André Boyer
Professeur Emérite en Sciences de Gestion,
Université de Nice Sophia-Antipolis,
Laboratoire ATHENA
boyer@unice.fr

LA PROBLÉMATIQUE DU BITCOIN

SOMMARIO

Bitcoin è sia un sistema di pagamento sia una valuta virtuale. Per creare e gestire bitcoin, si utilizza un software secondo un protocollo che retribuisce gli agenti che hanno supportato le transazioni. Il problema cruciale del sistema Bitcoin, basato su un software libero e open source, è quello della fiducia nel suo funzionamento. Bitcoin non si basa su alcuna garanzia tangibile, come tutte le valute fiduciarie: il valore di Bitcoin è il valore che gli è dato dai partecipanti al sistema.

Il sistema Bitcoin, a differenza dell'attuale sistema bancario di riserve frazionarie, è piuttosto un generatore di deflazione. In futuro, è possibile che i principi di una valuta crittografica come il sistema Bitcoin siano deviati dalle banche centrali. Questo sistema ha anche un grave difetto, quello dell'enorme consumo di energia elettrica che genera e solleva questioni etiche, economiche e informatiche.

Resta il fatto che non possiamo più ignorare che le cripto valute sono ormai arrivate.

RÉSUMÉ

Le Bitcoin est à la fois un système de paiement et une monnaie virtuelle. Pour créer et gérer les bitcoins, il s'appuie sur un logiciel qui génère des bitcoins selon un protocole permettant de rémunérer les agents qui ont pris en charge les transactions. Car le problème crucial du système Bitcoin, projet de logiciel libre et open source, est celui de la confiance dans son fonctionnement qu'il résout en s'appuya. Le Bitcoin ne repose sur aucune garantie tangible, comme toutes les monnaies fiduciaires : la valeur du Bitcoin est celle que lui accordent les participants au système Bitcoin.

Le système Bitcoin, à l'opposé du système bancaire actuel des réserves fractionnaires, est plutôt générateur de déflation. À l'avenir, il est possible que les principes d'une monnaie cryptographique tel que le système Bitcoin, soient détournés par les Banques Centrales. Ce système possède aussi un grave défaut, celui de l'énorme consommation d'énergie électrique qu'il engendre et soulève des questions éthique, économique et informatique.

Il reste que l'on ne peut plus ignorer que les crypto-monnaies ont désormais émergé.

1 INTRODUCTION

Le Bitcoin (de l'anglais bit : unité d'information binaire et coin « pièce de monnaie») est à la fois un système de paiement et une monnaie virtuelle, qui ont été inventés en 2008 par un inconnu caché sous le nom de Satoshi Nakamoto.
Le système de paiement Bitcoin permet d'effectuer des transactions d'un compte vers un autre, grâce à des logiciels appelés *wallets*, l'autorité surveillant la validité de la transaction étant assurée par des logiciels de vérification appelés *mineurs*.
Le principe de base de ce système consiste à garantir la validité d'une transaction (X a bien payé Y) à partir d'un registre accessible à tous les membres du réseau Bitcoin, appelé *chaîne de blocs* qui contient toutes les transactions en bitcoins depuis le début du fonctionnement du réseau en 2008, un registre qui ne peut être modifié par personne.
Le point de départ du système Bitcoin est donc la sécurité absolue des transactions, alors qu'il est adossé au réseau Internet qui offre pourtant d'immenses possibilités de fraude. Pour faire partie du système Bitcoin, il suffit d'installer un logiciel approprié à *Bitcoin Core* sur son ordinateur ou son smartphone, afin d'être payé ou de payer en bitcoins par l'intermédiaire d'un courtier en bitcoin. De plus des distributeurs et échangeur automatique de bitcoins sont progressivement installés dans le monde par ces courtiers, au nombre de mille sept cent environ, la majorité se trouvant aux Etats-Unis et quelques uns en France.
Aux Pays-Bas par exemple, des distributeurs de billets acceptent de grosses sommes d'argent liquide en euros ou en dollars pour créditer le portefeuille virtuel des clients en bitcoins, ou au contraire recevoir des Euros en échange de bitcoins, dans un quasi anonymat. Cependant la commission moyenne des distributeurs atteint 6%, alors que celle des sites spécialisés dans le commerce de bitcoins s'élève à environ 0,25 % du montant de la transaction. Naturellement, on accuse ces distributeurs de faciliter le blanchiment d'argent sale et l'évasion fiscale, loin des regards des autorités qui luttent contre des paradis fiscaux qui apparaissent démodés par rapport à l'apparition des monnaies virtuelles comme le bitcoin qui ne relèvent par définition d'aucune autorité monétaire.
Au départ, pour acheter ou de vendre des bitcoins, il faut toutefois ouvrir un compte en bitcoins auprès d'une plateforme d'échange ou d'un site de vente qui exigent les renseignements classiques au client pour ouvrir un compte et effectuer un dépôt en Euros par carte bancaire, Paypal ou virement SEPA. Le client est alors crédité en bitcoins, avec une adresse de portefeuille bitcoin. Il peut alors se livrer aux aléas de la spéculation puisque la valeur du bitcoin est passée de 1000$ à plus de 15000$ pendant l'année 2017, avec de fortes variations prévisibles. Pour effectuer ces opérations, il lui faudra acheter ou vendre, soit sur un site de vente qui lui fera son offre de prix, soit sur une plateforme d'échange qui met en relation des acheteurs et des vendeurs avec un prix uniquement déterminé en fonction de l'offre et la demande. Il reste cependant à comprendre le mécanisme de création de ce bitcoin qui a été acheté en vue de le garder ou le revendre.

2 CRÉER DES BITCOINS

En effet, pour créer et gérer les bitcoins, le système Bitcoin s'appuie sur un logiciel qui génère des bitcoins selon un protocole permettant de rémunérer les agents qui ont pris en charge les transactions.
Ces agents, grâce à leur puissance de calcul informatique, vérifient, sécurisent et inscrivent les transactions dans un registre virtuel, appelé « chaîne de blocs ». Alors que les autorités

monétaires partout dans le monde créent de la monnaie à leur guise et ne s'en privent guère, comment se crée un bitcoin ?

En pratique, cette création de bitcoins s'effectue de plus en plus difficilement : l'entité de base du système Bitcoin s'appelle un bloc. Les blocs sont reliés en une chaîne, d'où le nom de « chaîne de blocs ». Pour chaque nouveau bloc accepté, l'activité de vérification-sécurisation-enregistrement, appelée *minage*, est actuellement rémunérée par la mise à disposition pour le « mineur » de 12,5 bitcoins, soit actuellement prés de 200000$, auquel s'ajoute la rémunération des frais des transactions traités.

On imagine aisément que la concurrence est rude entre les mineurs ou le plus souvent entre des coopératives de mineurs qui unissent leurs efforts pour résoudre les problèmes qui leur sont proposés.

Que calculent les mineurs? Ils effectuent ce que les informaticiens appellent des « *hashs* cryptographiques » sur un « entête de bloc ». Un bloc est en effet composé d'un en-tête contenant les informations nécessaires à l'assemblage de la chaine de blocs, d'une taille fixe de 80 octets. Quant au *hash*, il désigne un moyen de replier un espace de données pour le faire entrer dans la mémoire de l'ordinateur. Lorsque ce hachage est à sens unique, c'est à dire lorsque le calcul de la fonction qui a permis de « caser » les données dans l'ordinateur est facile mais que le calcul de la fonction inverse, depuis les données «pliées » jusqu'aux données d'origine est impossible, on se réfère à un « hachage cryptographique ».

Cette fonction de hachage cryptographique permet, une fois les données pliées, de ne plus pouvoir les déplier, ce qui évite les erreurs et les manipulations par des acteurs malveillants.

Dans le système Bitcoin, le « mineur » est chargé de créer un bloc valide. Mais ce n'est pas facile à créer, car dés le début, pour éviter la création d'énormes blocs contenant de fausses transactions qui gonfleraient la chaîne de blocs que tout les participants doivent conserver à perpétuité, Satoshi Nakamoto avait fixé une limite de 1 Mo pour chaque bloc nouvellement créé. Le nombre de transactions croissant rapidement, la limite de 1Mo pour chaque bloc s'est révélée insuffisante et elle est passée à 2Mo depuis le 1er août 2017. Quoi qu'il en soit, 1Mo ou 2Mo, le problème pour un mineur est de proposer une nouvelle liste de chiffres et lettres qui ne puissent pas être retrouvés par le calcul et qui ne dépasse pas désormais 2Mo.

Pour chaque nouveau hash, le logiciel de minage utilise un nombre aléatoire différent que l'on appelle le *nonce*. Le contenu du bloc et la valeur du *nonce* déterminent le *hash* qui prend la forme d'une longue série de chiffres et de lettres. Pour éviter que trop de *hashs* ne soient proposés, alors que de toute façon le système Bitcoin est conçu pour qu'un seul hash en moyenne soit retenu toutes les dix minutes, une double difficulté est proposée aux mineurs :

- D'une part le hash proposé par un mineur doit être inférieur à une série de nombres donnés, appelée *difficulté cible.*
- D'autre part cette difficulté cible est modifiée toutes les deux semaines, période pendant laquelle le système Bitcoin permet la création de 2016 blocs.

En résumé, la quantité de bitcoins produite est automatiquement limitée par le système Bitcoin à un bloc toutes les dix minutes, qui a prévu de plafonner le nombre total de blocs du système Bitcoin à 21 millions vers l'année 2140. Cette limitation fait que la valeur des bitcoins augmente tant que les opérateurs économiques lui accordent une valeur d'échange et cette augmentation provoque l'accroissement de l'activité de minage, de plus en plus rentable mais aussi de plus en plus lourde en calculs et c'est cette activité de minage qui assure la fiabilité et le contrôle du système Bitcoin.

Une boucle est créé, qui fait que les mineurs travaillent à la fois pour eux et pour le système Bitcoin, ce dernier ayant aussi prévu de compenser une éventuelle baisse de la rentabilité du

minage par une augmentation progressive de la rémunération des mineurs au travers de frais de transaction croissants. Ce processus de création nous conduit à analyser le fonctionnement du système bitcoin.

3 LE SYSTÈME BITCOIN

Le problème crucial du système Bitcoin est celui de la confiance dans son fonctionnement. Il le résout en s'appuyant sur les mineurs.
À l'origine, le système Bitcoin est un projet de logiciel libre et open source, publié sous la licence MIT (*Massachussetts Institute of Technology*), une licence particuliérement ouverte puisqu'elle donne à toute personne un droit illimité d'utilisation et de modification. Le système fonctionne sans autorité centrale grâce au consensus de l'ensemble des « nœuds » du réseau. Ces nœuds sont les clients Bitcoin accessibles depuis l'extérieur ; ce sont eux qui vérifient les transactions et qui, si elles sont valides, les ajoutent au pool de transactions et de les rediffusent.
Une transaction en bitcoins se réalise en deux étapes:

- dans un premier temps, des nœuds du réseau (les mineurs) créent un nouveau bloc en regroupant des transactions récemment effectuées et en leur adjoignant un en-tête contenant notamment la date et l'heure, une somme de contrôle (*hash*) qui servira également d'identificateur unique du bloc et l'identificateur du bloc précédent.
- Dans un second temps, après avoir vérifié la validité de toutes les transactions que ce nouveau bloc contient et leur cohérence avec les transactions déjà enregistrées, chaque mineur l'ajoute à sa version locale du registre, appelée chaîne de blocs.

L'historique complet de toutes les transactions peut être lu en consultant tous les noeuds du réseau qui gèrent la chaîne de blocs. La recopie de ces transactions peut faire apparaître des différences entre fichiers. Dans ce cas, pour que la chaine de blocs soit acceptée, il faut que ces différences soient analysées et corrigées par le logiciel d'accès,
Lorsqu'elles ont été validées, ces données sont non modifiables ad vitam aeternam. Aussi, avant d'inscrire définitivement une transaction dans la chaîne de blocs, le réseau effectue t-il un ensemble de vérifications à plusieurs reprises. Toute transaction est prise en compte instantanément par le réseau et confirmée une première fois au bout de 10 minutes environ ; ensuite chaque nouvelle confirmation renforce la validité de la transaction dans le registre des transactions tenue par les nœuds, qui sont aujourd'hui un peu moins de dix mille.
Il n'existe cependant pas de garantie absolue que le système Bitcoin soit non décryptable, ce qui signifie que de « faux » bitcoins finiront par circuler mais cela ne détruit pas plus le système Bitcoin que les faux billets ne détruisent l'euro ou le dollar.
En résumé, les caractéristiques du Bitcoin sont les suivantes :

- ses fonctionnalités sont mises en oeuvre par des logiciels mis à disposition sous la forme de logiciel libre.
- L'utilisateur choisit son rôle dans le système, client ou « mineur », ainsi que les logiciels qu'il utilise.
- L'autorité de confiance du système n'est pas centralisée mais répartie entre les ordinateurs qui sont compétents pour la construction et l'entretien de la chaîne de blocs.

C'est donc un système qui est à l'opposé de l'organisation d'une Banque centrale, qui décide de l'émission de monnaie en se fondant sur des calculs économiques et financiers.
Aujourd'hui, le système Bitcoin est encore marginal au sein du système financier mondial puisque sa capitalisation ne dépasse guère 200 milliards de dollars début décembre 2017, encore qu'elle varie fortement tous les jours, soit un peu plus de 2% de la capitalisation boursière

mondiale de novembre 2017. Il s'y ajoute cependant la capitalisation des crypto-monnaies concurrentes, comme Bitcoin XT, Bitcoin Unlimited, Bitcoin Classic, Bitcoin Cash et Bitcoin Gold. On peut donc penser que le système Bitcoin pourrait s'emparer assez vite d'une part significative des capitaux mondiaux et c'est pourquoi l'on s'y intéresse.
Il est donc nécessaire de chercher à évaluer la valeur du bitcoin.

4 LA VALEUR DU BITCOIN

La croissance vertigineuse de la valeur du bitcoin, quelques centimes d'euros le 7 février 2011 lors de son lancement, alors qu'il affichait un cours de 18948,41 $ euros le 19 décembre 2017, avant de baisser brutalement en quelques heures, frappe l'imagination du grand public.
La première question qui se pose donc est la question de la stabilité de sa valeur. Pa rapport aux monnaies actuellement en circulation, va t-il croitre sans cesse ou croitre avec de fortes variations ou encore s'effondrer et disparaître ?
Il est certain que le Bitcoin ne repose sur aucune garantie tangible. Mais il s'agit d'un problème inhérent aux monnaies fiduciaires : notre boulanger accepte les Euros parce que lui-même sait (ou pense) que ses employés et ses fournisseurs l'acceptent et parce que ces derniers nous sont imposés par notre État. Mais une panique, bancaire qui ébranlerait le système est toujours possible. Au total, l'Euro n'a pas de valeur en soi, il n'a que la valeur que nous lui accordons, de gré ou de force.
La valeur du Bitcoin est celle que lui accordent les participants au système Bitcoin, qui sont au nombre de deux cent cinquante mille personnes environ dans le monde. Leur nombre s'accroit rapidement ainsi que celui des commerces qui l'acceptent en paiement, malgré des frais de transactions de l'ordre de 15 euros et le risque de fluctuation de sa valeur. Plus de cent mille sites internet l'acceptent dans le monde, dont Microsoft, Expedia ou Paypal. Si ces derniers continuent d'acheter et de vendre des bitcoins, la valeur du bitcoin devrait s'accroitre à moyen terme tout simplement parce qu'il va devenir rare, du fait du petit nombre de bitcoins créé par le système Bitcoin.
Mais cette construction peut aussi s'effondrer et disparaître. Il faut se rappeler à cet égard du système de l'Écossais John Law, qui se proposait d'utiliser du papier monnaie à la place des espèces métalliques. Ce système a été mis en place en France sous la Régence de Philippe d'Orléans entre 1716 et 1720 afin d'éponger le dette laissée par Louis XIV et ses guerres sans fin. Créée par Law, la Banque Générale, société par actions sur le modèle de la Banque d'Angleterre, suscitera la spéculation puis la panique, lorsque la confiance disparut, faisant effondrer le système. Mais par la suite, le papier monnaie s'est généralisé.
Est ce que le système Bitcoin n'est pas du même acabit, un premier essai condamné à disparaître avant de renaitre sous une autre forme ?
La menace qui plane sur le système Bitcoin réside dans la conjonction puissante des intérêts qu'il bouscule, à savoir ceux des banques privées et des autorités monétaires. Parmi ses détracteurs, on trouve le gouverneur de la Banque de France, François Villeroy de Galhau, qui estime que le bitcoin ne présente aucunes des caractéristiques d'une monnaie et Jamie Dimon, le PDG de JP Morgan Chase qui s'y connaît pourtant en spéculation, mais qui qualifie le bitcoin d'escroquerie, juste bonne pour la Corée du Nord.
En tout état de cause, On peut penser que, directement par une série d'interdictions ou indirectement par des mouvements spéculatifs orientés, le système Bitcoin ne finisse par s'effondrer sous les coups. On peut donc s'interroger sur la logique elle-même du système Bitcoin qui pourrait le condamner à la disparition ?

5 LA LOGIQUE DU BITCOIN

Le système Bitcoin est à l'opposé du système bancaire actuel des réserves fractionnaires, qui permet aux banques d'étendre leur offre de crédit au-delà de leurs réserves réelles tout en offrant aux déposants de retirer les fonds issus de leurs comptes courants à tout moment : c'est ainsi que les banques privées créent sans cesse de la monnaie, générant une inflation qui est fonction des politiques menées par la banque centrale dont elles dépendent.
À l'inverse, le bitcoin est plutôt générateur de déflation, puisque la quantité maximale de bitcoins susceptibles d'être créés est fixée à l'avance et que les bitcoins perdus par leurs propriétaires ne seront jamais remplacés. De ce fait, il s'apparente à l'étalon or, d'autant plus qu'il met fin au monopole des banques centrales pour l'émission de monnaie et qu'il n'est pas conçu pour s'adapter à la production de richesse.
C'est pourquoi le projet Bitcoin est une expérience originale qui applique en partie les thèses monétaires de l'école autrichienne d'économie et en particulier celles de Friedrich Hayek. Plus précisément il possède les caractéristiques suivantes :

- contrairement aux devises monétaires, Bitcoin n'est pas l'incarnation de l'autorité d'un État, d'une banque ou d'une entreprise. La valeur du bitcoin est déterminée de façon entièrement flottante par l'usage économique qui en est fait et par le marché des changes.
- Les règles organisant l'émission monétaire sont déterminées uniquement par le code informatique du logiciel Bitcoin.
- En tant que système de paiement, le fonctionnement du système Bitcoin ne requiert pas l'utilisation d'une infrastructure centralisée qui tienne la comptabilité des montants détenus. La garantie du système est fournie par la vérification, toutes les dix minutes environ, de la chaîne de blocs par un ordinateur du réseau choisi de façon aléatoire en fonction de sa puissance. Le système Bitcoin repose en effet sur un protocole cryptographique qui permet d'interdire la falsification des identifiants des parties prenantes.

À l'avenir, il est bien possible que les principes d'une monnaie cryptographique, tel qu'est le système Bitcoin, soient détournés par les Banques Centrales. Il serait alors dépossédé de son indépendance, déjà menacée par la perte de neutralité d'Internet aux Etats-Unis. Ainsi la Banque d'Angleterre aurait annoncé son intention d'introduire une crypto-monnaie nationale; elle a créé à cet effet un groupe de travail dès 2015 pour étudier les moyens d'introduire une crypto-monnaie liée à la livre sterling. Des négociations auraient été conduites avec d'autres banques centrales afin d'introduire une monnaie virtuelle qui utiliserait la technologie de la chaîne de blocs. Il semblerait aussi qu'Israël et la Suède considéreraient la possibilité d'introduire des crypto-monnaies nationales.
C'est ainsi que la logique d'un système monétaire cryptographique pourrait être captée par les Banques Centrales, encore que la disparition de la garantie de la monnaie par ces dernières semble inhérente à ce type de système.
Il reste que le système Bitcoin possède un grave défaut, celui de l'énorme consommation d'énergie électrique qu'il engendre.

6 LE BITCOIN ET L'ÉNERGIE

L'activité de minage, qui assure la création des bitcoins et la gestion du Système bitcoin, a entrainé en 2017 une consommation d'électricité énorme, de l'ordre de 3,7 milliards de kWh par an, soit plus que la consommation de tout l'île d'Irlande.

Dans le système Bitcoin, cette consommation est provoquée par sa politique de minage qui consiste à tirer au sort des ordinateurs pour effectuer le minage qui est réalisé toutes les dix minutes. Or la récompense de 12,5 bitcoins pour créer un bitcoin attire un nombre croissant d'acteurs vers le secteur du minage, car elle devient de plus en plus attractive avec la hausse de la valeur du bitcoin,

À l'avenir, l'optimisation des matériels et les progrès technologiques devraient quelque peu diminuer la consommation électrique, mais on estime que si les crypto-monnaies se généralisaient, la consommation d'énergie pour les gérer pourrait atteindre le double de la consommation électrique actuelle des Etats-Unis, ce qui est une perspective absurde du point de vue écologique.

Fondamentalement, la consommation d'énergie du système Bitcoin provient des opérations complexes de vérification qui sont nécessaires pour protéger le système Bitcoin de la fraude, en l'absence d'autorité centrale. Ces opérations complexes sont inhérentes au système qui propose aux mineurs un problème mathématique de plus en plus complexe afin de limiter le nombre de bitcoins créés et empêcher la fraude. Sans ces calculs complexes, le système Bitcoin serait submergé par les *hackers*.

La nécessaire rémunération des activités de minage a conduit au développement de technologies toujours plus spécialisées, avec des processeurs de plus en plus puissants. Depuis 2015, un mineur qui n'utilise pas un matériel informatique spécialement conçu à cet effet possède fort peu de chances de couvrir ses dépenses d'électricité, même en rejoignant une coopérative de minage.

La chaîne de blocs du système Bitcoin est en effet comparable à un livre public enregistrant les transactions gérées parallèlement par les noeuds du réseau, dont aucun ne joue un rôle privilégié. Ces noeuds du réseau, dont il est impossible de connaître le nombre exact, se comptent vraisemblablement en dizaines de milliers, et c'est leur redondance qui assure la continuité du service.

Mais les opérations sur les blocs sont de plus en plus compliquées en raison de la limite de 1 Mo, imposée originellement par le créateur du système en 2010, pour chaque bloc nouvellement créé toutes les dix minutes sur la chaîne de blocs bitcoin. Cette limite était destinée à empêcher l'attaque du réseau sous forme d'énormes blocs contenant de fausses transactions. Elle consistait en une solution transitoire, en attendant qu'une meilleure solution puisse être mise en place à l'avenir.

Depuis l'origine, cette limite imposée à la taille des blocs est source constante de débats. Quand en 2014, le nombre de transactions a fini par atteindre la limite de taille de bloc, le bassin de transactions en attente s'est saturé et il a fallu limiter ces dernières en introduisant des frais de transaction, de l'ordre de 15$ aujourd'hui, ce qui a rendu le système moins compétitif que Western Union ou Paypal.

Ce débat a fini par produire un consensus qui a consisté à passer à une taille de bloc de 2 Mo à partir de novembre 2017 pour *Bitcoin Core*. Mais la question de son évolutivité reste ouvert : un groupe dissident a augmenté unilatéralement la taille de bloc à 8 Mo pour une nouvelle crypto-monnaie appelé *Bitcoin Cash* auquel se sont ajoutées d'autres monnaies scripturales, *Bitcoin XT* crée en août 2015, *Bitcoin Unlimited* crée en janvier 2016 et *Bitcoin Gold* crée en octobre 2017, mais *Bitcoin Core* reste la seule version officielle soutenue par l'équipe de développement.

Pour toutes ces monnaies, s'applique toujours le principe de la chaine de blocs dont la gestion provoque des dépenses d'énergie considérables. Or, au delà du bitcoin, l'outil de la chaine de blocs est appelée à être utilisé dans tous les cas qui nécessitent une authentification des transactions sur Internet, au travers d'objets connectés en permanence ; ces objets, d'après un rapport de McKinsey, devraient être au nombre de 20 à 30 milliards en usage dans le monde en

2020, alors qu'Internet compte déjà pour 10% de la consommation électrique mondiale.

On peut donc observer que le système Bitcoin, avec son principe de chaines de blocs, soulève de nombreuses questions : éthique avec l'anonymat des opérateurs, économique avec sa valeur spéculative, monétaire avec la question de sa garantie, informatique avec la question de son évolutivité et finalement écologique avec le coût énergétique croissant du minage. Il reste que l'on ne peut plus ignorer que, d'une manière ou d'une autre, les crypto-monnaies ont désormais définitivement émergé, comme dans le passé l'or puis la monnaie fiduciaire sont successivement apparues.