombre d'ethers devrait se situer entre 0,1 et 2 % par an, soit au maximum 2 millions de nouveaux ethers la première année en se fondant sur une base arbitraire de 100 millions d'ethers au moment du passage en Proof of Stake.

Delegated Proof-of-Stake (DPoS)

La preuve d'enjeu ou preuve de participation déléguée[55] confie aléatoirement à un groupe de délégués des enjeux plus importants. « Cette méthode utilise certains avantages que l'on retrouve dans un vote d'actionnaires où le compte sélectionné doit agir de manière responsable. Néanmoins la méthode réintroduit la dangereuse attaque Sybil[56] dans laquelle l'identité d'un utilisateur peut être piratée et utilisée à mauvais escient » (wikipedia).

Dans les systèmes DPoS, les utilisateurs « votent » pour sélectionner des « témoins » auxquels ils ont confiance pour valider les transactions. Ceux qui ont recueilli le plus de votes gagnent le droit de valider les transactions. Ils peuvent même déléguer ce pouvoir de vote à d'autres utilisateurs.

Proposée initialement par Daniel Larimer (*BitShares*), des BC récentes l'ont adopté (Eos, Tezos) sans que l'on puisse aujourd'hui garantir leur propriétés et leurs résistances.

Le nombre de ces délégués varie de 21 à 101… Un premier travail théorique[57] fixe un nombre bien plus élevé en fonction d'hypothèses plus réalistes sur la taille du système réel.

8.1 Minimum Committee Size

To appreciate the benefits of delegation, recall that in the basic protocol (π_{DPoS}) a committee member selected by weighing by stake is honest with probability $1/2 + \epsilon$ (this being the fraction of the stake held by honest players). Thus, the number of honest players selected by k invocations of weighing by stake is a binomial distribution. We are interested in the probability of a malicious majority, which can be directly controlled by a Chernoff bound. Specifically, if we let Y be the number of times that a malicious committee member is elected then

$$\begin{aligned}\Pr[Y \geq k/2] &= \Pr[Y \geq (1+\delta)(1/2-\epsilon)k] \\ &\leq \exp(-\min\{\delta^2, \delta\}(1/2-\epsilon)k/4) \\ &< \exp(-\delta^2(1/2-\epsilon)k/4)\end{aligned}$$

for $\delta = 2\epsilon/(1-2\epsilon)$. Assuming $\epsilon < 1/4$, it follows that $\delta < 1$.

Consider the case that $\epsilon = 0.05$; then we have the bound $\exp(-0.00138 \cdot k)$ which provides an error of $1/1000$ as long as $k \geq 5000$. Similarly, in the case $\epsilon = 0.1$, we have the bound $\exp(-0.00625k)$ which provides the same error for $k \geq 1100$.

We observe that in order to withstand a significant number of epochs, say 2^{15} (which, if we equate a period with one day, will be 88 years), and require error probability 2^{-40}, we need that $k \geq 32648$.

---

[53] https://medium.com/@tuurdemeester/critique-of-buterins-a-proof-of-stake-design-philosophy-49fc9ebb36c6

[54] https://cointelegraph.com/news/the-inevitable-failure-of-proof-of-stake-blockchains-and-why-a-new-algorithm-is-needed

[55] Voir https://hackernoon.com/what-is-delegated-proof-of-stake-897a2f0558f9

[56] Une **attaque Sybil** consiste à contourner le système de réputation d'un réseau pair à pair en créant une grande quantité d'identités et en les utilisant pour avoir une influence disproportionnée

[57] Voir https://eprint.iacr.org/2016/889.pdf

Byzantine Fault Tolerant (BFT) Consensus

Plus récemment pour les blockchains d'entreprise (privées ou à autorisations) la tendance consiste à utiliser des protocoles de consensus plus traditionnels (Byzantine Fault Tolerance, 2017). Le consensus BFT est basé sur l'idée qu'un groupe de validateurs présélectionnés et autorisés va créer, vérifier et attester de nouveaux blocs. Ces validateurs créent à tour de rôle de nouveaux blocs et soumettent un bloc nouvellement créé à d'autres validateurs pour vérification et vote. Chaque validateur vote pour un bloc en le signant cryptographiquement. Une fois que le réseau reçoit au moins un vote majoritaire au 2/3 pour un bloc, il est finalisé et ajouté à la blockchain. Etant donné que les blocs valides contiendront les signatures numériques des validateurs, les nœuds se synchronisant avec la chaîne de blocs n'ont qu'à vérifier les signatures des validateur dans un bloc pour s'assurer qu'ils suivent la chaîne de blocs correcte. Le consensus BFT nécessite généralement un nombre minimum de nœuds pour que le réseau puisse fonctionner face à des acteurs malveillants. Par rapport au PoW, cette approche nécessite également l'échange de plus de messages de protocole pour coordonner le processus de consensus, ce qui limite son évolutivité. Alors que PoW peut supporter des milliers de nœuds, le BFT est limité à plusieurs centaines.

Autres

Slimcoin faisait le constat, en 2014, que le PoW est nécessaire, au début, pour constituer une masse minimale de crypto-monnaie, mais qu'après une combinaison de PoW, PoS et de Proof-of-burn (PoB, destruction de monnaie) renforce la sécurité de la Blockchain. Depuis la solution semble avoir disparu, comme beaucoup d'autres… Hyperledger propose sa propre grille d'analyse.

TABLE 1. COMPARISON OF PERMISSIONED CONSENSUS APPROACHES AND STANDARD PoW

	Permissioned Lottery-based	Permissioned Voting-based	Standard Proof of Work (Bitcoin)
Speed	GOOD	GOOD	POOR
Scalability	GOOD	MODERATE	GOOD
Finality	MODERATE	GOOD	POOR

Minage écologique?

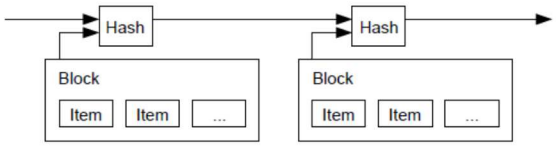
Dans le cas général d'une blockchain publique, est-il possible de miner sobrement et de donner une meilleure chance à tous sans arbitre centralisé ? Dans tous les cas de figure, il semble que les plus possédant (riches en crypto-monnaie ou possédant les plus de comptes d'accès, de mémoire, de cpu, etc.) resteront favorisés, mais toute loterie ou jeu aléatoire est victime de ce biais. Proposons une idée pour montrer la difficulté de cette recherche.

L'idée principale serait de **ralentir le minage**, c'est-à-dire de forcer les calculs à sens unique à utiliser une horloge beaucoup plus lente que celle des CPUs actuels. Il s'agirait en fait de caler les calculs sur un signal répétitif de type top départ (par exemple toutes les secondes). Cette horloge (suite de valeurs aléatoires imprédictibles) utiliserait une idée liée à l'horodatage du bitcoin[58].

[58] article fondateur de Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



Il s'agirait de *hasher* des événements du futur à un intervalle régulier. Les sources d'aléas imprédictibles sont nombreuses : les loteries physiques (à base de boules), les compteurs atomiques, les tweets, les journaux, les cours de la bourse, etc. La formule serait publique et vérifiable par tous. On génère ainsi une suite de nombres (512 bits, par exemple) faisant office de tics d'horloge pour le minage : Tm_1, Tm_2, …, Tm_k, TM_{k+1}, etc.

Cela imposerait alors de vérifier qu'un mineur ne puisse exécuter l'algorithme de minage (un calcul de *hash*) qu'à ce rythme et donc **une seule fois par événement d'horloge**. Un mineur i serait caractérisé par un bi-clé de minage ($KminPub_i$,$KminSec_i$) formé d'une clé publique et d'une clé secrète. Il lui faudrait donc signer chaque calcul avec sa clé secrète de minage de façon que la communauté puisse s'assurer que le résultat n'est fourni qu'une seule fois par tic de minage Tm_k. Ce contrôle pourrait-être systématique ou aléatoire (mécanisme à préciser).

Il faudrait de préférence distinguer ce bi-clé de minage de celui nécessaire aux transactions. Cela permettrait de **séparer les rôles** et de protéger, quelque peu, les acteurs. Un acteur (homme ou machine) pourrait décider d'être : un client, un mineur, un client-mineur. Le minage pourrait-être occasionnel ou systématique. Il faudrait sûrement **encourager les mineurs systématiques** pour assurer un rythme régulier de validation des blocs de la chaine.

Il faudrait dans ce cas limiter la puissance d'un individu, d'une organisation ou d'un robot à acquérir une puissance de minage lui permettant de pervertir la blockchain (*sybil attacks*). Pour cela, la technique du **Proof-of-Work classique pourrait être utilisée à l'enrôlement**. Typiquement un bi-clé de minage n'est introduit dans la communauté comme **clé active de minage** qu'après un temps de minage classique lié à la taille du réseau (24 heures, par exemple, pour tout nouvel arrivant). Les **clés publiques actives de minage** seraient stockées dans la blockchain.

La fonction de minage (formule à préciser à base d'un hash avec un aléa) devrait donner à chaque mineur une chance égale de gagner à ce qui s'apparente, dans ce cas, à **une vraie loterie**. Gagner à la loterie consiste à trouver un résultat commençant, par exemple, avec un nombre de zéros fixé par le système. Il s'agirait d'avoir la garantie, en fonction du nombre de mineurs actifs estimé, d'avoir suffisamment de gagnants pour valider le nouveau bloc de la chaîne. Si le quota n'est pas atteint, on peut attendre la loterie suivante (toujours rythmée par les Tm_k). Cette loterie serait assortie à des gains variés selon la nature du cas d'usage de la blockchain. Dès qu'un seuil de gagnant est atteint pour la validation de la blockchain, on la valide et on passe au bloc suivant qui démarre avec un $Tm_{k'}$ ultérieur.

Il faudrait étudier :

- La validité des concepts (attaques du système)

- L'algorithmique précise avec ses formules
- Le calibrage des variables
- L'intégration dans des logiciels libres diffusés
- Une expérimentation in situ
- Evaluer le rythme atteignable de validation des blocs
- L'acceptation par les usagers d'une inscription différée

Cela montre la difficulté à remplacer des techniques de minage éprouvées par l'usage.

Ne pas miner ?

Enfin, de nouvelles idées proposent de se passer du minage[59].

Par une approche de type tombola, le protocole devrait fournir : un protocole de tombola multipartite, un schéma de preuve de transcription ; un schéma de preuve d'engagement, un mécanisme de subvention. Tout cela en remplaçant la récompense en crypto-monnaie par des tickets de tombola. L'article, au titre racoleur, décrit un système cryptographique complexe. Attendons sa réalisation pour en mesurer les éventuelles vertus. Une analogie est faite avec le jeu de grattage « gratta a vinci » mais rien n'est dit comment limiter la possession de tickets de tombola ou comment s'assurer qu'il y a un gagnant.

Il s'agit là de pistes très fécondes de travaux de recherche…

Tezos emploie le terme de boulanger à la place de miner. Importance de la novlangue…

[59] Beyond Bitcoin, https://eprint.iacr.org/2016/747.pdf

SmartContrats

Les smart-contracts et les langages informatiques des crypto-monnaies restent encore aujourd'hui au stade expérimental.

Nous donnons quelques pistes sans répondre à la question philosophique sous-jacente : quel est le pourcentage des contrats entre humains qui peuvent s'automatiser, c'est-à-dire ne plus accepter d'arrangement, de cas particuliers, etc ?

Leur sécurité relève de preuves formelles de sécurité ce qui n'est pas encore la pratique la plus répandue et qui dépend aussi fortement des langages utilisés. Le langage le plus utilisé proposé par Ethereum est Solidity avec une syntaxe proche de Javascript[60].

Le langage de script Ethereum est présenté comme "Turing-complete", c'est à dire qu'il permet d'écrire des programmes avec des boucles, une possibilité qui a été soigneusement écartée par le langage de script Bitcoin pour des raisons de sécurité. En effet, si des boucles sont possibles, le réseau peut faire l'objet d'une attaque dite "en déni de service" (Denial of Service ou DoS en anglais), avec des scripts qui demanderaient aux nœuds du réseau d'exécuter des boucles sans fin, monopolisant les capacités de calcul du réseau. Pour prévenir ce risque, le mécanisme prévu par le protocole Ethereum comporte des commissions de transactions proportionnelles au nombre de cycles de calcul exigés par le script de la transaction. Cependant, la commission est perçue seulement par le premier valideur qui inclut la transaction dans un bloc mais ceux qui construisent les blocs suivants doivent la valider aussi. Ils ont donc une incitation à ne pas vérifier un script complexe. Comment ce risque pourrait-il être évité ?

Bogue d'appel récursif DAO

Pour une analyse de l'attaque, on peut se référer aux nombreux articles la détaillant[61].

La plateforme DAO (decentralized autonomous organisation), qui détient 9,2 millions d'Ether, soit l'équivalent de 134 millions de dollars, a été la cible au matin du 17 juin 2016 d'une attaque qui exploite une vulnérabilité dans le code des smart contracts et siphonne des dizaines de millions d'ether. Un portefeuille, identifié comme le réceptacle du butin, détient déjà 3,5 millions d'ether, soit 47 millions de dollars au taux de conversion actuel (14 dollars pour un ether).

Les forums de discussion des geeks ont souligné la maladresse de la programmation du smartcontrat en question.

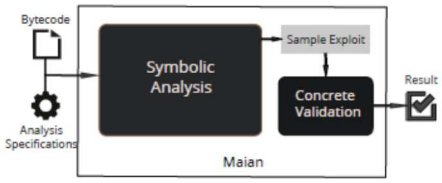
Il n'y a pas eu de vol de TheDAO. La vulnérabilité à été découverte par l'utilisateur Eththrowa de Reddit et Slock.it l'a corrigé en moins de 24h. Slock.it a simplement oublié que patcher un réseau en p2p public en furtive aurait été une meilleure idée, que de publier ça sur Github accompagné d'un CP sur Medium par Tual. La narrative étant développé sur une base fausse, il n'y a eu aucun vol. Il y a eu un déploiement d'une médiocrité (vite fait, mal fait) jamais vu pour un réseau valorisé à plus d'1 milliard de $.

[60] https://www.ethereum-france.com/reponses-sur-ethereum/

[61] Comme http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/

Contrats non sécurisés

Un article[62] recense l'ensemble des problèmes rendus possibles par l'instabilité de programmes non prouvés formellement autour des bonnes propriétés de sécurité :



Category	#Candidates flagged (*distinct*)	Candidates without source	#Validated	% of true positives
Prodigal	**1504** (*438*)	1487	1253	*97*
Suicidal	**1495** (*403*)	1487	1423	*99*
Greedy	**31,201** (*1524*)	31,045	1083	*69*
Total	34,200 (2,365)	34,019	3,759	89

Table 1: Final results using invocation depth 3 at block height BH. Column 1 reports number of flagged contracts, and the distinct among these. Column 2 shows the number of flagged which have no source code. Column 3 is the subset we sampled for concrete validation. Column 4 reports true positive rates; the total here is the average TP rate weighted by the number of validated contracts.

- Des contrats prodigues ou généreux - des contrats intelligents qui, lorsqu'ils sont attaqués, envoient des fonds pour les garder en sécurité à la mauvaise adresse Ethereum (attaquant ou non) ;
- Des contrats gourmands ou gloutons - des contrats intelligents qui peuvent être bloqués par quelqu'un d'autre et geler des fonds pour toujours ;
- Des contrats suicidaires - des contrats intelligents qui peuvent être tués par quelqu'un d'autre et pas seulement par le propriétaire.

L'analyse a porté (avec l'outil intitulé Maian) sur 970 898 contrats et a détecté plus de 34 000 contrats vulnérables.

Complexité

Par ailleurs, le langage de script Ethereum peut conduire à des transactions très complexes : la fameuse DAO comportait près de 700 lignes de code (sans compter les lignes de commentaires).

Comment peut-on envoyer des millions de dollars sur un tel script quand on sait qu'il faut s'attendre à 10 bugs pour 1000 lignes de code ? Dans le cas de la DAO, un bug a été exploité par un hacker…

Personne ne conteste sérieusement que c'était une erreur d'envoyer autant d'ether dans un contrat à un stade aussi précoce du développement d'Ethereum. Malgré les avertissements multiples de la communauté, et du site de The DAO, l'ampleur des montants envoyés au contrat a été inattendue mais surtout incontrôlable, dans la mesure où aucun plafond de montant collecté n'avait été défini dans le contrat. Et une forme d'enthousiasme communicatif a sans doute conduit de nombreuses personnes à se lancer sans méfiance dans cette aventure.

Aujourd'hui plus qu'hier, il est évident pour tous que le framework de développement des contrats Ethereum n'est pas finalisé. Les modèles sont quasiment inexistants, les logiciels en cours de développement et les bonnes pratiques en cours de conception.

[62] Finding The Greedy, Prodigal, and Suicidal Contracts at Scale, http://ilyasergey.net/papers/maian-draft.pdf

Futur

Maturité

La maturité des technologies Blockchain n'est aujourd'hui mesurable qu'à la réalité de déploiements suffisamment massifs. Cela n'empêche en rien les expérimentations à des échelles plus réduites en laboratoire, mais l'extrapolation reste difficile étant donné le nombre de paramètres en jeu et l'inconnue des attaques auxquelles il faudra faire face (ce sont des théorèmes d'indécidabilité comme le théorème du virus qui gouvernent la cybersécurité).

En cryptographie, depuis 2000 surtout, s'est développée la formalisation mathématique de la preuve de sécurité qui est la preuve qu'un ensemble d'algorithmes cryptographiques respecte les définitions de sécurité qui leur sont requises. Cela permet, notamment, d'estimer les difficultés calculatoires sous des hypothèses minimales (fonctions à sens unique, existence de l'ordinateur quantique, ressources disponibles, etc.). Mais, il a également été prouvé très tôt que ces preuves de sécurité sont à prendre avec précaution[63].

Le minage, garant de la décentralisation, ne semble pas avoir encore atteint cette maturité, m^me si de premiers résultats théoriques sont disponibles. L'épreuve empirique, qui semble nécessaire, apparaît parfois comme la seule mesure de sa robustesse. Il faudrait pourtant pouvoir adapter ce minage aux propriétés de sécurité recherchées. Le critère privé/public apparaît, bien sûr, comme essentiel.

Limitations

On cite toujours le nombre de transactions absorbables à la seconde. On est alors très loin des capacités des systèmes dits centralisés. Mais des solutions sont explorées aujourd'hui pour la montée en charge comme la parallélisation de blockchains collatérales, le recours à des bases de données liées à la blockchain ou encore la création d'une nouvelle couche de protocole allégé et rapide « au-dessus » de la blockchain mais bénéficiant de sa sécurité.

Mais d'autres paramètres sont à considérer[64] :

- La taille maximale des blocs (courmment 1 MB aujourd'hui)
- Le passage à l'échelle
- La complexité des smartcontrats
- La qualité de la programmation
- Le modèle économique
- Etc.

De nouvelles architectures sont déjà proposées pour contourner ces limitations[65].

"delivery at the scale of Facebook and support transactions at the speed of Visa"

---

[63] Voir, par exemple, https://link.springer.com/chapter/10.1007%2FBFb0055731

[64] Beyond Bitcoin: A Critical Look at Blockchain-Based Systems, http://www.mdpi.com/2410-387X/1/2/15/pdf

[65] A better blockchain architecture, https://www.rchain.coop/#home
https://github.com/rchain/

Obscurité

On peut souvent s'interroger sur le discours marketing dénué de toute approche scientifique…

Voici, sans commentaire, quelques annonces de startup françaises :

http://www.agate-id.com/

Agate ID uses a proprietary blockchain technology to help you process, manage and safeguard sensitive data.

https://uniris.io/fr/

Uniris est une solution biométrique couplée à une technologie Blockchain qui permet de s'authentifier en se passant de ses login et mots de passe, de payer sur internet sans carte bancaire, et d'en finir avec l'insécurité sur internet.

Nouvelle Génération de Blockchain : Uniris permet de gérer en moins d'une seconde des milliards de transactions pour l'ensemble de la population mondiale. Uniris repose sur une nouvelle génération de Blockchain (12 brevets déposés) qui tout en gardant la transparence et la sécurité de la Blockchain permet d'y associer les identités digitales, les smart-contract et l'archivage des données.

Conclusion

La blockchain, par la mise en commun à grande échelle de techniques cryptographiques, de communications pair-à-pair, de contrôles décentralisés représente clairement une avancée de rupture pour des usages qui vont bien au-delà des monnaies électroniques.

Comme solution de confiance, elle nécessite d'abord l'adhésion de ses usagers autour d'une compréhension de ses objectifs et de ses fonctions. Cela n'empêche en rien, des solutions propriétaires mais leur impose une certaine transparence. L'obscurité sied mal à la sécurité.

Elle n'est une solution de sécurité qu'à la condition d'une analyse complète de ses propriétés (triptyque traditionnel Disponibilité Intégrité Confidentialité). S'attacher à des briques consolidées par la pratique est une condition minimale de succès.

Le respect de la vie privée représente un défi majeur comme pour l'ensemble de la numérisation de la société mais avec la dimension supérieure de l'immuable.

Plus elle connaitra des succès, plus elle sera attaquée.

Rien n'est simple au royaume du consensus numérique qu'on l'appelle minage, loterie ou tombola.

Peu de solutions survivront au foisonnement artificiel actuel.

-_-_-_-