Blockchain : Éléments d'explication et de vulgarisation, Pourquoi s'intéresser à la blockchain aujourd'hui ?

Philippe Marrast

Séminaire IFERISS-IMH : Blockchain et Santé : Perspectives d'applications et enjeux juridiques
Intervention du 12 Octobre 2018

Blockchain : Éléments d'explication et de vulgarisation

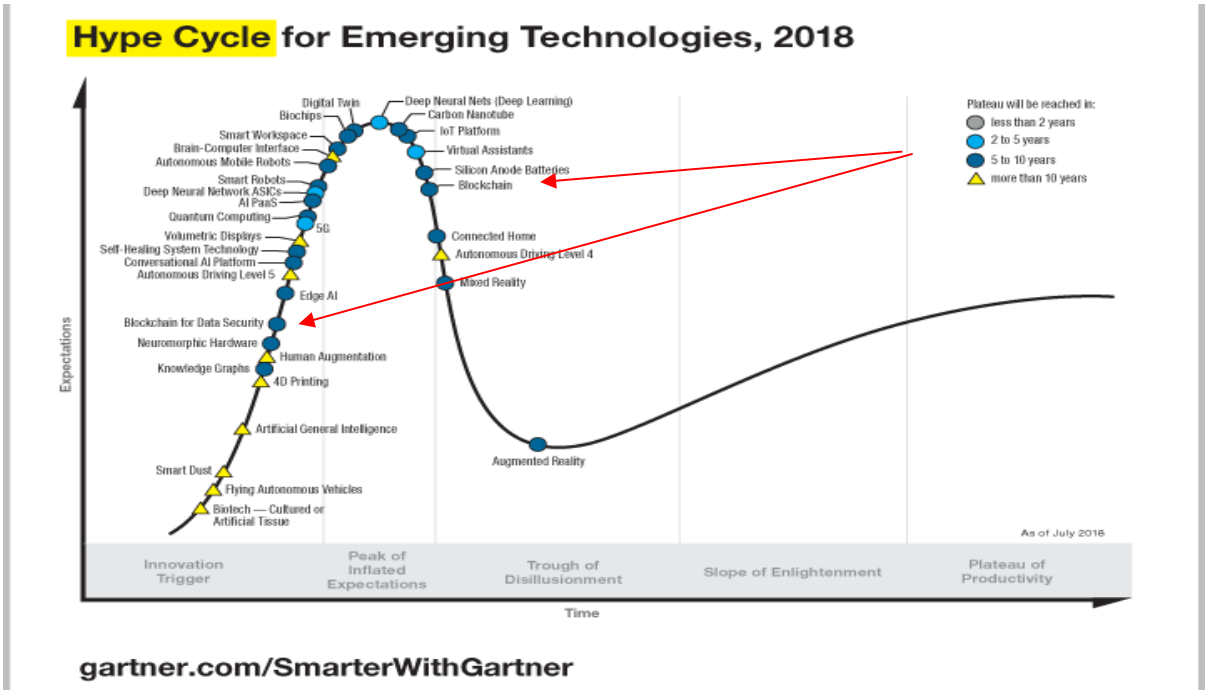
Philippe Marrast,
MCF Sciences de l'information et de la communication, Phd en Informatique

CERTOP CNRS | IUT de Tarbes | IFERISS

Pourquoi s'intéresser à la blockchain aujourd'hui ?

Depuis plusieurs années, notamment avec l'émergence et l'adoption massive des cryptomonnaies, en particulier le BitCoin, la technologie blockchain est devenue un centre d'intérêt d'actualité que ce soit pour les sciences en tant qu'innovation technologique qui traverse nombre de domaines industriels ou sociétaux, pour l'économie comme nouveau marché spéculatif, pour l'environnement du fait de l'énergie importante que ces technologies consomment, ou encore pour le droit et la protection de la donnée.

Malgré un engouement très fort des promoteurs de cette technologie et un marché extrêmement dynamique généré, la blockchain reste encore, du point de vue du groupe *Gartner*, une technologie émergente qui mettra encore quelques années à se stabiliser et à devenir « mature ». Les applications dans le domaine de la santé n'échappent pas à cette réalité et doivent encore faire leurs preuves.



Étant chercheur dans le domaine de la santé, des technologies et me posant plus particulièrement la question du déplacement et de la transformation des inégalités sociales de santé du fait de l'équipement technologique des organisations de santé, de l'activité des professionnels, de la prise en charge des patients et des populations, la technologie Blockchain est un sujet de curiosités et d'interrogations notamment du point de vue des inégalités sociales de santé.

Cette présentation propose de revenir sur l'histoire de la blockchain, puis de développer les principes fondamentaux de son fonctionnement pour ouvrir une discussion entre promoteurs de cette technologie et détracteurs. En conclusion j'ouvrirai quelques pistes de réflexion sur cette technologie prometteuse et ces incidences en termes d'inégalités de santé.

Histoire de la blockchain

1991 : La technologie Blockchain est initialement un système d'horodatage et de certification de documents qui a été conceptualisée par un collectif de chercheurs (Stuart Haber and Stornetta)

1995 : Le NY Times met en place la première blockchain dans le journal, cette technologie qui est toujours active, est la plus longue blockchain de l'histoire.

1994-2005 : Nick Szabo développe les concepts de base des cryptomonnaies, en particulier du concept de minage et lance Bitgold, le précurseur de Bitcoin.

2009 : Satoshi Nakamoto, qui est à ce jour encore non identifié (cela pourrait être Nick Szabo ou un collectif ou un inconnu) publie un article qui pose les bases de Bitcoin

2013-2015 : Vitalik Buterin développe Ethereum qui est à la fois une monnaie cryptographique (la 2ème après Bitcoin) et une plateforme applicative distribuée.

L'air du temps : Actuellement, la blockchain pourrait venir s'insérer comme élément d'un méta système qui mêlerait les technologies de big-data (cloud), la blockchain (intégrité référentielle) et les IA (deep learning, machine learning) : Deep Brain Chain, Cortex Virtual Machine…

Domaines d'utilisation de la blockchain

Aujourd'hui, de nombreux domaines s'intéressent ou ont développé des produits et des solutions techniques basées sur la technologie Blockchain.

Du fait de l'engouement et des promesses de la blockchain en matière de rapidité et de sécurisation des transactions, **le secteur de la banque et de la finance** est largement impliqué dans cette technologie. Différents prestataires et acteurs du domaine proposent des solutions de portefeuilles électroniques, permettent des transactions financières rapides et sécurisées entre particuliers et professionnels, et entre organismes bancaires.

La certification de documents est un autre grand domaine concerné par cette technologie. Du fait de la capacité à rendre l'information irrépudiable et publiquement certifiée, différentes mises en œuvre à base de blockchain ont été réalisées. On peut citer par exemple, l'état civil et le permis de conduire à base de blockchain développé par le gouvernement Australien, la certification de diplômes ou différents documents notariés. Des solutions existent aussi pour la protection des droits d'auteurs, ou la protection industrielle.

Associée à des technologies d'objets connectés, la blockchain pourrait jouer un rôle majeur dans **le secteur de la logistique et de la distribution.** La blockchain permet potentiellement d'opérer un suivi certifié et un contrôle sécurisé lors du transport. La sécurité, la traçabilité alimentaire et le respect de la chaîne du froid sont là aussi des enjeux majeurs dont certains grands acteurs se sont emparés (IBM trust Food, Carrefour).

Dans le domaine de la santé des applications à grande échelle de cette technologie sont encore très peu développées, mais il existe des expérimentations dans le domaine des essais cliniques, pour la traçabilité des produits pharmaceutiques, ou encore comme technologie de support pour des dossiers patients électroniques.

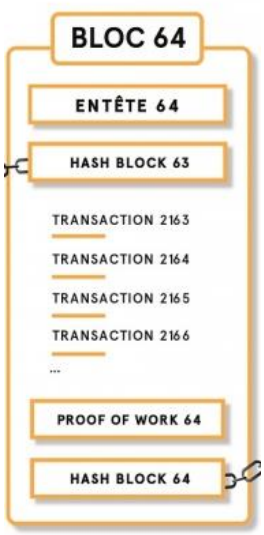
Principes de fonctionnement de la blockchain

Le bloc

Les blocs d'une blockchain peuvent contenir **différents types de données**, des enregistrements de transactions (Bitcoin), des images, du texte, des applications, …

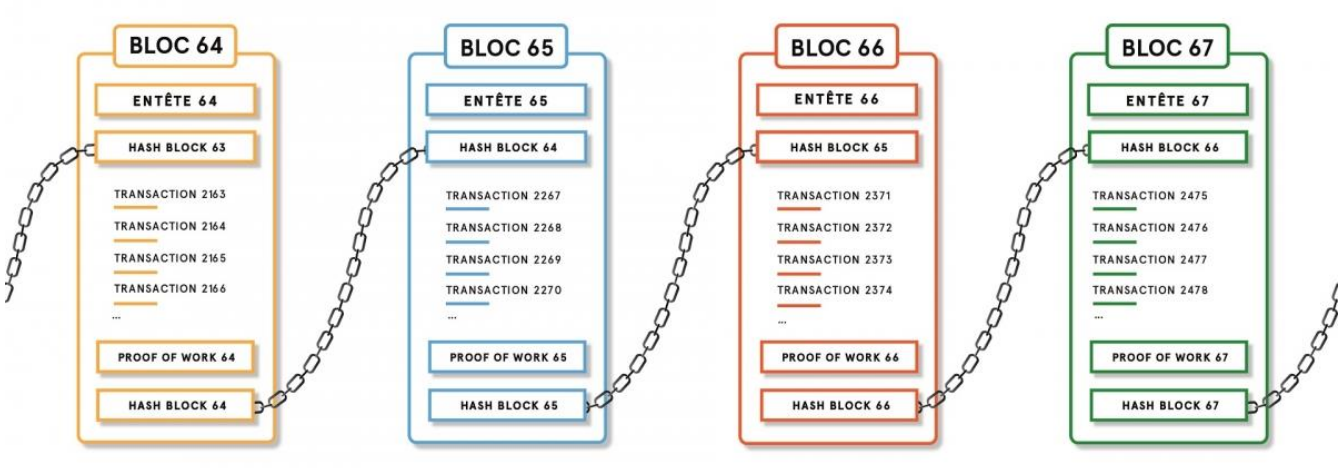
Ces données peuvent être chiffrées ou être enregistrées en clair.

Les en-têtes de blocs sont des données techniques et des métas-données (horodatage, propriétaire, signature électronique, chainage…).



La chaine

Dans une blockchain, chaque bloc d'information est lié, « chaîné » au bloc précédent. Ce chaînage s'effectue à l'aide de la **signature numérique** de chaque bloc qui est transmise au suivant dans la chaîne. Cette signature est appelée **« Hash » du bloc**. Le Hash est le **condensé électronique de 256 bits** d'un bloc de données de la blockchain. C'est la robustesse de ce chaînage qui garantit la fiabilité de la blockchain.



Cette signature électronique de 256 bits est obtenue grâce à un algorithme de chiffrement dit asymétrique (SHA 256, Keccak-256). Cet algorithme possède les caractéristiques suivantes:

- il est déterministe, c'est à dire qu'une donnée produit toujours le même *hashé*,

- il est rapide,

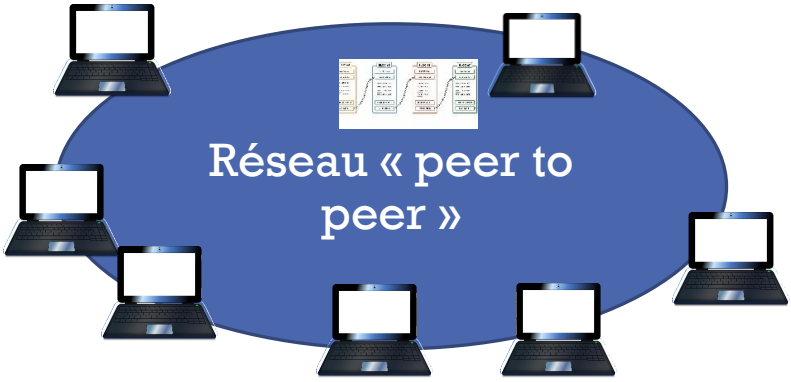
- il est irréversible car on ne peut pas retrouver la donnée originale quand on connaît sa signature sauf par un temps de calcul prohibitif avec les technologies actuelles,

- il est *anti-collision*. Deux données différentes, même très légèrement, produisent deux signatures complètement différentes.

INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C

**Chaque bloc contient la signature du bloc précédent et la sienne.
Une blockchain est donc une liste liée d'éléments, unique, extensible, et résistante à la contrefaçon des blocs par revérification des hash des blocs.**

Distribution de la chaine dans le réseau blockchain



Chacun dans le réseau de la blockchain (privé ou public) est représenté par une adresse.

La chaine est copiée ou mise à jour sur toutes les machines de ce réseau pair-à-pair (tout le monde « directement » connecté à tout le monde).

Cette distribution des données sur tout le réseau permet une résistance aux pannes, aux pertes, aux effacements.

Grâce à un mécanisme dit « de consensus », le réseau valide les nouvelles données et chaque machine possède une copie de la chaîne identique et certifiée par toutes les machines du réseau. La technologie blockchain développe intrinsèquement une **fonction d'autorité** et de « notaire » distribuée qui garantit l'intégrité et l'unicité de la chaîne **sans instance centrale de certification**.

Ajout d'un bloc, le « minage »

Pour ajouter un nouveau bloc à la chaîne, un défi est lancé aux « mineurs ». Ce défi est motivé par une récompense qui peut être soit directement une rétribution du réseau en cryptomonnaie, soit une récompense par la machine qui propose un nouveau bloc à valider au réseau.

L'objectif de ce défi est double. Il s'agit dans un premier temps de valider la fiabilité et la sincérité des données du bloc proposé au minage (notamment dans le cas de transactions financières), mais aussi de maintenir constante la vitesse de création de nouveaux blocs dans la chaîne qui est associée à la création de cryptomonnaies et à l'économie de la blockchain.

Selon le type de réseau blockchain, l'opération de minage utilise différentes modalités. Dans le réseau Bitcoin par exemple, le défi va consister à trouver la valeur qui rajoutée à un bloc de données permet de trouver un hash qui commence par une série de 0. Cette série de 0 est appelée le « Nonce ».

La validation d'un bloc nécessite un travail calculatoire important (environ 10 minutes sur bitcoin). Ce calcul produit la « preuve de travail » qui est rajoutée au bloc et génère une récompense pour le mineur gagnant.

```
Hello world ! 0 : 3f6fc92516327a1cc4d3dca5ab2b27aeedf2d459a77fa06fd3c6b19fb609106a
Hello world ! 1 : b5690c48c2d0a09481186aaa99e4e090901ff2ac4d572e6706dfd30eefc22a27
Hello world ! 2 : 5b6fd9c27fcb54ca23404d9428f081b7c9280ba6370e33a6a20b16f40ce76320
Hello world ! 3 : 9c5d769416aa0ca894abf22bd17bd30fbb6959291423ae1903a9f86a1fe7ce78
Hello world ! 4 : 4efc65df7933e4f5cc21947c61d5cc6bd11d644794bfa210603b0547c4b1cc3e
Hello world ! 5 : 441b15b67d791620cd50ea537144e3115422e33bdb1b1b9b110d3265f7a9199b
Hello world ! 6 : d368331386f0cf773ad53910fefcef4bdceeb526e408d3fbc9408d6f6e481ca4
Hello world ! 7 : 013cc9722f38d2eb6186b75e2e7cbe6e7818e0612a2774d4400416b17ae03b87
Hello world ! 8 : 3a92631799b478c3bcc554df8401b09900fbdb58cc0e58efe711cc475ee097b3
Hello world ! 9 : 66658881696164fcb04f32ec505bb5e515000a85baf691beb63fc9d3f4d0fee2
....
Hello world ! 88 : 80d009db72c6ad35241bb3dbac77cbe177c6a803fe67527c159dbfaf2cbf9f5c
Hello world ! 89 : a5b1e789f691f9793f8a84f8ebae3d8e28d49cbe0eeea2da621cd409e3bdee2b
Hello world ! 90 : 4eba5b2459caac3d9ff3b787aaa5cac481aaa4a0232fbbe02a8ee4d1101c2ca2
Hello world ! 91 : c811722c68b53614d58d37dcad9d540c2bce9f85b5ccae94424ff4716eea1765
Hello world ! 92 : e30c716fccda22f394a8e80a2670b97968b5416b8b39e2061a7b7d1a9f41e0a9
Hello world ! 93 : 965425c39d4e24c532721d7f7b77a00b31b0c0d0e316d46240c4e6bec9c09f65
Hello world ! 94 : 7090a0e5d88cff635e42ea33fcd6091a058e9cdd58ab8cd5c21c1c70421e35c6
Hello world ! 95 : b74f3b2cf1061895f880a99d1d0249a8cedf223d3ed061150548aa6212c88d43
Hello world ! 96 : [illegible]fa886965af084808d22116edde4383cbaa16fd1fbcf3db61421b9990b9
Hello world ! 9[illegible] : 000ba6[illegible]a46d1d317684925a0ef070e30193ff5fa6124aff76f513d96f49349d
```

La preuve de travail a été trouvée après 98 calculs.

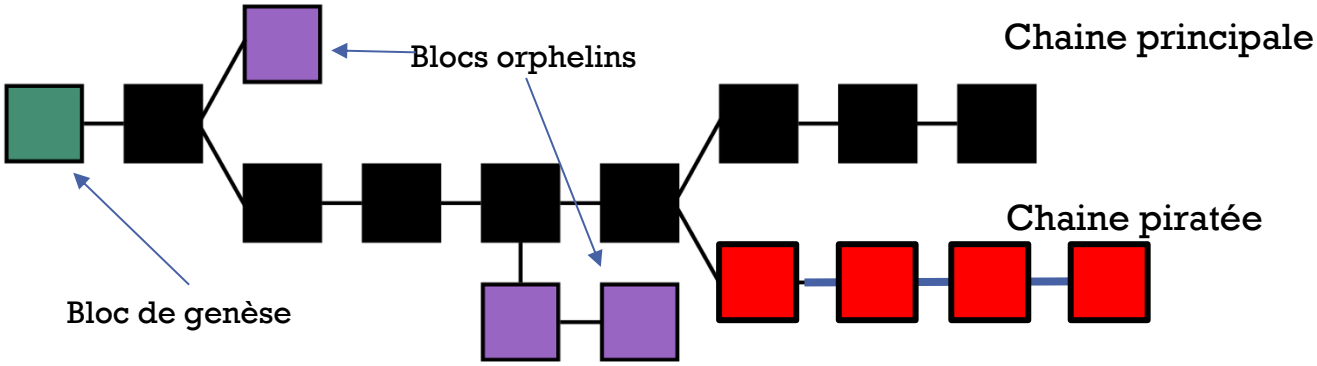
Le « nonce » : Actuellement à 32 zéros successifs sur bitcoin soit de 1 à 2^ 32 calculs nécessaires pour relever le défi et gagner de la monnaie virtuelle (la difficulté est augmentée pour rester autour de 10 minutes en moyenne)

Comme la production de nouvelles données dans la blockchain est concurrentielle, plusieurs blocs peuvent être envoyés simultanément au réseau pour validation. Le bloc avec la preuve de travail qui est produit en premier est rajouté à la chaîne. La nouvelle chaîne est validée par re-calcul du bloc plus la preuve de travail par le reste du réseau puis diffusée à tous les nœuds du bloc.

Il existe donc 2 types de nœuds sur le réseau blockchain les utilisateurs qui produisent de l'information et les mineurs qui produisent des preuves de travail. Les mineurs et les utilisateurs ont tous une copie locale de tout ou partie de la chaîne.

Plusieurs mineurs travaillent donc parallèlement à trouver la preuve de travail et à créer de nouveaux blocs pour essayer de gagner de la cryptomonnaie. Mais, dans le même temps, un autre mineur peut résoudre un autre bloc de données et le diffuser à une autre partie du réseau qui le valide aussi car le temps de propagation sur le réseau n'est pas nul.

Deux « branches » ou « fork » de la chaîne existent donc en même temps, ce qui est contraire à la règle d'unicité de la chaîne. Dans ce genre de conflit, c'est la branche de la chaîne la plus longue qui est retenue, l'autre finit par être supprimée par le réseau et produit des blocs orphelins.



Si la chaîne qui est créée est une tentative de piratage (en rouge sur la figure), il faut que le système qui détourne la chaîne soit plus puissant que tout le reste du réseau pour continuer à miner de nouveaux blocs dans la branche de la chaîne piratée plus vite que la chaine principale (au moins 51% de la puissance de calcul donc). On parle dans ce cas **« d'attaque des 51 % »** qui peut introduire dans la blockchain des données falsifiées et la faire valider par tout le réseau blockchain comme étant des données authentiques.

Le travail pour miner un nouveau bloc (bitcoin) est extrêmement coûteux en puissance, à tel point que les systèmes de minage aujourd'hui ne sont plus accessibles à des particuliers. Ce sont des fermes de minage qui sont utilisées et dont la consommation électrique ne fait qu'augmenter au fil du temps.

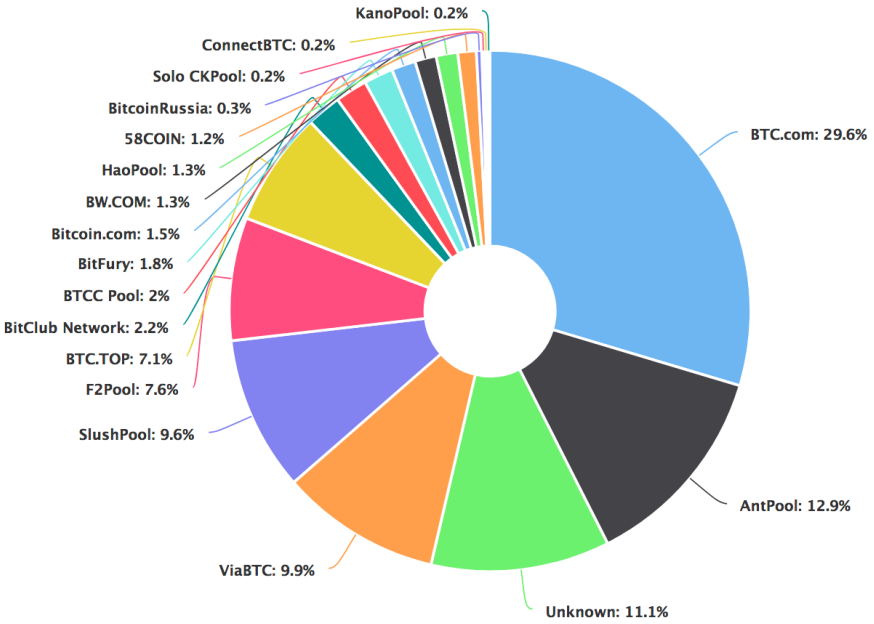
On considère que la consommation électrique de la technologie blockchain est aujourd'hui équivalente à la consommation électrique annuelle de l'Autriche.

Key Network Statistics

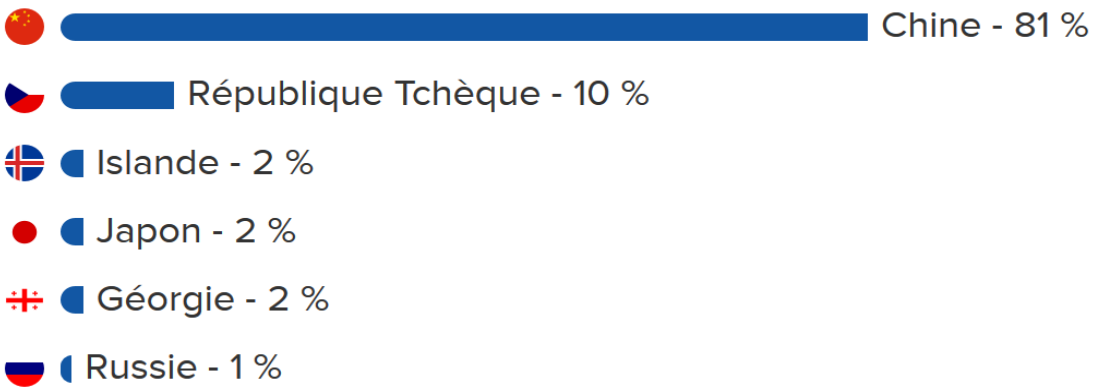
Description	Value
Bitcoin's current estimated annual electricity consumption* (TWh)	73.12
Bitcoin's current minimum annual electricity consumption** (TWh)	59.89
Annualized global mining revenues	$4,880,046,695
Annualized estimated global mining costs	$3,656,073,069
Current cost percentage	74.92%
Country closest to Bitcoin in terms of electricity consumption	Austria

Il y a plus préoccupant que la question de la consommation électrique. Alors que cette technologie promeut une utopie d'espace ouvert, concurrentiel et où chacun participe sur un pied d'égalité, la puissance de calcul sans cesse plus élevée et nécessaire à la résolution des défis de minage a provoqué une centralisation très forte des systèmes de minage, les « pools » de minage qui sont la propriété d'organismes privés. Comme le montrent les figures ci-dessous, un petit nombre de pool possède une puissance de calcul tout à fait considérable et sont massivement localisés en Chine.

Puissance de minage des plus gros « pools » de minage du monde :



Localisation géographique de ces « pools » :



Les différents types de blockchain et de « minage » associés

Il existe différentes méthodes de consensus selon le type de réseau blockchain envisagé. Ces différents modes de consensus permettent dans une certaine mesure de réduire la tendance à la centralisation des ressources du processus de minage.

- Blockchain publique (Bitcoin, Ethereum,…) : Dans ce type de blockchain, tout le monde peut participer au minage ou au rajout d'information, les données sont accessibles à tous en lecture, les algorithmes de minage sont ouverts et ne centralisent pas le processus.

- Blockchain de consortium (R3, EWF, B3i) : Dans ce type de blockchain, tout le monde peut participer à la création de nouveaux contenus, mais la validation de l'information est centralisée par un groupe accrédité. Elles sont principalement utilisées dans le domaine de la banque ou de l'assurance.

- Blockchain privée : dans ce dernier type, la production de contenus et la validation sont restreintes à un réseau de machines fermé.

Source : https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

Selon le type de blockchain mis en œuvre, différents mécanismes de consensus existent.

	Pubiic	Private/Federated
Access	• Open read/write	• Permissioned read and/or write
Speed	• Slower	• Faster
Security	• Proof of Work • Proof of Stake • Other consensus Mechanisms	• Pre-approved participants
Identity	• Anonymous • Pseudonymous	• Know identities
Asset	• Native Asset	• Any Asset

Public vs Private Blockchains
Source: Chris Skinner's Blog

On retrouve la preuve de travail dans les blockchains publiques (bitcoin, ethereum). Ce mécanisme a été présenté plus tôt. Il est robuste, mais lent et coûteux en énergie.

La méthode des généraux byzantins est plutôt dédiée aux réseaux de consortium ou aux réseaux privés (hyperledger, ripple, stellar). La validation des nouveaux blocs est confiée à des nœuds de confiance dédiés (généraux).

La preuve de participation est une nouvelle forme de consensus pour les blockchains publiques (Ethereum bientôt, peercoin). Le calcul de la preuve est simplifié et le vote est donné aux utilisateurs qui participent le plus au réseau (argent possédé, activité, degré de confiance).

La preuve de participation déléguée ressemble au mécanisme de preuve de participation, sauf que les participants à la blockchain forment par vote différents *pools* de miners. Le *pool* qui gagne le défi partage la récompense entre les mineurs qui ont participé au travail une fois la preuve apportée.

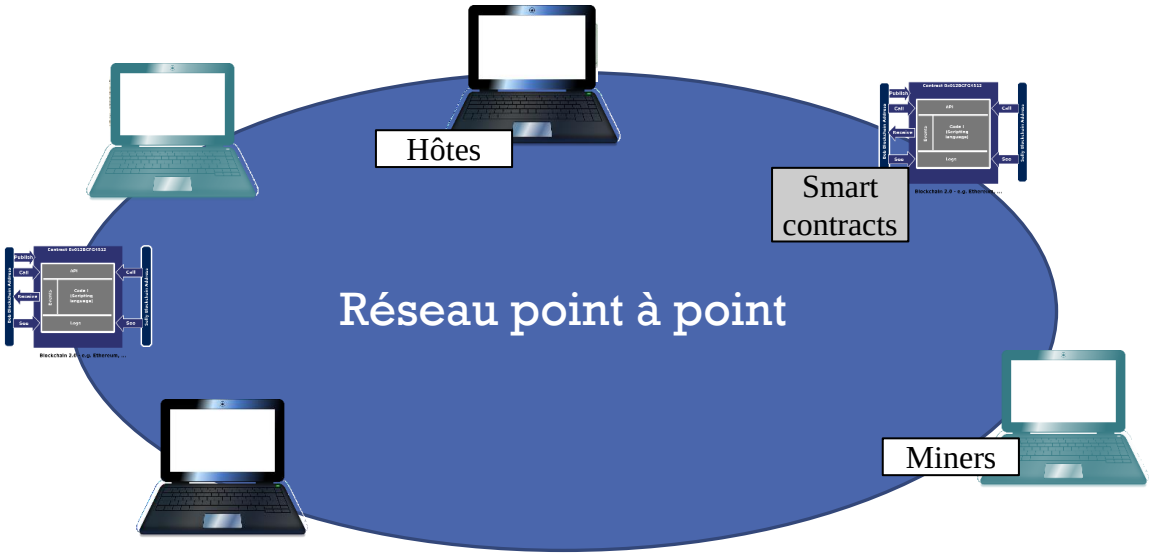
Les applications en blockchain : « smart » contracts et applications décentralisées D-Apps

Les blockchains ne sont plus seulement des systèmes de stockage d'information authentifiée et décentralisés. Depuis quelques années, Vitalik Buterin dans le réseau Ethereum a mis au point des applications qui fonctionnent sur des réseaux blockchain appelés des *« Smart » Contracts*, ce terme ayant été proposé et conceptualisé par Nick Szabo en 1994.

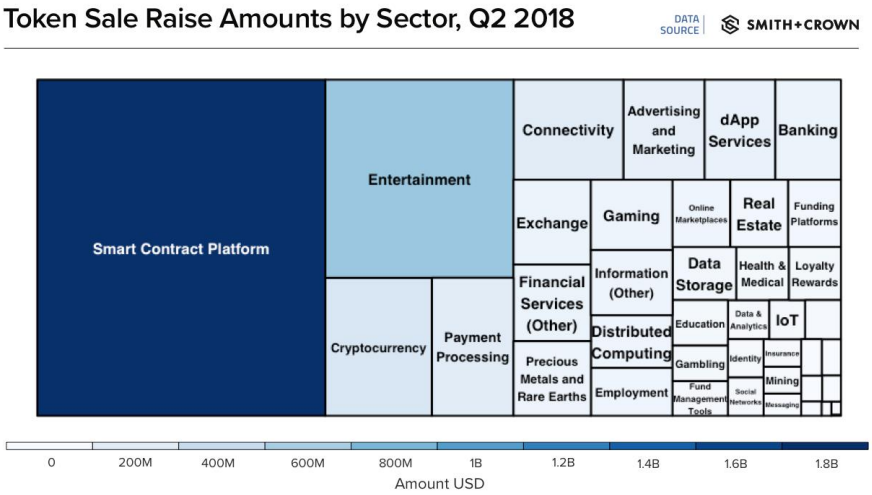
Certaines adresses dans le réseau sont en fait des programmes autonomes qui peuvent lire et écrire dans la blockchain. Ces programmes exécutent automatiquement des actions conditionnelles en fonction de règles inscrites dans la blockchain (*code is law*) et si les conditions nécessaires (*triggers*) sont réunies pour pouvoir les exécuter.

Exemple : assurance pour un retard de vol d'avion, airbnb…

Leurs transactions et leur fonctionnement sont soumis aux mêmes règles de transparence, de contrôle et d'irréversibilité que les autres hôtes du réseau.



Si les technologies d'applications distribuées et de *smart contracts* sont encore émergentes, il n'en reste pas moins qu'elles sont dans une dynamique très forte en termes d'investissements comme en témoigne cette distribution des levées de fonds par domaines d'application de la blockchain.



Les arguments des promoteurs de la blockchain

Au-delà des caractéristiques technologiques de la blockchain, des tensions importantes traversent et questionnent cette innovation d'un point de vue des usages et des potentialités.

Les promoteurs de la blockchain s'appuient sur le constat d'un certain nombre de dérives des technologies « traditionnelles » de l'internet :

- La sécurité est fragile avec la présence de nombreux virus, de pratique de *phishing* ou de piratage et de détournement d'informations ou de systèmes.

- D'autres pointent la question de la gouvernance du web, avec une centralisation autour de peu d'acteurs, les industries du GAFAM notamment, surtout privés et qui exploitent et font commerce des données des utilisateurs.

- La centralisation et la facturation par des tiers de médiation des transactions, en particulier dans le domaine de la banque ou des services à valeur ajoutée (amazon, airbnb, uber…).

- Les données personnelles sont mal protégées et sont exploitées aux dépends des utilisateurs.

Corollairement, ces mêmes promoteurs mettent l'accent sur les potentialités de la technologie Blockchain à diminuer ou annuler ces problématiques :

- La blockchain garantit l'intégrité des données ;

- La blockchain permet intrinsèquement la décentralisation de la donnée, de la décision, de la transaction, du calcul ;

- La monnaie est produite et utilisée sans contrôle centralisé et le paiement est réalisé très rapidement - le temps du minage de la donnée - et surtout sans intermédiaire. Les technologies de crypto-monnaies ont fait leurs preuves : Bitcoin, Ether, Wei… ;

- Contrairement aux transactions bancaires, il y a une rapidité effective et maîtrisée des transactions sur la blockchain et les échanges ont lieu sans tiers de médiation. Conséquemment, les frais de transaction sont très limités ;

- Les données personnelles sont sécurisées à l'intérieur de coffres forts numériques et les utilisateurs peuvent monétiser librement leurs données, leur puissance de calcul, des biens et des services divers.

Les arguments des détracteurs ou des sceptiques de la blockchain

Pour venir contraster le discours des promoteurs de la technologie blockchain, d'autres arguments sont évoqués pour contrebalancer ce discours pro-technologique.

Malgré une probabilité faible, les risques de piratage et d'attaque des 51% existent réellement. D'autre part, si les « grosses » blockchains (Bitcoin, Ethereum) sont difficiles à hacker, les *smart contracts* eux peuvent contenir des bugs. Ainsi en 2018, Bitcoin Gold, MonaCoin et Verge ont été attaquées pour un détournement de 20M$. La même année, 264 000 comptes utilisateurs ont été hackés sur Atlas Quantum (Données personnelles + Coins).

Un autre argument avancé concerne les fermes de minage dont la vocation même est de « cracker » des données chiffrées afin de produire la preuve de calcul. Les mots de passe, parfois faibles, choisis par les utilisateurs pour chiffrer leur données ou pour s'authentifier sont ainsi exposés à des attaques par une « force brute » de calcul.

Le réseau blockchain lui-même, du fait de la puissance de calcul qu'il nécessite pour fonctionner, peut être victime d'applications pourtant non frauduleuses. En 2018 le réseau Ethereum a souffert de problèmes de disponibilité suite au détournement de la puissance de calcul du réseau par une application de loterie qui a utilisé près de 30% de la puissance totale d'Ethereum.

Indépendamment des problématiques plutôt technologiques d'attaque ou de piratage, les fraudes et les détournements d'argents sont aussi nombreux. En 2017 par exemple, 80 % des ICO (Initial Coin Offering : levées de fond) autour de la technologie blockchain ont été frauduleuses pour un montant global de 1,3 Mdr$.

Il existe une autre problématique beaucoup plus constitutive de l'utopie associée à la blockchain qui stipule que la chaîne est unique et immuable, il s'agit d'une pratique appelée le « Hard fork » qui consiste en une « modification » dure du réseau *a posteriori*. Cela peut avoir lieu suite à une attaque ou un piratage de la blockchain, ou bien dans le cas où 2 branches concurrentes ont continué à exister simultanément sur la blockchain. Dans ce cas, et contrairement à l'immuabilité théorique, on peut modifier les règles (et parfois l'histoire) d'une blockchain moyennant un certain consensus des utilisateurs du réseau et donc en quelques sortes, soit revenir en arrière dans la production de la blockchain, soit supprimer une partie de l'information qu'elle contient, soit éventuellement créer une nouvelle blockchain « dissidente » de la principale.

Dernier argument avancé, malgré les nombreuses solutions technologiques proposées, il n'existe toujours pas de standard internationaux, ces solutions sont toujours « propriétaires ».

La blockchain en santé: Encore au stade des hypothèses

Dans le domaine de la santé, la technologie blockchain en est encore à ses débuts. Le même discours que celui des promoteurs de la blockchain est tenu, fiabilité, authenticité et unicité des données, efficacité et rapidité des transactions, articulation de différents acteurs, sécurisation des données et des transactions.

Des expérimentations fonctionnent déjà comme *passcare*, le passeport de santé qui permet de connecter dans un même système tout l'historique (https://www.usinenouvelle.com/editorial/la-blockchain-une-technologie-a-fort-potentiel-dans-la-sante.N673619)

Même si on est encore loin d'un système d'information hospitalier entièrement intégré, sécurisé et interopérable grâce à des systèmes de blockchain, de grands acteurs se positionnent autour de cette technologie à fort potentiel. La vision actuelle se résume assez bien par le schéma ci-dessous.

Dans cette vision, la technologie blockchain viendrait s'appuyer sur les différentes applications qui gèrent des silos informationnels en rajoutant la sécurisation des transactions et du partage d'information. Au-dessus de cette couche, les applications réparties et la monétisation inhérente à la technologie permettraient la création d'un « écosystème » technologique et industriel innovant qui produirait une richesse d'informations qualifiées pour nourrir des systèmes d'aide à la décision et au pilotage basés sur des intelligences artificielles et des technologies de machine-learning.

Synthèse

La blockchain est une base de données distribuée entre tous les utilisateurs du réseau dans laquelle l'information est non répudiable. Les données et les transactions qu'elle contient sont historisées, archivées et certifiées par l'ensemble des machines du réseau.

De mon point de vue, trois enjeux centraux sont adressés par cette technologie :

- L'intégrité de l'information qui est réputée totale, mais qui peut être remise en question par les usages et les actes de piratage ;
- L'économie du minage qui induit une mise en concurrence de la production d'information et de sa validation ;
- Les intermédiaires des plateformes technologiques qui produisent et promeuvent ces technologies et qui ont un pouvoir considérable sur la nature même de la blockchain et de son fonctionnement ;

Si la technologie bitcoin est mature, la blockchain et les solutions techniques qui sont développées grâce à elle, doivent encore faire leurs preuves. Pourtant la dynamique économique importante autour de cette technologie, les nombreux domaines qui sont concernés et la carrure des acteurs qui s'y intéressent et investissent des sommes importantes, laissent présager d'une montée en puissance rapide des implémentations techniques et de nouveaux usages, y compris bien sûr dans le domaine de la santé.

Conclusion

La blockchain rejoue le débat de l'innovation technologique avec ses promoteurs et ses opposants, en le déplaçant vers une formalisation potentiellement contraignante de plusieurs aspects : de l'histoire inscrite dans la blockchain, du sens de l'information, de la valeur, de la décision, des règles. D'autre part, la blockchain produit une forme de moralisation implicite car elle inscrit une vision unique et autoritaire de l'état d'un monde qui est vu comme étant un processus linéarisé d'évènements, d'informations et de transactions, et dont les décisions sont uniquement basées sur des règles « objectives ».

Parallèlement, c'est la première information qui est « minée » qui fabrique un nouveau pan de l'histoire collective, la blockchain installe ou renouvelle la compétition pour la production historique qui fait ensuite autorité.

Ces technologies quoique constitutivement ouvertes, explicites et mettant tout le monde sur un même pied d'égalité restent pourtant difficiles à saisir, à cerner ; génèrent du fait de l'économie et de la compétition liées au minage des accumulations de puissance de calcul et donc de richesses ; et semblent ne pas résister aux stratégies de détournement, de piratage et de réécriture malgré la promesse d'une historisation et d'un horodatage uniques et certifiés.

A ce stade, des parallèles sont possibles entre le développement de la blockchain et l'histoire de l'internet et du web, lequel s'est élancé sur une utopie ouverte, égalitaire, collaborative ; lequel a subi une importante bulle spéculative en 2000 ; pour être finalement aujourd'hui un espace plus ou moins privatisé par des géants qui centralisent de nombreuses ressources, et qui se sont installés en médiateurs d'un nombre important d'éléments sociaux, historiques et économiques.

Un travail important à la fois sur le plan des Sciences Humaines et Sociales, du droit, de la santé et de l'ingénierie technologique est à faire pour mesurer la portée et les conséquences de ces nouvelles technologies et en matière d'inégalités sociales de santé tout particulièrement.

Webographie

https://www.hbrfrance.fr/chroniques-experts/2018/05/20131-breve-histoire-de-blockchain/

https://dzone.com/articles/an-introduction-to-ethereum-and-smart-contracts-bi

https://motherboard.vice.com/en_us/article/j5nzx4/what-was-the-first-blockchain

https://www.lemonde.fr/big-browser/article/2018/09/01/la-premiere-blockchain-de-l-histoire-date-de-1995-et-elle-est-imprimee-sur-papier_5349082_4832693.html

https://www.anf.es/pdf/Haber_Stornetta.pdf

https://link.springer.com/content/pdf/10.1007%2FBF00196791.pdf

https://www.forbes.fr/technologie/lintelligence-artificielle-sassocie-a-la-blockchain-en-2018/?cn-reloaded=1

http://www.bortzmeyer.org/a-quoi-sert-blockchain.html

http://www.mbadmb.com/2016/12/27/blockchain-isu2/

https://blockgeeks.com/guides/what-is-hashing/

https://bitcoin.fr/nicehash-attaquer-une-blockchain/

https://digiconomist.net/bitcoin-energy-consumption

https://www.buybitcoinworldwide.com/fr/minage/pools/

https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe

https://www.niceideas.ch/roller2/badtrash/entry/blockchain-2-0-from-bitcoin

https://journalducoin.com/altcoins/smith-crown-bear-market-crypto/

https://medium.com/@cyrilpaglino/blockchain-protocoles-d%C3%A9centralis%C3%A9s-et-crypto-actifs-ou-la-plus-grande-r%C3%A9volution-technologique-72cc9599a32d

https://www.cnetfrance.fr/news/attaque-des-51-le-bitcoin-et-les-cryptomonnaies-sont-ils-vraiment-securises-39869293.htm

https://journalducoin.com/exchanges/piratage-donnees-utilisateurs-atlas-quantum/

https://www.nextinpact.com/news/100336-the-dao-pirate-derobe-50-millions-dollars-contre-attaque-se-prepare.htm

https://journalducoin.com/blockchain/le-nouveau-telegram-passport-serait-vulnerable-aux-attaques-par-force-brute/

https://journalducoin.com/blockchain/augur-devient-officiellement-autonome-kill-switch-active/

https://www.bfmtv.com/tech/sur-le-web-une-plateforme-permet-de-parier-sur-l-assassinat-de-trump-1495380.html#xtor=AL-68

https://journalducoin.com/ico/etude-cabinet-statis-80-pourcent-ico-2017-scams/

https://www.forbes.com/sites/robertpearl/2018/04/10/blockchain-bitcoin-ehr/#5ad0ac9979e7

https://hitinfrastructure.com/news/healthcare-blockchain-standards-support-collaborative-development

http://blockchainpartner.fr/wp-content/uploads/2017/06/Sant%C3%A9-Industrie-Pharmaceutique-Blockchain.pdf