La Blockchain, au-delà du Bitcoin

Il existe déjà sur le Bitcoin et la nombreuse famille des monnaies virtuelles une abondante littérature qui évoque les espoirs et les fantasmes que génèrent les crypto-monnaies. Mais pour qui n'est encore ni utilisateur dans ses paiements ni prosélyte convaincu, il n'est pas si facile de comprendre le principe de fonctionnement qui sous-tend le succès grandissant de cet argent dématérialisé sans intermédiaire.

Pour savoir ce qui se passe en coulisses, il est nécessaire d'appréhender correctement ce qu'est la **blockchain***. C'est bien délicat, et rares sont les explications limpides qui nous permettent de saisir l'essentiel. L'article « Chaîne de blocs » de Wikipédia utilise très vite des prérequis dont ne disposent probablement pas les Dupuis-Morizeau : « système cryptographique », « base de données distribuée », « nœud de stockage », etc.*

Heureusement, il arrive que nous rencontrions un article qui présente des qualités de clarté telles que nous nous faisons un devoir de le partager. Qui plus est, nous y découvrons que le bitcoin n'est qu'un exemple aujourd'hui notoire des très nombreuses possibilités d'application de la blockchain dans des domaines très variés, ce qui pourrait à moyen terme changer beaucoup de choses dans notre vie quotidienne…

L'auteur, Jean-Paul Delahaye est un universitaire, mathématicien et informaticien, chercheur à l'Université de Lille 1. Nous le remercions d'avoir accepté que nous reprenions ici, mis à jour pour les données numériques, son texte déjà publié en 2014 sur le blog de Scilogs.

La puissance de la blockchain

Imaginez qu'au centre de la place de la Concorde à Paris, à côté de l'Obélisque on installe un très grand cahier, que librement et gratuitement, tout le monde puisse lire, sur lequel tout le monde puisse écrire, mais qui soit impossible à effacer et indestructible. Cela serait-il utile ?

Il semble que oui.

– On pourrait y consigner des engagements : *« je promets que je donnerai ma maison à celui qui démontrera la conjecture de Riemann : signé Jacques Dupont, 11 rue Martin à Paris ».*

– On pourrait y déposer la description de ses découvertes rendant impossible qu'on en soit dépossédé : *« Voici la démonstration en une page que j'ai trouvée du Grand théorème de Fermat …»*.

– On pourrait y laisser des reconnaissances de dettes qui seraient considérées valides tant que celui à qui l'on doit l'argent n'a pas été remboursé et n'est pas venu l'indiquer sur le cahier.

– On pourrait y donner son adresse qui resterait valide jusqu'à ce qu'une autre adresse associée au même nom soit ajoutée, annulant la précédente.

– On pourrait y déposer des messages adressés à des personnes qu'on a perdues de vue en espérant qu'elles viennent les lire et reprennent contact.

– On pourrait y consigner des faits qu'on voudrait rendre publics définitivement, pour que l'histoire les connaisse, pour aider une personne dont on souhaite défendre la réputation, pour se venger, etc.

Pour que cela soit commode et pour empêcher les tricheurs d'écrire en se faisant passer pour vous, il faudrait qu'il soit possible de signer ce qu'on écrit. Il serait utile aussi que l'instant précis où est écrit un message soit précisé avec chaque texte déposé sur le grand cahier (horodatage).

Imaginons que tout cela soit possible et qu'un tel cahier soit mis en place, auquel seraient ajoutées autant de pages nouvelles que nécessaire au fur et à mesure des besoins. Testaments, contrats, certificats de propriétés, récits divers, messages adressés à une personne particulière ou à tous, attestations de priorité pour une découverte, etc., tout cela deviendrait facile sans avoir à payer un notaire, ou un huissier. Si un tel cahier public était vraiment permanent, infalsifiable, indestructible, et qu'on puisse y écrire librement et gratuitement tout ce qu'on veut, une multitude d'usages en seraient imaginés bien au-delà de ce que je viens de mentionner.

Un tel objet serait plus qu'un cahier de doléances ou un livre d'or, qui ne sont pas indestructibles. Ce serait plus qu'un tableau d'affichage offert à tous sur les murs d'une entreprise, d'une école ou d'une ville, eux aussi temporaires. Ce serait plus que des enveloppes déposées chez un huissier, coûteuses et dont la lecture n'est pas autorisée à tous. Ce serait plus qu'un registre de brevets, robuste mais sur lesquels il est coûteux et difficile d'écrire. Ce serait plus que les pages d'un quotidien qui sont réellement indestructibles car multipliées en milliers d'exemplaires, mais sur lesquelles peu de gens ont la possibilité d'écrire et dont le contenu est très contraint.

Place de la Concorde ?

Bien sûr, ce cahier localisé en un point géographique unique ne serait pas très commode pour ceux qui habitent loin de Paris. Bien sûr, ceux qui y rechercheraient des informations en tournant les pages se gêneraient les uns les autres, et

gêneraient ceux venus y inscrire de nouveaux messages. Bien sûr encore, faire des recherches pour savoir ce qui est écrit dans le cahier (telle dette a-t-elle été soldée ? Telle adresse est-elle la dernière ? etc.) deviendrait vite impossible en pratique quand le cahier serait devenu trop gros et que ses utilisateurs se seraient multipliés.

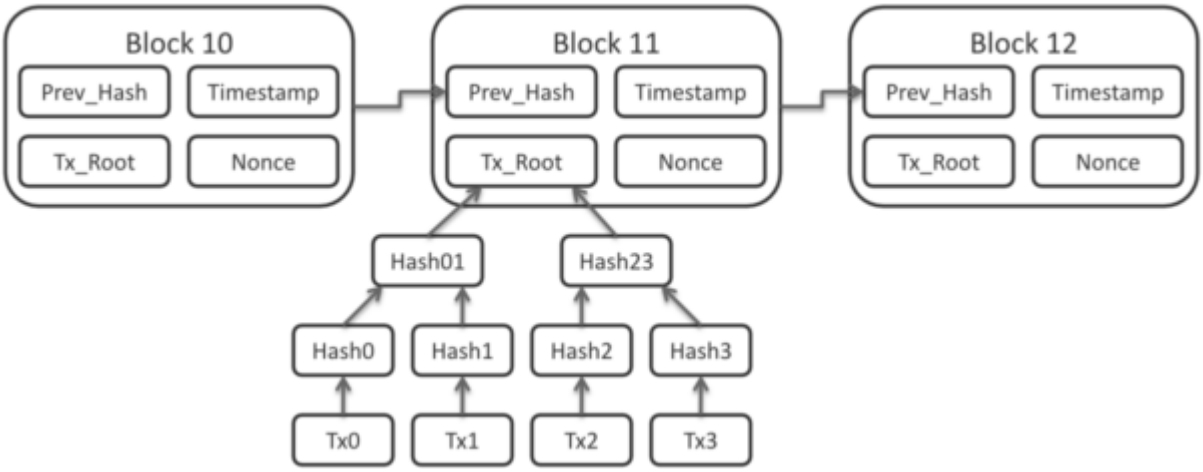
Ces trois inconvénients majeurs :
a) localisation unique rendant l'accès malcommode et coûteux ;
b) impossibilité de travailler en nombre au même instant pour y lire ou y écrire ;
c) difficulté de manipuler un grand cahier…
… peuvent être contournés. L'informatique moderne avec la puissance de ses machines (y compris les smartphones) et ses réseaux de communication est en mesure de les surmonter.

D'ailleurs cette idée d'un grand *cahier informatique, partagé infalsifiable et indestructible du fait même de sa conception* est au cœur d'une révolution qui débute. Nous la baptiserons la «révolution de la blockchain » (nous allons expliquer pourquoi) ou plus explicitement et en français : « la révolution de la programmation par un fichier partagé et infalsifiable ».

L'idée de Nakamoto

Le nom proposé vient de la *blockchain* du *bitcoin*, la monnaie cryptographique créée en janvier 2009, et qui a depuis connu un développement considérable et un succès réel très concrètement mesurable : la valeur d'échange des devises émises en *bitcoins* dépasse aujourd'hui 5 milliards d'euros. Au cœur de cette monnaie, il y a effectivement un fichier informatique infalsifiable et ouvert. C'est celui de toutes les transactions, baptisé par Satoshi Nakamoto son inventeur : la *blockchain*. C'est un fichier partagé, tout le monde peut le lire et chacun y écrit les transactions de *bitcoins* qui le concerne, ce qui les valide. La *blockchain* existe grâce à un réseau pair à pair, c'est-à-dire géré sans autorité centrale

par les utilisateurs eux-mêmes. Certains de ces utilisateurs détiennent des copies de la *blockchain*, partout dans le monde. Ces centaines de copies sont sans cesse mises à jour simultanément, ce qui rend la *blockchain* totalement indestructible, à moins d'une catastrophe qui toucherait en même temps toute la terre. Ce fichier a été rendu infalsifiable par l'utilisation de procédés cryptographiques qui depuis sa création en 2009 se sont révélés résister à toutes les attaques : personne jamais n'a pu effacer ou modifier le moindre message de transaction auparavant inscrit dans la *blockchain* du *bitcoin*.



C'est possible, cela existe !

Le rêve du grand cahier de la place de la Concorde est donc devenu possible, et en réalité ce que l'informatique moderne, les réseaux et la cryptographie ont su créer dans le monde numérique est bien supérieur à tout ce qu'on aurait pu tenter de faire avec du papier, du métal ou tout dispositif composé d'objets physiques. En particulier :

a) l'accès à la *blockchain*, grâce aux réseaux, se fait instantanément de n'importe où dans le monde, pourvu qu'on dispose d'un ordinateur ou simplement d'un smartphone ;

b) des milliers d'utilisateurs peuvent y lire simultanément sans se gêner ;

c) chacun peut gratuitement et sans limitation ajouter de

nouveaux messages de transactions selon un procédé qui assure la cohérence et la robustesse du fichier *blockchain*.

La taille de la *blockchain* du *bitcoin* s'accroît progressivement, mais reste manipulable par les formidables machines dont nous disposons tous aujourd'hui. Elle comporte aujourd'hui 54 giga-octets (5,4 10^10 caractères), ce qui est l'équivalent d'environ 54 000 ouvrages de 200 pages. Cela semble énorme, mais nos ordinateurs sont maintenant assez puissants pour cela.

L'exploration par son ordinateur de ce qui est inscrit donne librement accès à tout le contenu de cette *blockchain* quasi-instantanément de n'importe quel endroit du monde. C'est d'ailleurs, dans le cas du *bitcoin*, ce qui permet de calculer le solde des comptes. Les systèmes de signatures cryptographiques garantissent que les messages de transaction que vous inscrivez sur la *blockchain* concernant vos comptes ont été écrits par vous. L'ordre des inscriptions fournit aussi une datation (horodatage) des transactions et donc les ordonne. Tout cela est fait, sans qu'aucune autorité centrale ne s'en occupe, puisque ce sont certains des utilisateurs (appelé « mineurs » dans le cas du *bitcoin*) qui en opèrent la surveillance, et qui se contrôlent mutuellement, assurant l'honnêteté des sauvegardes et leur cohérence.

L'exemple d'une monnaie est la plus spectaculaire et la plus visible aujourd'hui des merveilles que réalise une *blockchain*. Qu'on ait pu ainsi créer une monnaie, grâce à un fichier partagé, semble incroyable. Cela d'autant plus qu'il s'agit d'une monnaie d'un nouveau type : elle ne repose sur aucune autorité émettrice, autorise des transactions quasi-instantanées gratuitement d'un point à l'autre du globe.

De nombreuses variantes

Au-delà du miracle que constitue cette monnaie (nous ne reviendrons pas sur le détail de son fonctionnement), c'est l'ensemble de tout ce que rend possible ce type d'objet qu'est une *blockchain* que nous voulons évoquer, car il semble bien qu'un nouveau monde économique, social, législatif, politique et monétaire en résulte. Aujourd'hui, nous n'en avons pas pris la mesure.

Le *bitcoin* utilise une *blockchain* qui lui est propre et ne sert a priori qu'à inscrire des transactions, mais l'idée de cette *blockchain* peut se décliner d'une multitude de façons donnant naissance à autant d'applications nouvelles. Nous avons sans doute pour l'instant entrevu que quelques aspects de ce que de tels dispositifs autorisent. Il s'agit rien moins que de l'apparition d'un nouveau type d'objets réels, aussi durs que le métal, contenant des informations d'une complexité sans limites. Nos ordinateurs aux extraordinaires capacités de calcul y accèdent instantanément grâce aux réseaux, explorant rapidement ce qui s'y trouve, y déposant de nouveaux messages éventuellement cryptés, et les extrayant aussi rapidement. Ces nouveaux objets du fait de leur nature numérique et de leurs propriétés de robustesse et d'ubiquité – ils existent partout dans le monde à la fois – ont des propriétés qu'aucun objet du monde n'a jamais possédées.

Il existe aujourd'hui des centaines de variantes du modèle *bitcoin*. Ce sont essentiellement d'autres monnaies – on parle de crypto-monnaies – qui chacune s'appuie sur une *blockchain*

particulière. Cependant depuis qu'on a compris que l'idée de Nakamoto était beaucoup plus générale, d'autres systèmes avec *blockchain* sont apparus ou sont en cours de développement.

Une révolution en marche

Certaines des idées évoquées au départ peuvent se mettre en place soit grâce à une nouvelle *blockchain*, soit en essayant d'utiliser la *blockchain* du *bitcoin* qu'on détournera de sa fonction première pour lui faire réaliser des opérations non prévues par Nakamoto. Dom Steil un entrepreneur s'occupant du *bitcoin* et auteur de nombreux articles sur les nouvelles technologies a exprimé assez clairement l'idée de cette révolution :

> *« La blockchain est intrinsèquement puissante du fait que c'est la colonne vertébrale d'un nouveau type de mécanisme de transfert et de stockage distribué et open source. Elle est le tiers nécessaire pour le fonctionnement de nombreux systèmes à base de confiance. Elle est la feuille universelle d'équilibrage utilisée pour savoir et vérifier qui détient divers droits numériques. De même qu'Internet a été la base de bien d'autres applications que le courrier électronique, la blockchain sera la base de bien d'autres applications qu'un réseau de paiement. Nous en sommes aux premiers instants d'un nouvel âge pour tout ce qui est possible au travers d'un réseau décentralisé de communications et de calculs. ». Voir* ***ici****.*

Jon Evans un ingénieur informaticien et journaliste spécialisé dans les nouvelles technologies partage cet enthousiasme :

> *« La technologie blockchain au cœur du bitcoin est une avancée technique majeure qui, à terme, pourrait révolutionner l'Internet et l'industrie de la finance comme nous les connaissons ; les premiers pas de cette révolution en attente ont maintenant été franchis. »*

« La « blockchain » –le moteur qui sert de base au bitcoin– est un système distribué de consensus qui autorise des transactions, et d'autres opérations à être exécutées de manière sécurisée et contrôlée sans qu'il y ait une autorité centrale de supervision, cela simplement (en simplifiant grossièrement) parce que les transactions et toutes les opérations sont validées par le réseau entier. Les opérations effectuées ne sont pas nécessairement financières, et les données ne sont pas nécessairement de l'argent. Le moteur qui donne sa puissance au bitcoin est susceptible d'un large éventail d'autres applications. » (ici et ici)

La machine qui inspire confiance

comment la technologie derrière le Bitcoin pourrait changer le monde

Namecoin, Twister, Ethereum

Parmi les *blockchain* autres que celle du *bitcoin* et ayant pour objets des applications non liées à la monnaie, il faut citer le Namecoin un système décentralisé d'enregistrement de noms : on écrit sur la *blockchain* du Namecoin des paires (nom, message). Un des buts de Namecoin est la mise en place d'un système d'adresses pour les ordinateurs connectés au réseau internet qui pourrait se substituer au système actuel DNS (Domaine name system) en partie aux mains d'organisations américaines. Les créateurs de cette *blockchain* affichent les objectifs suivants : protéger la libre parole en ligne en rendant le web plus résistant à la censure ; créer un nom de domaine «.bit» dont le contrôle serait totalement décentralisé ; mémoriser des informations d'identité comme des adresses email, des clefs cryptographiques publiques. Ils évoquent aussi la possibilité avec cette *blockchain* d'organiser des votes ou des services notariés. Malheureusement cette *blockchain* est peu commode car les dépôts d'informations y

sont payants (en *namecoin*), et même si les coûts sont très faibles, ils compliquent beaucoup son utilisation. Voir ici.

Plus récemment a été créé Twister, un système concurrent de Twitter (le système de micro-blogging bien connu) mais totalement décentralisé et donc libre de toute censure ou contrôle. La *blockchain* de Twister ne sert dans ce cas pas à stocker toute l'information de la plateforme de micro-bloging (qui est distribuée sur un réseau pair à pair évitant que les nœuds du réseau aient à gérer de trop gros volumes de données) mais seulement les informations d'enregistrement et d'authentification. Voir ici.

Un projet plus ambitieux car se voulant le support possible d'applications complexes basé sur une notion de contrat (*smartcontract*) est en cours de développement : il se nomme *Ethereum*. La *blockchain* associée à *Ethereum* émettra une monnaie (l'*éther*) sur le modèle de *bitcoin*, mais ce ne sera qu'une des fonctions de cette *blockchain. Voir ici.*

Une autre avancée toute récente a été proposée par Adam Back, inventeur déjà d'une monnaie électronique précurseur du *bitcoin*. Back a constaté que le *bitcoin* ne peut évoluer que très lentement car les décisions pour ces évolutions se font selon un processus qui exige un accord difficile à obtenir de la part de ceux qui travaillent à le surveiller et qui ne sont pas organisés en structure hiérarchique –c'est un problème avec les applications totalement décentralisées dont le contrôle n'est aux mains de personne. Il a aussi noté que beaucoup d'idées innovantes proposées par des *blockchain* nouvelles n'ont qu'un succès limité. En valeur, le *bitcoin* reste très dominant parmi les monnaies cryptographiques. Avec une équipe de chercheurs, il a mis au point une méthode liant les *blockchains* les unes aux autres. Ce système de « *sidechain* » permettra de faire passer des unités monétaires d'une chaîne A vers une autre B. Elles disparaîtront de la chaîne A pour réapparaître sur la chaîne B et pourront éventuellement revenir dans A. Chaque *blockchain* est un petit

univers où il est utile de disposer d'une monnaie (par exemple sur Namecoin, il y a une monnaie). Cependant faire accepter une nouvelle monnaie et stabiliser son cours est difficile et incertain. De plus chaque *blockchain* est une expérience comportant des risques qui sont d'autant plus grands qu'elle est récente et innovante. Le système des *sidechain* une fois mis en place (ce n'est pas si simple et aujourd'hui aucune *sidechain* ne fonctionne) permettra de tester rapidement de nouvelles idées. Chacune pourra « importer » la monnaie d'une autre *blockchain*, sans doute la monnaie *bitcoin* qui est la mieux installée et celle pour laquelle la confiance est la plus forte. Le système est conçu pour que la chaîne qui « prête » de l'argent à une autre ne risque pas plus que ce qu'elle prête et donc ne prenne qu'un risque limité.

> ***« Une forme d'anarchie à base numérique va poursuivre son développement »***

On le voit, la complexité (de nos puces, de nos machines, de nos applications, de nos réseaux informatiques) a créé un univers où les nouveaux objets indestructibles que sont les *blockchains* changent les règles du jeu : moins de centralisation, moins d'autorité, plus de partages sont possibles. Une forme d'anarchie à base numérique va poursuivre son développement. Le monde qui en sortira est difficile à imaginer, mais il se forme et même si on peut le craindre autant que certains l'appellent de leurs vœux, il sera là bientôt.

Liens mentionnés par l'auteur de l'article

- The Power of The Blockchain: Future Developments and Applications
- The coming digital anarchy
- The power of the blockchain

- How Bitcoin’s Block Chain Could Stop History Being Rewritten
- Blockchain : La dénationalisation de la monnaie
- Alternative chain
- The Power of The Blockchain: Future Developments and Applications
- Decentralized Money: Bitcoin 1.0, 2.0, and 3.0
- Bitcoin’s blockchain could revolutionise more than just how we do business
- Bitcoin 2.0: Sidechains And Ethereum And Zerocash, Oh My!
- Could the Bitcoin network be used as an ultrasecure notary service?
- Twister (software)
- Twister-a P2P microblogging platform
- Ethereum
- Enabling Blockchain Innovations with Pegged Sidechains

D’autres liens intéressants sur la question et autour

- Site en français dédié à la blockchain
- Thierry Crouzet appelle de ses vœux une « bookchain », une blockchain de publication textuelle
- Blockchain, vous avez dit Blockchain ?, un article récent de l’Usine Digitale qui en examine sommairement les enjeux juridiques pour l’entreprise.
- Disruption : la blockchain sur le radar des banques, un article de ZDNet.fr qui évoque l’intérêt des entreprises bancaires pour « le potentiel de cette architecture décentralisée de confiance »
- The trust machine, un article (en anglais) du très sérieux magazine The Economist, qui consacre à la blockchain la couverture de son numéro d’octobre 2015.

Crédits Images

- « Bitcoin accepted here », Francis Storr (CC BY-SA 2.0)
- Schéma des blocs par Matthäus Wander (CC BY-SA 3.0) via

Wikimedia Commons

- *The trust machine*, image de couverture du magazine The Economist du 30 octobre 2015,