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.

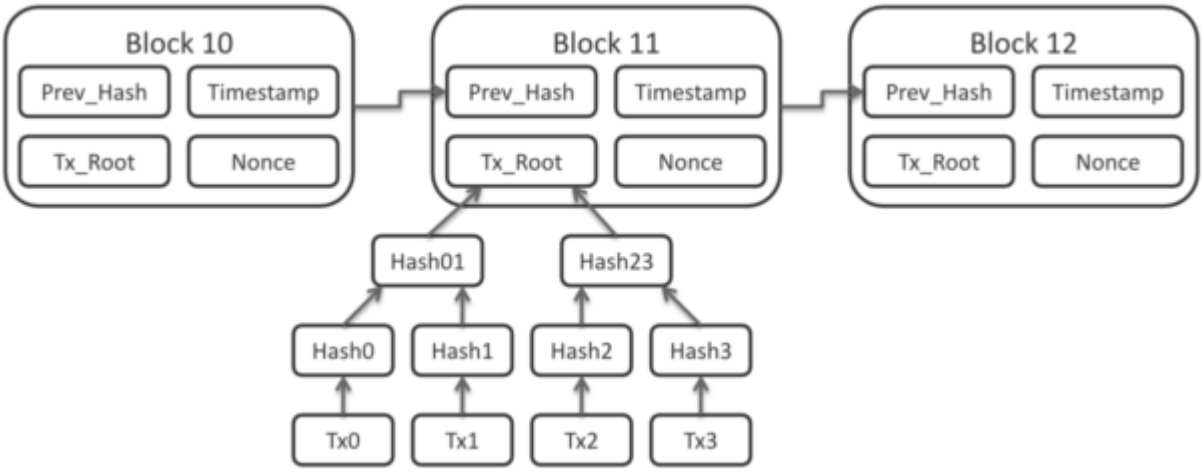
Ces trois inconvénients majeurs :
a) localisation unique rendant l'accès malcommode et coûteux ;
b) impossibilité de travailler en nombre au même instant pour y lire ou y écrire ;
c) difficulté de manipuler un grand cahier…
… peuvent être contournés. L'informatique moderne avec la puissance de ses machines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

---

Pourquoi les banques entrent en guerre contre la monnaie Bitcoin

La Banque de France a publié ce jeudi 5 décembre une note sur le bitcoin « monnaie non régulée qui n'offre aucune garantie ». Cela a été repris dans tous nos grand médias, d'autant que la banque centrale chinoise s'y est mise à son tour, interdisant officiellement à ses institutions d'utiliser cette *drôle* de monnaie (conséquence directe : chute momentanée de son cours en yuans de près de 35%).

Or, quand on lit les articles de la presse nationale, on est frappé par le long exposé anxiogène des risques que représente bitcoin, reprenant ainsi les arguments dans la Banque de France, trop rarement (litote) contrebalancé par ses avantages.

Or ils sont nombreux, à commencer par, tiens, tiens, pouvoir (enfin) se passer des banques… CQFD

Maintenant que le bitcoin a grandi et que de plus en plus d'organismes l'acceptent comme mode de paiement, la guerre est ouvertement déclarée. Parce que se passer des banques, c'est tout simplement *révolutionnaire* par les temps qui courent où l'économique a pris le pas sur la politique…

PS tout à fait personnel : Les banques (avec la complicité des

gouvernements) ont quand même beau jeu de nous faire la leçon après la crise des subprimes. 2 infos récentes du mois dernier qui intéressent beaucoup moins les médias que les pseudo-problèmes sociétaux (et surtout pas sociaux) du mariage, du racisme ou de la prostitution : une rallonge de 1,5 milliard d'euros aux collectivités pour qu'elles renoncent à tout contentieux contre les banques et Euribor, Libor : la manipulation des taux coûtera 1,7 milliard d'euros d'amende à six banques européennes (mais minimisées selon leur ordre d'arrivée). On nous prend vraiment pour des cons !

Pourquoi les banques déclarent la guerre au Bitcoin

Why Banks are Declaring War on Bitcoin

Mark Maunder – 5 décembre 2013 – Blog personnel
(Traduction : Goofy, crendipt, Shanx, Jérémie, Jérémie, Tr4sK, Asta, Omegax, Sky + anonymes)

Et si nous vivions dans un monde où toutes les transactions se faisaient de personne à personne et ne coûtaient quasiment rien ?

Et si nous vivions dans un monde où la valeur de l'argent épargné augmentait petit à petit, non pas grâce aux intérêts, mais simplement parce que, avec le temps qui passe, vous pouvez acheter plus de trucs avec la même somme ?

Et si s'endetter devenait une très mauvaise idée parce que, si vous détenez 10 unités de monnaie aujourd'hui, et que la valeur de celle-ci augmente lentement, alors vous devrez graduellement de plus en plus d'argent ? Ainsi, personne ne voudrait s'endetter.

Et si s'endetter devenait une très mauvaise idée parce qu'épargner devient une très bonne idée, parce que quelle que soit la somme que vous possédez, elle vaut de plus en plus à mesure que le temps passe ? Elle augmente non pas parce qu'elle est exploitée par une banque, mais parce que plus de gens veulent la même somme.

C'est le monde vers lequel nous nous dirigeons, car c'est ainsi que Bitcoin fonctionne. Un univers en parallèle des banques qui laisse celles-ci en position de faiblesse.

Bitcoin n'est pas une banque centrale où l'afflux d'argent peut-être régulé par une charte, charte pouvant être contrôlée par les lobbys et manipulée par les grands industriels. L'apport de la monnaie Bitcoin est gouverné par un algorithme, et cet algorithme assure que le Bitcoin sera toujours sujet à la déflation. Cela signifie que le rythme auquel la monnaie Bitcoin est créée ralentira progressivement pour complètement s'arrêter tôt ou tard. Par conséquent, aussi longtemps que l'activité économique (qui dicte la demande monétaire) augmente doucement, cette devise vaudra progressivement un peu plus.

Traditionnellement, la déflation, pendant laquelle la monnaie vaut plus et les prix des denrées et services chutent, est le pire cauchemar des économistes. Ceci parce que lorsque vous êtes en déflation, les salaires baissent. La plupart des

consommateurs sont endettés d'une façon ou d'une autre. Si vous devez 100 000 dollars pour votre maison et que votre salaire passe de 50 000 à 30 000 dollars par an, vous avez un gros problème. Vous commencez à dépenser moins, l'activité économique ralentit et cela alimente une déflation plus forte. Une économie peut ainsi entrer dans une spirale déflationniste.

Dans l'économie Bitcoin, la déflation est au cœur de la devise. Cela signifie que c'est une très mauvaise idée d'emprunter de l'argent en Bitcoin parce que vous devrez de plus en plus au fur et à mesure que le temps passe et que vous ne serez jamais en mesure de le rembourser. En revanche, si vous ne vous endettez jamais et que vous décidez d'épargner, l'argent que vous conservez vaudra un peu plus chaque jour.

C'est un cauchemar pour les banques parce qu'elles veulent que vous empruntiez toujours plus afin que vous payiez des intérêts sur vos emprunts. Elles veulent ainsi maintenir un écart entre les intérêts que vous payez, et ceux qu'elles paient pour emprunter l'argent qu'elles vous ont prêté.

C'est un plus grand cauchemar encore parce que les banques veulent que vous ouvriez un compte d'épargne et y déposiez de l'argent afin que vous puissiez percevoir des intérêts dessus et rester en phase avec l'inflation. Si vous ne déposez pas suffisamment d'argent à la banque dans un contexte inflationniste, votre argent perdra de la valeur. Mais si vous déposez de l'argent dans une banque, elle l'investira à votre place, percevra des intérêts, vous reversera des intérêts à un taux plus bas et conservera la différence. Donc si vous n'alimentez pas un compte d'épargne parce que votre argent prend de la valeur automatiquement par la déflation, les banques perdent.

Pour résumer, vous n'empruntez pas et vous ne déposez pas votre argent dans un compte d'épargne ou un compte d'investissement pour suivre le rythme de l'inflation, par

conséquent les banques perdent les revenus des prêts et des dépôts qui leur permettent d'emprunter peu et de prêter beaucoup, qui est un de leurs modèles économiques de base.

Donc, que reste-t-il à faire aux banques ? Eh bien, elles pourraient seulement passer leur temps à faciliter les transactions comme le font Visa, Mastercard, le réseau SWIFT, Western Union Money Transfer et d'autres. Mais on a déjà dit que les transactions Bitcoin sont faites de personne à personne et coûtent très peu. Les banques ne perçoivent même pas ce revenu.

Et c'est pour cela que les banques travaillent très, très dur en coulisse pour essayer de tuer Bitcoin avant qu'il ne les tue. Voilà quelques exemples :

- Capital One ferme les comptes bancaires si Bitcoin est mentionné.
- Les comptes Coinabul ont été fermés par Chase et US Bank parce qu'ils vendaient des Bitcoins.
- La plupart des banques canadiennes "Big 6" ont fermé les comptes bancaires de quiconque facilitait l'échange de Bitcoin.
- Commonwealth bank, la plus grande banque australienne, a fermé le compte de Coinjar pour avoir traité des transactions par Bitcoin.
- De même, certains individus ont déclaré que leur compte bancaire a été fermé pour avoir simplement transféré de l'argent de leur compte personnel pour acheter des Bitcoins.
- Citi Foundation, la branche de bienfaisance de Citi Group, a investi dans une étude qui essayait de lier Bitcoin à la récente arrestation du créateur du marché noir Silk Road. L'étude a été discréditée en quelques minutes par la publication d'un membre de Reddit et plus tard retirée.

Les banques qui sont le plus effrayées sont celles qui se

développent dans les pays comme l'Afrique du Sud, où les frais de transactions sont bien plus élevés que dans les pays développés. Ces frais sont élevés car les déposants ont tendance à être en moins bonne santé et épargnent de plus petites sommes, donc pour contrebalancer le fait qu'il y ait moins d'argent pour que les banques puissent investir, celles-ci assomment leurs clients avec de gros frais de transactions. Les pays développés ont tendance à avoir de nombreuses populations migrantes qui envoient de l'argent dans leurs familles à l'aide de services tels que *Instant Money* qui permet l'envoi d'un code par SMS à une personne qui peut ensuite aller dans un supermarché local afin de recevoir la somme associée. Les frais de transactions pour de tels services sont élevés et si Bitcoin devient un mode de transfert et de stockage d'argent plus efficace en terme de coûts, les banques des pays développés vont perdre un business très lucratif.

La guerre contre le Bitcoin vient tout juste de commencer. Les banques traditionnelles ont un gros stock de munitions pour la mener car leurs munitions c'est l'argent.

L'Internet des débuts était plus libre que celui d'aujourd'hui. Les monnaies chiffrées sont peut-être plus libres aujourd'hui qu'elles ne le seront jamais.

Annexe

On pourra relire à l'occasion ces 3 articles du Framablog :

- Bitcoin libérera-t-il la monnaie à l'échelle d'Internet ?
- Comment le Bitcoin peut faire tomber les États-Unis d'Amérique
- La monnaie électronique, 33 questions à Lionel Dricot (alias Ploum)

La monnaie électronique, 33 questions à Lionel Dricot (alias Ploum)

Lionel ou plutôt Ploum dans sa vie en ligne, beaucoup de lecteurs réguliers du Framablog le connaissent : non content de prendre position pour la monnaie électronique ou le revenu de base, il s'efforce de mettre en œuvre concrètement les solutions qu'il prêche. C'est ainsi qu'il a décidé de monnayer de façon originale ses billets de blog depuis quelque temps.

Tandis qu'il est sur la route du nanowrimo comme son copain Pouhiou en ce mois de novembre, nous avons souhaité faire le point avec lui sur l'état de son expérience, son évolution probable, et recueillir ses réponses et autres prédictions sur le développement ou non de ces pratiques numériques qui pourraient changer le monde.

C'est notre techie émérite Luc qui est aux commandes pour tourmenter Ploum de ses questions.

Bonjour Ploum. Tu pourrais te présenter un peu pour nos lecteurs qui ne te connaîtraient pas encore ?

Je suis blogueur, développeur de logiciel libre, ingénieur. J'aime écrire, je m'intéresse au futur et à notre société en général. J'ai même écrit des articles pour le Framablog.

2. Tu peux nous présenter aussi un peu Bitcoin et Flattr ?

Bitcoin est une monnaie, un moyen d'échange. Flattr est un moyen de transmettre des euros à un créateur. Les deux ne sont pas liés, même si on peut charger son compte Flattr avec des bitcoins (ils seront automatiquement convertis en euros). Mais le mieux c'est que je vous renvoie aux articles à ce sujet. J'ai écrit Bitcoin pour les nuls ainsi qu'une présentation du bitcoin pour Framasoft. Quand à Flattr, je le décris dans cet article.

5. Qu'est-ce qui t'a décidé à proposer ces modes de soutien sur ton blog ? Tu y trouves quoi par rapport à des moyens classiques comme le virement, la CB ou Paypal ?

Au départ, l'idée était de simplement jouer avec ces technologies. Sur le forum Bitcoin, tout le monde s'encourageait à accepter les bitcoins dans son business. Mais moi, mon blog n'était pas un business. Je ne gagnais strictement rien. Je me suis dit que j'allais donc accepter les dons à titre symbolique et pour tester. Pareil pour Flattr. En parallèle, en tant que membre du Parti Pirate, je me posais pas mal de questions sur les « business models » liés à la création. Comment trouver une alternative au traditionnel « Si on pirate de la musique, les musiciens

n’auront plus de sous » ? C’est un processus assez long que j’ai nourri d’expériences, de lectures, de rencontres.

J’ai fini par prendre conscience que, sans m’en rendre compte, moi aussi je créais. Et que donc, si je voulais avoir des arguments clairs, il fallait que j’arrive à monétiser ma création. Pas dans le but d’en vivre, mais simplement pour prouver que c’était possible. Si moi, avec un blog qui reste somme toute confidentiel, je peux faire un peu d’argent, c’est que le modèle existe. Ce que j’essaye de montrer aussi, c’est que je gagne un peu d’argent avec des créations qui sont libres et gratuites (mon blog est sous licence CC By) mais que je ne pourrais rien gagner du tout si, au contraire, je décidais de me protéger et tentais d’empêcher mes lecteurs de partager ce que j’écris.

22. Quels ont été les retours des lecteurs ?

Comme je l’ai dit, tout cela s’est fait progressivement, sans que j’en aie forcément conscience. Mon premier article sur bitcoin et Flattr date de 2010. Le véritable changement a eu lieu lorsque j’ai décidé de « rendre mon blog payant », en juillet 2013. Pour tout avouer, j’avais commencé cet article comme un texte générique d’encouragement à donner aux créateurs sur le Web. Et puis j’ai trouvé particulièrement amusant de le tourner d’une manière provocante. Je trouvais cela plus efficace, plus parlant. À vrai dire, je n’étais pas certain que cela fonctionnerait. Je m’attendais à beaucoup de retours de type « Mais pour qui tu te prends ? » ou « Franchement, tu te considères à ce point important qu’il faille te payer ? ». Mais je n’ai eu que très très peu de retours négatifs. Peut-être même pas du tout.

En fait, la démarche a été extrêmement bien comprise et j’ai réellement senti que j’avais mis les mots sur quelque chose qui était déjà partagé par beaucoup de monde. Je ne m’attendais pas à ce que ça fonctionne réellement mais j’ai reçu des dizaines de soutiens concrets. J’en ai été

personnellement tout retourné. Pour la première fois, je me rendais compte que ce que je faisais pouvait avoir de l'importance pour les gens. C'est même tombé dans l'extrême inverse avec des lecteurs s'excusant de ne pas pouvoir payer. Du coup, j'essaie maintenant d'insister : si ce que j'écris est disponible gratuitement c'est justement pour que tout le monde puisse y avoir accès, sans contrainte. Si j'ai été utile ou si j'ai fait plaisir à quelqu'un qui a du mal à joindre les deux bouts, c'est merveilleux. J'espère que cette personne me sera reconnaissante et, qu'à son tour, elle décidera d'être utile ou de faire plaisir à quelqu'un d'autre.

Appel aux dons dans le blog de Ploum

31. Tu saurais nous donner une estimation chiffrée de ce que tu as gagné avec Flattr ? Avec Bitcoin ? Sur combien de temps ?

J'envoie chaque année les comptes détaillés de mes gains Flattr à mes supporters Flattr. Mais je vais faire quelques révélations en primeur pour Framasoft.

Jusqu'à l'année 2012, Flattr me rapportait entre 4 et 40 € par mois. J'ai gagné 155 € en 2011 et 240 € en 2012. En 2013, les choses ont commencé à exploser. Suite à mon article suggérant de tester Flattr, mes gains sont montés entre 80 € et 120 € par mois. L'article pour rendre mon blog payant m'a propulsé sur orbite avec des gains entre 160 et 225 € par mois, rien que sur Flattr. Donc oui, l'article pour rendre mon blog payant a été un véritable déclencheur auprès de mon public.

Pour tous les créateurs, je le dis et le répète : vous devez convaincre votre public. Vous devez expliquer pourquoi le public devrait vous payer. Et il faut répéter cela régulièrement tout en évitant d'être lassant. C'est un équilibre très difficile. Juste mettre un bouton Flattr et attendre ne sert à rien. Flattr est un moyen de paiement. Mais il faut donner envie au public de payer.

Pour les autres moyens de paiement, j'avoue ne pas tenir de comptes car cela m'ennuie profondément. Mais rendre mon blog payant fait que, de temps en temps, je reçois un don Paypal ou un virement surprise. C'est quand même toujours très agréable et c'est extrêmement motivant ! Même un petit don me donne envie de me jeter sur mon clavier pour me surpasser. Cela me donne l'impression d'être utile.

Après, il faut relativiser. Je ne peux pas vivre de mon blog. Mais on n'en est pas tellement loin. En discutant autour de moi, j'ai découvert qu'il y avait des journalistes *freelance*, des musiciens ou des écrivains qui gagnaient moins que moi ! Les chiffres sont donc devenus assez importants pour me permettre d'affirmer que le modèle fonctionne et qu'il pourrait même se révéler préférable pour les créateurs par rapport au modèle actuel.

24. Dans ton billet, tu poussais les développeurs, les artistes, etc. à utiliser ces moyens de soutien. Tu as convaincu beaucoup de gens ? Tu as eu des retours ?

J'observe de temps en temps des blogueurs qui copient un de mes billets sur le sujet pour faire un appel au don. Cela me fait plaisir (je précise qu'ils me préviennent). Mais je fais partie d'une mouvance plus large où je ne suis qu'un élément parmi tant d'autres. Lorsqu'on observe un auteur comme Neil Jomunsi se poser des questions sur un modèle traditionnel (il vend ses nouvelles et livres sur Amazon/Kobo/etc) et observer qu'il gagne plus avec Flattr qu'avec Amazon, on ne peut pas dire « Il a été convaincu par Ploum ». Non, il baigne tout

simplement dans un écosystème qui remet certaines choses en question.

Je fais partie de cet écosystème et si je peux aider des lecteurs à se poser des questions, c'est génial. D'ailleurs, je me remets moi-même sans arrêt en question en lisant d'autres personnes. Mais, au final, ce n'est pas un qui convainc l'autre. C'est un groupe qui évolue. Et je trouve cela très positif. Il n'y a pas une bonne solution qui va supplanter une mauvaise. Il faut juste remettre en marche l'évolution permanente que certains s'entêtent à vouloir freiner.

Ploum voit loin. Aux avant-postes des nouveaux usages numériques, il nous confirme que la voie est libre, depuis cette percée vers l'avenir où se cache étrangement le profil de la Castafiore.

25. Que réponds-tu aux créateurs qui disent que le modèle du don, c'est revenir à une forme de mendicité ?

Je comprends très bien cette position car j'étais comme eux. Comme je l'explique, je pensais qu'on pouvait donner de l'argent de deux façons : soit parce qu'on avait besoin/envie

de quelque chose qui n'était pas disponible gratuitement (on parle alors d'un « achat ») soit en donnant volontairement (la « charité »). Et demander la charité a souvent une connotation négative.

Mais cette vision vient tout simplement de l'erreur que nous faisons de confondre prix et valeur. Cette erreur est tellement forte qu'il a été observé que les livres électroniques en dessous de 3-4 € ne se vendent pas car les gens considèrent que, si c'est bon marché, c'est nul.

Pourtant, rien n'est plus faux ! Prenez un MP3 téléchargé d'une musique. Et prenez la même musique issue du CD collector avec boîte platinée or. L'un est gratuit, l'autre est très cher. Pourtant, au moment de l'écoute, vous ne pourrez pas les différencier ! La valeur est exactement la même ! Et si la musique est bonne, cela peut être une très grande valeur même si le MP3 est gratuit.

En conclusion, on peut donc dire que, aujourd'hui, pousser les gens à acheter un CD ou de la musique en ligne payante, c'est de la mendicité. En effet, la même musique est disponible gratuitement ! Demandez d'ailleurs à ceux qui achètent leur musique en ligne pourquoi ils ne téléchargent pas sur The Pirate Bay. Dans la plupart des cas, la réponse sera « Pour soutenir l'artiste ».

C'est donc un non-sens de parler de mendicité alors que nous sommes déjà dans cette situation. Le paiement est *déjà* volontaire. Ce que je reproche c'est que l'incitation à payer est extrêmement négative (on nous menace, on nous insulte, on détruit la notion du partage) alors qu'avec le prix libre, l'incitant est positif (payez comme vous le voulez, autant que vous pouvez pour soutenir l'auteur et l'aider à diffuser son art auprès de ceux qui ne peuvent pas payer). D'ailleurs, l'expérience In Rainbows de Radiohead ou les Humble Bundles prouvent amplement que l'incitant positif est commercialement bien plus rentable que le négatif ! De plus en plus d'artistes

le comprennent. D'ailleurs, aujourd'hui même, Moby vient d'annoncer la disponibilité gratuite de son dernier album via Bittorrent…

26. Si tu pouvais changer quelque chose à Bitcoin ou Flattr, ce serait quoi ?

À Bitcoin, ce serait la facilité d'utilisation. J'y avais réfléchi et je pense que beaucoup de gens se penchent dessus. Cela va prendre du temps et, aujourd'hui, c'est vraiment le problème le plus critique (la sécurité étant notamment affaiblie par la complexité de Bitcoin). Avec Flattr, j'ai quelques idées mais j'en discute justement avec l'équipe de Flattr. Du coup, je vais garder la surprise

29. …et la valeur fluctuante du Bitcoin ? Elle ne te gène pas ? Le bitcoin qui passe de 150 à 300 € en une semaine, t'en penses quoi ?

Que l'euro fluctue beaucoup par rapport à mes bitcoins Plus sérieusement, il faut garder à l'esprit que la valeur qui importe c'est celle du moment où on dépense ses bitcoins. J'ai découvert que pizza.be et pizza.fr acceptaient les bitcoins. Du coup, c'est moins la valeur en euro du bitcoin qui importe que le prix de la pizza. Plus il y aura de sites acceptant les bitcoins, moins on se préoccupera de la valeur en euros.

Ceci dit, c'est aussi une excellente leçon d'économie. Je suis de l'avis de Rick Falkvinge qui estime que Bitcoin va complètement révolutionner la société.

J'entends beaucoup dire que le problème de Bitcoin, c'est qu'il est inégal. Que les premiers arrivés sont les plus riches. Mais, historiquement, ça a toujours été comme ça. La plupart des fortunes de France remontent à la noblesse d'empire. Les riches n'ont jamais rien fait qu'hériter des situations qu'ils ont parfois fait fructifier. Mais c'est facile de devenir encore plus riche quand on est déjà riche. Bitcoin n'est, malheureusement, pas un outil social. En

revanche, je suis persuadé qu'il va justement permettre l'émergence de nouveaux paradigmes sociaux. Je pourrais vous en parler pendant des heures

Crédit photo Antanacoins licence CC BY-SA 2.0.

61. Tu expérimentes Patreon, ça fonctionne ? Et Gittip alors, pourquoi tu n'es pas convaincu ?

Patreon est très brouillon. Le site est à la limite de l'incompréhensible et le modèle de versement rend les charges très lourdes. Pour certains dons de 1$, je n'ai reçu que 40 centimes ! C'est quand même dérangeant surtout que j'ai suggéré plusieurs fois des améliorations mais je n'ai jamais eu de réponse. Patreon bénéficie de l'aura de son créateur, Jack Conte, mais, au contraire de Flattr, je le trouve très mal géré, mal pensé. J'espère qu'ils vont s'améliorer.

À l'inverse, Flattr est très bien léché mais ne bénéficie pas de l'aura d'un artiste renommé. De plus, Flattr n'est pas dans la Silicon Valley et, blasphème absolu, n'est pas en dollars !

Quand à Gittip, j'ai testé mais je n'ai tout simplement pas compris l'intérêt. Flattr et Patreon tente chacun de résoudre un problème clair. Je n'ai pas perçu le problème que Gittip tentait de résoudre. Je trouve plus simple de faire un don par

Paypal/Bitcoin que par Gittip. Ceci dit, j'ai un compte sur Gittip et peut-être que cela va s'améliorer.

28. Comment perçois-tu l'évolution de ces solutions de financements alternatifs dans les prochains mois/années ?

Tout comme on a observé une explosion des acteurs du crowdfunding (Kickstarter, Ulule, Kisskissbankbank, etc), je pense qu'on va voir une explosion des solutions de micro-financement. Et puis qu'un filtre va se faire. C'est assez logique. Je prédis par contre de plus en plus de sites qui vont accepter les bitcoins et qui vont même en faire leur monnaie courante. En effet, le problème pour un européen sur Patreon, c'est que tout se fait en dollars. Il est donc dépendant du cours du dollar. Pour un américain sur Flattr, il est en euros. Pour le reste du monde, les deux situations sont problématiques. Je pense qu'on va observer graduellement un mouvement vers le bitcoin comme étalon de la monnaie internet.

J'ai également prédit, dans une petite fiction appelée « Le blogueur de demain », l'arrivée d'outils de financements à l'échelle individuelle. On va en arriver à un niveau où chacun pourra faire sa comptabilité et ses petits projets personnels directement en ligne. Un voyage avec des amis ? Un repas de Noël en famille ? L'achat d'une voiture en couple ? Le budget sera établi sur un service en ligne et l'argent sera directement dessus.

Au final, de moins en moins d'argent transitera par les banques. On paiera directement avec son smartphone et on achètera des cartes de crédit prépayées. La notion même de « salaire » va s'effilocher. Les gens seront de plus en plus auto-entrepreneurs et travailleront au coup par coup.

Ce scénario peut se révéler idyllique, chacun ayant plus de temps pour les projets qui lui tiennent à cœur, l'argent perdant de l'importance, tout comme il peut être apocalyptique s'il est nécessaire de travailler 80h par semaine pour se

payer de quoi manger. C'est la raison pour laquelle je suis un fervent supporter du revenu de base : avec un revenu de base et une indépendance vis-à-vis des banques, le net sera un véritable outil de libération sociale.

33. Selon toi, quelles sont leurs principaux inconvénients et freins à l'adoption ?

Je suis toujours surpris de voir que des gens éduqués, des intellectuels, refusent d'acheter en ligne par simple crainte irrationnelle de « l'arnaque ». Il y a un réel souci à ce niveau. Parfois, des lecteurs me disent qu'ils veulent me soutenir mais ils n'ont pas de carte de crédit, ils n'ont pas d'argent en ligne. J'avoue que, au 21e siècle, c'est tout de même un frein à l'utilisation de beaucoup de services.

La France est spécialement en retard par rapport à la Belgique. En Belgique, toutes les banques sont entièrement accessibles en webbanking depuis des années et il est possible de faire gratuitement, en un seul clic, un virement vers n'importe quel compte en banque européen (zone SEPA). Lorsque j'entends des Français qui me disent devoir se rendre au guichet pour effectuer un virement ou des suisses me dire qu'effectuer un virement vers la Belgique coûte 10-15 € (ce qui me semble illégal selon l'accord SEPA), j'en reste effaré. J'ai l'impression que nous ne vivons pas dans la même époque. C'est une des raisons qui rendent les USA si attirants pour les sociétés web : un système bancaire unifié, une langue quasi-unique.

D'une manière générale, c'est très difficile d'expliquer un modèle basé sur Flattr et Bitcoin à une personne pour qui acheter un livre sur Amazon relève de la témérité absolue ou de la science-fiction. Peut-être que je vais parfois un peu trop vite en besogne mais il ne faut pas sous-estimer la vitesse à laquelle peut se produire un changement total de mentalités. Il y a un point de non-retour où, tout d'un coup, l'opinion bascule. Aujourd'hui encore, le net est relativement

« accessoire » dans la société actuelle. Beaucoup pointent du doigt qu'il est moins important que ce que les geeks disent. C'est vrai. Mais je prédis qu'il sera beaucoup plus important dans le futur que tout ce qu'on peut imaginer.

42. Un petit mot de la fin ?

mmmh Aka m'a promis plusieurs fois d'intégrer Flattr sur le Framablog. S'il ne le fait pas, la prochaine fois ça se règlera à coup de frites dans les narines, une fois.

Comment le Bitcoin peut faire tomber les États-Unis d'Amérique

Un peu d'économie sur le Framablog aujourd'hui, avec le *pirate* Rick Falkvinge qui voit dans la monnaie **Bitcoin** une alternative à la fictive toute-puissance du dollar.

Comment le Bitcoin peut faire tomber les États-Unis d'Amérique

[How Bitcoin can bring down the United States of America]

Rick Falkvinge – 4 juin 2013 – Site personnel
(Traduction : Slystone, nhrx, letchesco, Asta, Gatitac, rou + anonymes)

Le Bitcoin représente une menace importante pour la domination monétaire des États-Unis, la seule chose qui conforte encore leur statut de superpuissance mondiale. Suite aux défauts de paiement des États-Unis sur leurs emprunts internationaux le 15 août 1971, la balance commerciale américaine avait été maintenue grâce aux menaces militaires et en incitant les gens à acheter des dollars pour financer la consommation permanente des États-Unis. Alors que d'autres devises n'ont pas réussi à dépasser le dollar américain, et donc ce mécanisme qui

maintient la dominance économique de la nation, le Bitcoin pourrait bien y parvenir.

Pour comprendre ce scénario, il faut saisir à quel point les États-Unis sont en faillite. Pour certaines raisons, la plupart des feux de l'actualité sont actuellement braqués sur l'échec de l'Euro ; ceci probablement à cause du fait que le dollar américain a échoué depuis longtemps, et qu'il est maintenu sous perfusion en faisant éclater non sans mal une bulle spéculative par jour. Une version ELI5 est disponible ici *(NdT : ELI5 : « explain it like I'm five », expliquez-le-moi comme si j'avais 5 ans)*, mais en un mot, les États-Unis sont en défaut de remboursement de leurs emprunts internationaux suite à la guerre du Viêtnam, et depuis ont dû emprunter de plus en plus pour financer leur consommation extravagante. Depuis bien longtemps ils empruntent toujours plus, pour simplement rembourser les intérets des emprunts antérieurs. L'an dernier, le déficit du budget des États-Unis a atteint le niveau astronomique de 50 % – pour chaque dollar de recette, deux ont été dépensés. Étrangement, peu de monde en parle – j'imagine que si c'était le cas, la capacité des États-Unis à rembourser leurs emprunts serait remise en question, ce qui provoquerait l'écroulement du château de cartes comme si une tonne de briques était déversée dessus, alors personne n'a intêret à faire des vagues. Après tout, tout le monde est assis sur des réserves de dollars qui deviendraient sans valeur du jour au lendemain si ceci devait arriver.

Les États-Unis ont relancé leurs planches à billets le 15 août 1971 et ne les ont pas arrêtées depuis. Rien que pour l'année 2011, 16 mille milliards (un 16 suivi de douze zéros) de dollars ont été imprimés pour maintenir l'économie américaine. Pour se faire une idée, c'est un peu plus que le produit intérieur brut des États-Unis. Pour chaque dollar produit à partir de la valeur (ajoutée), un dollar supplémentaire a été imprimé à partir de rien, dans l'espoir que quelqu'un voudrait

bien l'acheter. Et les gens l'achètent ! C'est un fait, il y a ici un mécanisme clé qui force les gens à continuer à acheter des dollars américains.

Les États-Unis sont maintenus en vie en tant que nation par le fait que si quelqu'un souhaite acheter des produits à une autre nation comme la Chine, il doit d'abord acheter des dollars américains puis les échanger contre la marchandise qu'il désire en Chine. Cela conduit tous les pays à acheter des tas de dollars américains pour remplir leurs réserves monétaires.

Le fait que les gens soient obligés de continuer d'acheter des dollars américains pour obtenir ce qu'ils veulent de n'importe qui d'autre dans le monde est le mécanisme qui maintient l'ensemble de l'économie américaine et, plus important encore, alimente son armée qui applique à son tour ce mécanisme (voir en Irak, Libye, Iran, etc.). C'est un cycle de domination économique imposé par la force.

(À noter que l'on peut se demander dans quelle mesure la classe moyenne américaine profite encore de ce système. Il y a dix ans, cette boucle auto-alimentée faisait que le niveau de vie moyen aux États-Unis était sensiblement supérieur à celui du reste du monde occidental. De nos jours, les États-Unis arrivent souvent derniers des indicateurs de niveau de vie.)

Puisque les articles sur « la fin du monde » sont d'habitude rejetés comme relevant d'illuminés conspirationnistes, je voulais commencer cet article en présentant des faits économiques reconnus. Les États-Unis sont en faillite et la seule béquille pour les maintenir debout est leur armée, ainsi que le fait que tout le monde a de lourds investissements dans le pays, si bien que personne ne veut les voir faire faillite. Donc les emprunts et les dépenses excessives continuent une journée de plus… jusqu'à ce que cela ne soit plus possible.

Que se passerait-il si les États-Unis étaient un jour

incapables de poursuivre leurs dépenses démesurées ? On assisterait à un crash gigantesque de l'économie mondiale, mais plus important, les États-Unis s'effondreraient à la mode soviétique, mais plus gravement encore, en raison de différences structurelles. (Pour comprendre ces différences, réfléchissez au fait que les transports publics ont continué de fonctionner pendant l'effondrement soviétique et que la plupart des familles étaient déjà bien préparées pour faire face à la pénurie de nourriture. Aux États-Unis vous verriez à la place des gens isolés dans des banlieues sans carburant, sans nourriture ni médicaments, avec seulement plein d'armes et de munitions. Consultez l'étude d'Orlov sur l'écart entre les effondrements et le retard d'effondrement pour plus d'informations sur cette différence structurelle).

Arrivent les Bitcoins, qui peuvent briser le cercle vicieux des emprunts et des dépenses excessives.

Comme nous l'avons vu, la raison pour laquelle les gens sont obligés d'acheter du dollar américain, c'est qu'il est la base du système d'échange de valeur. Si vous voulez un gadget fabriqué en Chine ou en Inde, vous devez d'abord acheter des dollars américains, pour ensuite échanger ces dollars contre le gadget. Mais nous l'avons observé, le Bitcoin dépasse de loin le dollar sous tous ses aspects en tant que gage de valeur pour le commerce international. Utiliser des Bitcoins c'est moins cher, plus facile et bien plus rapide que les actuels transferts de valeur internationaux.

Pratiquement toutes les personnes impliquées dans le commerce international à qui j'ai parlé passeraient à un système semblable à Bitcoin si elles en avaient la possibilité, évacuant des années de frustrations héritées du système bancaire actuel (qui utilise le dollar américain). Si cela arrivait, les États-Unis ne seraient plus en mesure de trouver des acheteurs pour leurs dollars fraîchement imprimés qui maintiennent leur économie (et financent leur armée).

Si ce cycle de monopole et dépendance commerciale du dollar prend fin, les États-Unis d'Amérique s'écrouleront. Lourdement. Cela semble inévitable désormais, et le Bitcoin est peut-être le système qui rompra ce cycle.

Crédit photo : Zcopley (Creative Commons By-Sa)

Bitcoin libérera-t-il la monnaie à l'échelle d'Internet ?

« Papa, tu faisais quoi quand les crédits Facebook sont devenus l'unique moyen de paiement sur internet ? »

C'est par cette phrase cinglante que s'achève le billet de notre ami Ploum, qui nous a fait l'honneur d'un article original sur le Framablog.

Le propos se divise en deux parties.

La première nous explique très clairement pourquoi nous avons urgemment besoin d'un système d'échange monétaire libre et décentralisé, à fortiori lorsqu'il s'agit de micropaiements ou de microdons.

La seconde est consacrée à **Bitcoin** (cf cette vidéo) qui semble

potentiellement d'ores et déjà répondre au besoin mais qui n'est pas sans poser questions et problèmes[1].

Je ne sais si Bitcoin s'imposera, mais celui qui réussira lui ressemblera.

Et ce jour-là Papa sera fier d'annoncer à son rejeton qu'on pourra non seulement se passer des crédits Facebook mais qu'on n'aura plus à trembler servilement lorsque les bourses mondiales se mettent à tousser.

Décentralisation monétaire

Ploum – juillet 2011
Licence Creative Commons By-Sa

Quelle que soit votre motivation profonde, vous êtes beaucoup, parmi les lecteurs de Framasoft, à voir dans l'Internet un espace de liberté, d'expression, de communication, d'échanges, d'entraide et bien d'autres.

Afin que cette liberté soit garantie, il est nécessaire d'éviter à tout prix une centralisation qui mettrait le pouvoir absolu d'un service donné dans les mains d'une seule personne, entreprise ou gouvernement. En effet, un service décentralisé assure non seulement la pérennité du réseau mais permet également une indépendance d'un client par rapport à un fournisseur de service.

C'est pour cette raison qu'à Framasoft nous sommes de fervents défenseurs de l'email, que nous utilisons XMPP à la place de MSN, que nous préférons identi.ca à Twitter et que nous suivons avec impatience les progrès de Diaspora pour proposer une alternative à l'omniprésent Facebook.

Mais si l'entraide, la communication et l'échange sont de très belles choses, ils ne sont malheureusement pas entièrement suffisants et la majorité d'entre nous, Framasoft inclus, a encore terriblement besoin d'argent.

Alors que le troc est entièrement décentralisé, chacun troquant selon ses convenances, l'argent est un service totalement centralisé fourni par les états. D'ailleurs, ne parle-t'on pas de « banque centrale » ?

Ce système est, de plus, complètement opaque, les citoyens devant entièrement faire confiance à l'état central qui, lui-même, délègue une partie de ce pouvoir aux banques privées.

Le fait que ce soit un bien ou un mal reste sujet à interprétation. Néanmoins, en regard de la crise économique de 2008, il faut bien admettre que le résultat de l'actuelle politique économique centralisée est relativement mitigé. C'est d'ailleurs une des raisons pour laquelle certaines collectivités ont développé des systèmes d'échange locaux (SEL), en temps qu'alternative locale et auto-gérée à l'économie traditionelle.

Sur le réseau la situation n'est guère meilleure. Quelques acteurs centralisés comme Visa et Paypal monopolisent les transferts entre monnaie réelle et monnaie virtuelle. Cette situation d'oligopole leur est, bien entendu, fortement profitable : taxes à l'entrée d'argent dans le système, taxe à la sortie d'argent du système, commission sur chaque transaction. Sans compter que toutes vos dépenses, représentant une grande part de votre vie privée, sont fichées et archivées entre les mains d'entreprises pas toujours scrupuleuses.

Au final, il s'ensuit un véritable racket de l'internaute : afin que votre correspondant puisse recevoir 1€ au bout de la ligne, il n'est pas rare de devoir verser 1,20€, 1,50€ voire 1,80€, sous forme de frais fixes et de pourcentage sur la transaction. Ces frais, négligeables pour les grosses sommes, empêchent tout développement réel des petits transactions, des microdons, des micro-achats. Ces entreprises acquièrent également un pouvoir politique, s'octroyant le droit de « geler » ou de supprimer des comptes, comme ce fut le cas

pour Wikileaks.

Le transfert de petites sommes est pourtant un moteur de notre économie. Si l'on hésite à acheter un album de musique à 14€, acheter une chanson à 1€ peut se faire sur un coup de tête. Les grandes entreprises ont donc développé des systèmes de « comptes » ou d'abonnements. Vous versez une somme importante en une fois que vous pourrez dépenser petit à petit. L'Apple Store ou les crédits Facebook fonctionnent sur ce principe. Mais outre le fait que ces systèmes sont centralisés, ils nécessitent d'immobiliser une grosse somme d'un seul coup et ne sont bien sûr pas interopérables. Une fois vos 25€ versés sur Facebook, ils sont irrécupérables et non-transférables en dehors des applications Facebook.

Quelques alternatives tentent également de proposer un modèle original, comme Flattr. Flattr offre en effet de déterminer une somme mensuelle fixe qui sera divisée par le nombre de dons faits chaque mois. Néanmoins, cela reste centralisé et avec des frais prohibitifs. Ainsi, Framasoft ne touche que 90% des dons faits via Flattr.

Une solution idéale serait de proposer un système d'échange monétaire libre et décentralisé. Un tel système existe et a un nom : Bitcoin.

Techniquement, le fonctionnement de Bitcoin est relativement complexe, se basant sur des algorithmes cryptographiques et le peer-to-peer. Le gros problème d'une monnaie virtuelle est d'éviter la « double dépense ». Par essence, une information virtuelle peut être répliquée à l'infini, problème qui tracasse l'industrie musicale depuis plusieurs années.

Bitcoin résout ce problème en utilisant le peer-to-peer. Lorsque Alice donne un bitcoin à Bob, elle rend la transaction publique. Les participants au réseau bitcoin (les « mineurs ») vérifient que la transaction est légitime en s'assurant que, dans leur historique des transactions, Alice est bien la

dernière personne à avoir reçu ce bitcoin précis, chaque bitcoin étant unique. Les « mineurs » annoncent sur le réseau que la transaction est confirmée. Quand suffisamment de « mineurs » ont confirmé la transaction, Bob peut considérer que Alice ne pourra plus dépenser son bitcoin et qu'il en est donc le propriétaire. Si Alice tente de redépenser son bitcoin, les « mineurs » refuseront la transaction, arguant que, d'après l'historique, Bob est le légitime propriétaire du bitcoin.

Pour encourager les « mineurs » à faire ce travail de vérification, le réseau gratifie le premier mineur à vérifier chaque bloc de transactions d'un bonus. Ce bonus, qui est pour le moment de 50 bitcoins, décroît avec le temps et a pour conséquence de distribuer la monnaie graduellement à travers le réseau.

Le nombre de bitcoins ainsi générés étant une fonction décroissante, on a pu calculer que le nombre total de bitcoins ne dépasserait jamais 21 millions.

Intrinsèquement, le bitcoin n'a aucune valeur. C'est juste la preuve qu'un échange a été fait. Mais n'en est-il pas de même pour n'importe quelle monnaie ?

Afin de garantir l'anonymat, les transactions ne se font pas directement entre Alice et Bob mais entre deux adresses du type 1GTkuikUyygRtkCy5H6RMuTMGA1ypqLc1X, qui est la partie publique d'une clé de cryptage asymétrique. Bob donne à Alice son adresse et seul eux deux savent à qui appartient l'adresse. Le réseau ne possède aucun moyen de lier l'adresse réceptrice à Bob. Bob, de son côté, possède la partie privée de la clé, lui permettant de prouver qu'il est bien le destinataire de tous les bitcoins envoyés à cette adresse. Bob peut générer autant d'adresses qu'il le désire et l'usage est de générer une adresse par transaction.

La facilité d'échange et la rareté du bitcoin en font un

candidat idéal pour une monnaie électronique décentralisée. Des sites de vente en ligne acceptant les bitcoins sont donc apparus sur le net. Beaucoup de personnes, tablant sur un succès futur des bitcoins, on décidé d'en acheter une certaine quantité, ce qui a fait monter le prix du bitcoin. Une véritable économie parallèle s'est développée, principalement basée sur la spéculation. La valeur du bitcoin est passée de 0,01€ en novembre 2010 à 25€ en mai 2011, avant de redescendre aux alentours de 10€ en juin 2011.

Si Richard Stallman n'a pas encore pris de position publique au sujet du bitcoin, le fait qu'il s'agisse d'un logiciel libre, décentralisé et permettant des paiements anonymes en fait la coqueluche de certains libristes. La Free Software Foundation elle-même accepte dorénavant les donc en bitcoins. Après moins de deux jours, plus de 270 bitcoins avaient été envoyés anonymement, l'équivalent de près de 700€ de dons à l'époque et 2700€ actuellement !

Mais tout n'est pas rose au pays des bitcoins et les critiques sont nombreuses.

Beaucoup s'étonnent notamment au fait d'attacher de la valeur à quelque chose qui n'en a pas. À ce sujet, le bitcoin ne diffère pas d'un bout de papier ou même d'un morceau de métal jaune brillant. La valeur attachée à un objet est en effet liée à la confiance que le possesseur a de pouvoir échanger cet objet. Mais entre accorder sa confiance à un gouvernement et l'accorder à un réseau P2P décentralisé, il y a un pas que beaucoup hésitent à franchir.

Le bitcoin est anonyme et permet de gros échanges d'argent sans aucun contrôle, tel la vente de drogue ou de services illicites. Les partisans du bitcoin répliquent que bitcoin n'est qu'un outil, comme l'est la monnaie papier. Beaucoup d'outils facilitent les activités illégales: Internet, la cryptographie, le réseau Tor. Il est d'ailleurs déjà possible d'acheter de la drogue en ligne en payant en bitcoins. Faut-il

bannir ces outils pour autant ? Une chose est certaine: le bitcoin opère dans une zone encore floue de la légalité. Même les activités parfaitement licites sont confrontées à un problème de taille: comment déclarer des revenus en bitcoins ? Faut-il payer des impôts ? À ce titre, Bitcoin peut être considéré comme un gigantesque SEL à l'échelle d'Internet.

Nombreux, également, sont ceux qui pointent l'inégalité de Bitcoin. En effet, les premiers bitcoins étaient très faciles à générer. Les tous premiers entrants ont donc, sans effort, récolté des milliers de bitcoins. Est-ce que le fait d'avoir cru en bitcoin avant tout le monde est suffisant pour justifier leur nouvelle richesse ? Le bitcoin n'est-il pas une gigantesque pyramide de Ponzi ? De manière amusante, cette critique semble typiquement européenne. Dans un monde où la richesse est un signe de succès, les Américains ne semblent en effet pas y voir le moindre inconvénient, surtout dans la mesure où cet enrichissement entièrement virtuel ne s'est pas fait au détriment d'autres personnes.

Économiques, philosophiques, morales, techniques ou politiques, Bitcoin interpelle et soulève de nombreuses questions à propos du système dans lequel nous vivons, ne laissant personne indifférent. À tel point que certains se demandent si le prix actuel du bitcoin n'est pas entièrement artificiel et créé par l'enthousiasme des spéculateurs. Sa difficulté d'utilisation et l'apparent amateurisme des sites acceptant les bitcoins ne semblent pas plaider en faveur du bitcoin.

En Juin 2011, MtGox.com, le principal site d'échange de bitcoin contre des dollars, a été piraté et des opérations ont été réalisées de manière frauduleuse, plongeont l'économie du bitcoin dans l'incertitude pendant une semaine complète. La valeur du bitcoin n'en a que peu souffert mais, pour certains, l'évênement a été un signal d'alarme: le bitcoin est encore très expérimental et sa valeur peut tomber à zéro en quelques heures.

Mais, malgré tout, Paypal, les crédits Facebook et les pièces d'or de World of Warcraft nous ont démontré que la généralisation des monnaies virtuelles est une évolution inéluctable. Si elle n'est pas exempte de critiques, Bitcoin semble à ce jour la seule alternative libre et décentralisée utilisable.

Bitcoin disparaitra-t-il comme une bulle spéculative après quelques mois ? Transformera-t-il durablement la société ? J'avoue ne pas en avoir la moindre idée mais je sais que mon plus grand cauchemar est de me réveiller un matin avec une petite tête blonde me demandant auprès de mon lit: « Papa, tu faisais quoi quand les crédits Facebook sont devenus l'unique moyen de paiement sur internet ? »

Notes

[1] Crédit photo : TraderTim (Creative Commons By-Sa)