Comment éviter la centralisation de Bitcoin

Nous recensons 19 idées fausses au sujet de la monnaie virtuelle Bitcoin et prédisons ce qui l'attend : minage centralisé, puis gouvernance centralisée.

Établir des quotas nationaux de minage serait peut-être la moins pire des solutions pour éviter la centralisation. Plus généralement, nous introduisons l'idée d'*oligopoles à défiance maximale* comme solution pragmatique aux problèmes de consensus distribué.

READ THE HYPERTEXT VERSION HERE:
http://www.pabr.org/bcendgame/bcendgame.fr.html

Historique des versions		
1.0	2014-09-03	Première publication.
1.1	2014-09-21	Ajout : oligopoles à défiance maximale.
1.2	2014-11-16	Ajout : section sur la "toile de confiance".
1.3	2016-06-17	Ajouts : remarque sur la rareté en tant que convention ; post-scriptum. Ajout : erreur n°19.

Table des matières

1. Introduction

Le contrôle de la monnaie a toujours été un levier d'action puissant pour les gouvernements, au moins depuis l'Empire romain. On peut donc s'étonner que Bitcoin soit toujours là après 5 ans alors que des projets antérieurs de monnaies virtuelles ont été tués dans l'oeuf très rapidement. Le système Bitcoin est-il réellement plus résilient que ses prédécesseurs ? A-t-il vraiment toutes les qualités qu'on lui attribue ? Ou n'est-ce qu'une gigantesque arnaque pyramidale décentralisée et anti-écologique, comme le disent ses détracteurs ?

Quel que soit son avenir, Bitcoin mérite d'être étudié en tant que premier système logiciel combinant une large palette de disciplines :

- la cryptographie, l'art de sécuriser les données et les communications ;
- la théorie systèmes distribués, dont le problème des généraux byzantins et le théorème CAP ;
- l'économie et la théorie des jeux (comment construire des systèmes économiques durables) ;
- la politique (la recherche du consensus).

Cet article suppose que le lecteur connaît les concepts de Bitcoin tels que la *blockchain*, le minage et le problème du monopole à 51 %. Des notions élémentaires d'économie sont également requises.

2. Conventions

"Bitcoin", avec une majuscule, désigne le système dans son ensemble. "bitcoin", sans majuscule, désigne une unité de compte de la monnaie.

Conformément à l'usage dans la communauté Bitcoin, nous parlons non pas de "comptes" mais de "portefeuilles" Bitcoin pour rappeler que contrairement aux comptes bancaires, ils ne sont a priori pas contrôlés par un tiers de confiance.

Conformément aux définitions adoptées par plusieurs institutions bancaires, nous écrivons que Bitcoin est une monnaie virtuelle même si les devises traditionnelles sont aujourd'hui tout aussi virtuelles (dans le sens de "dématérialisées") que Bitcoin.

3. Idées fausses au sujet de Bitcoin

N.B. : Pour avoir une vision d'ensemble plus équilibrée, consulter en complément [BITCOINIT_MYTHS].

3.1. Erreur n°1 : Bitcoin repose sur des techniques cryptographiques révolutionnaires

En réalité, Bitcoin n'utilise que deux concepts cryptographiques très anciens :

- La cryptographie asymétrique : Une clé publique identifie un compartiment ("adresse Bitcoin") d'un portefeuille, et la clé privée correspondante autorise les mouvements depuis ce compartiment.
- Les fonctions de hachage à sens unique, utilisées pour réduire la bande passante, pour protéger les clés publiques, et dans le cadre du système de minage.

Concrètement, les primitives retenues sont ECDSA (2005), SHA256 (2001) et RIPEMD-160 (1996).

D'autres systèmes de monnaie électronique recourent à des concepts plus sophistiqués tels que les signatures aveugles et les preuves à divulgation nulle de connaissance. La raison est souvent que ces autres systèmes privilégient la non traçabilité, alors que Bitcoin se préoccupe avant tout d'éliminer les tiers de confiance.

3.2. Erreur n°2 : Les transactions Bitcoin sont anonymes et non traçables

Bitcoin respecte l'anonymat dans la mesure où n'importe qui peut créer et utiliser un portefeuille sans s'identifier.

Cependant, l'anonymat ne garantit pas la non traçabilité. Au contraire, le mode de fonctionnement de Bitcoin implique que toutes les transactions soient publiques. L'immobilier est vraisemblablement le seul autre type d'actifs qui soit soumis à une telle obligation de transparence.

La communauté Bitcoin recourt à plusieurs techniques pour échapper à cette contrainte :

- Il est fortement déconseillé de publier des adresses Bitcoin, bien que ce soit la démarche naturelle pour recevoir des dons.
- Certains logiciels de gestion de portefeuille s'abstiennent de réutiliser des adresses ou de centraliser les fonds vers une adresse unique, même lorsque cette façon de procéder semble naturelle. Mais cela ne fait que compliquer ou retarder l'analyse des flux.
- Le fait d'utiliser un portefeuille en ligne (géré par un tiers de confiance) apporte un peu de confidentialité. Mais il reste possible de suivre les flux à la trace avec la coopération du fournisseur du service.
- Il existe des tiers de confiance dont la seule activité consiste à "mélanger" (*mix*) les bitcoins d'un grand nombre d'utilisateurs. Il est également question d'implémenter de tels mécanismes de mélange de façon décentralisée.
- Il y a des entreprises apparemment ordinaires dont l'activité est techniquement équivalente à du blanchiment. Par exemple, début 2013, les jeux d'argent représentaient la moitié des transactions Bitcoin et 5 % du volume [http://lsvp.com/2013/08/23/at-least-half-of-all-bitcoin-transactions-are-for-online-gambling/gambling].
- Mentionnons également que révéler la clé privée d'une adresse revient à transférer des bitcoins sans publier la transaction dans la *blockchain*. Ce procédé implique évidemment que le récipiendaire fasse totalement confiance à l'émetteur, sauf peut-être si les clés sont générées et conservées dans un support sécurisé de type carte à puce.

Avec Bitcoin, comme on le devine dans ces exemples, la frontière est ténue entre d'une part, vouloir protéger sa vie privée, et d'autre part, blanchir délibérément de l'argent sale. Pour éviter d'attirer la suspicion, les utilisateurs devraient au minimum s'abstenir de recourir à des prestataires étranger soumis à des réglementations financières trop laxistes. Malheureusement la *blockchain* n'enregistre pas à quel moment l'argent change de propriétaire. Par conséquent, si un utilisateur honnête paie un marchand et si le marchand transmet immédiatement les fonds à un service de blanchiment notoire, l'utilisateur aura du mal à prouver sa bonne foi.

3.3. Erreur n°3 : Les transactions Bitcoin sont instantanées

Il est vrai que n'importe qui peut émettre une transaction Bitcoin en quelques secondes, en choisissant parmi une grande variété de logiciels et de services en ligne de gestion de portefeuille.

Mais les transactions Bitcoin ne sont pas validées instantanément. Techniquement, elles ne sont même jamais vraiment définitives (sauf par effet de bord du *checkpointing* [https://en.bitcoin.it/wiki/Checkpoint_Lockin], dans certaines implémentations). Le système fait seulement en sorte que la probabilité qu'elles soient invalidées décroisse rapidement :

Hors-ligne, en l'espace de quelques secondes . L'émetteur signe une transaction, et le récipiendaire contrôle la validité de la signature. Du point de vue de la sécurité, c'est équivalent à un chèque anonyme.

En ligne, en l'espace de quelques secondes . La transaction est diffusée au réseau Bitcoin. Le récipiendaire obtient un accusé réception d'un ou plusieurs noeuds bénéficiant d'une bonne connectivité avec le reste du réseau Bitcoin. À ce stade le récipiendaire peut raisonnablement considérer que l'émetteur dispose bien des fonds, que le réseau fera son possible pour détecter les tentatives de fraude, et que la transaction a de bonnes chances d'être ajoutée à la *blockchain* quelques minutes plus tard. Notons que le concept de noeuds bien connectés suggère que "tous les noeuds sont égaux, mais certains le sont plus que d'autres". Nous en reparlerons plus loin.

En ligne, sous 10 minutes . Le récipiendaire obtient une première confirmation de la transaction par une preuve de travail (*proof-of-work*) du réseau. Notons que ce délai de plusieurs minutes est incompatible avec de nombreux usages tels que les paiements en magasin, les machines à café, les péages et les distributeurs de billets. Les palliatifs proposés recourent à des transactions hors de la *blockchain* et à des tiers de confiance.

En ligne, après 1 heure . Le récipiendaire a obtenu six confirmations, ce qui est traditionnellement considéré comme suffisant pour la plupart des usages. Nous reviendrons sur la pertinence de ce seuil plus loin.

En ligne, après 17 heures . Le récipiendaire a obtenu 100 confirmations. C'est le délai de maturation que Bitcoin utilise en interne pour valider les bitcoins nouvellement créés.

3.4. Erreur n°4 : Bitcoin est une monnaie

Les économistes caractérisent une monnaie par ses trois fonctions principales :

- **Moyen de paiement .** En l'état (août 2014), Bitcoin n'est pas utilisable hors ligne. Il n'a cours légal nulle part. Aucun gouvernement ne l'accepte en paiement d'impôts ou de taxes. De plus en plus de commerçants l'acceptent, mais seulement par l'intermédiaire de prestataires tiers.

- **Unité de compte .** Du fait de sa grande volatilité, Bitcoin est actuellement peu utile en tant qu'unité de mesure. Les commerçants qui l'acceptent fixent leurs prix en monnaie traditionnelle et affichent les prix en bitcoins à la volée, en appliquant le taux de change proposé par leur prestataire. Une généralisation de l'usage stabiliserait les cours, mais seulement dans une certaine limite, faute d'une autorité centrale pour assurer la liquidité, combattre les spéculateurs et sanctionner les manipulations de type "*pump and dump*" et "*short and distort*". Dans le meilleur des cas, à court terme, les cours resteront influencés par les fluctuations des prix de l'électricité et des semi-conducteurs.

- **Réserve de valeur .** N'ayant aucune valeur intrinsèque et ne présentant aucune garantie de pérennité, les bitcoins ne sont certainement pas un support d'investissement sans risque.

De plus, on attend implicitement d'une monnaie qu'elle soit fongible, ce qui signifie que deux masses de pièces, de billets ou de dépôts bancaires représentant des montants identiques doivent être interchangeables. Or, la traçabilité intrinsèque de Bitcoin implique qu'un bitcoin qui vient d'être miné pourrait valoir davantage qu'un autre qui a transité par un service de blanchiment ou un site de jeux d'argent. Il est envisagé d'ajouter un mécanisme pour mettre des bitcoins sur liste rouge, c'est à dire de les marquer comme étant d'origine douteuse [http://www.coindesk.com/bitcoin-tracking-proposal-divides-bitcoin-community/].

Notons que les devises traditionnelles ne sont pas parfaitement fongibles non plus. Par exemple, fin mars 2013, un euro déposé sur un compte à Chypre valait indubitablement moins qu'un euro conservé n'importe où ailleurs.

3.5. Erreur n°5 : Bitcoin est une devise / Bitcoin est une commodité

Cela relève d'une décision de politique fiscale, avec des conséquences non négligeables pour les acteurs soumis à la TVA. Si Bitcoin est considéré fiscalement comme une devise, alors les commerçant

peuvent l'accepter de la même façon qu'un paiement en devise étrangère. Si c'est une commodité, alors le fisc considérera que les commerçants qui l'acceptent font du troc.

3.6. Erreur n°6 : Bitcoin est forcément une devise puisqu'il a un code ISO comme l'USD et l'EUR

Il est vrai que l'ISO a officiellement attribué à Bitcoin un code à trois lettres, ce qui constitue un pas vers sa légitimation. Notons que le code est non pas BTC mais XBT.

Cependant, la norme ISO 4217 n'est pas limitée aux devises. Elle prévoit aussi des codes pour l'or (XAU) et d'autres commodités.

3.7. Erreur n°7 : En tant que devise et que système de traitement des paiements, Bitcoin a des frais de fonctionnement faibles

On peut estimer le coût de fonctionnement du système Bitcoin sur la base des données ci-dessous, qui datent de mi août 2014.

- Puissance de hachage totale : 200 PH/s
- Récompense du minage : 25 bitcoins toutes les 10 min
- Minage effectué dans sa totalité sur du matériel récent coûtant 0,7 USD par GH/s et consommant 0,77 J/GH
- Le matériel doit être renouvelé tous les 6 mois
- Coût de l'électricité : 0,15 USD/kWh.

Sous ces hypothèses, les coûts d'exploitation de Bitcoin sont d'au moins 250 millions d'USD par an, soit environ 4 % de la masse monétaire.

D'après certaines estimations le volume de transactions quotidien est d'environ 59 million USD ([BLOCKCHAININFO_STATS]). Le coût de fonctionnement s'élève dont à 1,2 %. N.B. : Cette estimation est peut-être très inférieure à la réalité car la *blockchain* ne permet pas de distinguer les opérations purement comptables des transactions commerciales.

Sans chercher à déterminer si Bitcoin est plus ou moins coûteux que les devises et systèmes de paiement traditionnels, il est évident qu'une version centralisée de Bitcoin serait plus efficace.

Ces frais sont indolores pour les utilisateurs car ils sont négligeables par rapport à l'inflation (4 % contre 13 % - voir Section 3.12, « Erreur n°12 : Bitcoin est déflationnaire »). Mais cela ne peut pas continuer éternellement, et fait penser à un système de Ponzi.

Sous les mêmes hypothèses très optimistes, la production d'un nouveau bitcoin coûte 190 USD (matériel : 35 USD, électricité : 154 USD). En tenant compte de la base installée moins performante, des infrastructures et du refroidissement, le coût de production réel est probablement très proche du taux de change de 500 USD. Notons que cela n'a rien de surprenant : Alors que les banques centrales ont le monopole de l'émission de leurs devises, n'importe qui peut se lancer dans le minage et produire des bitcoins. Dans une industrie sans barrières à l'entrée, les cours de marché ne peuvent pas dépasser les coûts de production de façon significative et durable. Le marché des métaux précieux n'est pas très différent puisque le cours de l'or (environ 1300 USD/oz) est proche du coût de son extraction dans les mines (environ 1200 USD/oz).

Est-il souhaitable qu'une monnaie ne vaille pas plus que le coût de production de ses supports symboliques ? C'est un autre débat.

3.8. Erreur n°8 : Bitcoin est un système ouvert et égalitaire

Il est vrai que Bitcoin permet à n'importe qui disposant d'un accès Internet de réaliser des transactions internationales, ce qui constitue une innovation sociétale majeure. Plusieurs milliards d'individus n'ont pas de compte bancaire, mais bon nombre d'entre eux ont un smartphone.

Cependant, le processus de minage favorise ceux qui ont accès à de l'électricité, des semi-conducteurs et des infrastructures bon marché, de préférence sous un climat froid. Il n'y a pas si longtemps, le phénomène des *botnets* de minage était préoccupant, car ils avaient accès à toutes ces ressources gratuitement ; heureusement les ASICs les ont rendus obsolètes. L'activité de minage semble actuellement se concentrer en Chine [http://bitcoinmagazine.com/12914/bitcoins-made-in-china/], vraisemblablement à cause de la proximité des usines de semi-conducteurs et d'un possible subventionnement du coût de l'électricité.

3.9. Erreur n°9 : La hausse récente du taux de change traduit forcément une forte demande pour les bitcoins

Commençons par comprendre comment la valeur de marché des bitcoins est déterminée.

La production de bitcoins est parfois présentée comme un processus industriel, appelé d'ailleurs "minage". Mais cette analogie ne tient pas la route. En effet, le rythme de production des bitcoins a été planifié dès l'origine [https://en.bitcoin.it/wiki/Controlled_supply]. Quelle que soit l'intensité de l'investissement dans le minage, et quoi que fassent les mineurs, le mécanisme d'ajustement de la difficulté les empêchera de produire plus de 25 bitcoins par période de 10 min (en août 2014).

En réalité, l'émission des bitcoins ressemble plutôt à une vente aux enchères. Tous se basse comme si une banque centrale mettait en vente 25 bitcoins par période de 10 min. Chaque mineur estime combien les autres sont prêts à dépenser et décide de suivre ou non. Comme Bitcoin ne veut pas d'une banque centrale, l'argent va à l'industrie de l'énergie et des semi-conducteurs, mais cela ne change rien au mécanisme de détermination des prix.

Malheureusement, il est bien connu que la vente aux enchères de ressources rares conduit souvent à des valorisations surestimées. Par exemple, les enchères pour l'attribution du spectre radio aux opérateurs télécom sont parfois organisées de telle sorte que le plus offrant paie le prix proposé par le deuxième plus offrant, plutôt que le sien. On estime que sans cette précaution les candidats paieraient trop cher et feraient faillite. Dans le cas de Bitcoin la seule chose qui peut empêcher la surenchère est l'offre provenant du marché secondaire, c'est à dire les bitcoins anciens proposés à la vente dans les bureaux de change. En août 2014 la production quotidienne de nouveaux bitcoins correspond à environ 2 millions de USD, et le volume quotidien dans les bureaux de change à environ 3 millions de USD. Il est difficile de dire si ce ratio entre le marché primaire et le marché secondaire suffit à déterminer un prix de marché équitable.

Compte tenu de tout ce qui précède, plusieurs facteurs peuvent expliquer la hausse de la valeur de marché des bitcoins :

- Une réelle demande de la part des utilisateurs et des investisseurs.
- L'anticipation que, dans un contexte de réglementation de Bitcoin par les états, les bitcoins issus du minage vaudront plus que ceux qui ont transités par des adresses douteuses. Ceci expliquerait une divergence entre le marché primaire (le minage) et le marché secondaire (les bureaux de change), et le sur-investissement dans le minage. Notons que de ce point de vue, le *"cloud mining"* pourrait être considéré comme une technique de blanchiment.
- Le progrès technique rapide : Lorsque les cours de marché chutent sous le coût de production moyen, la seule façon pour les mineurs de dégager un bénéfice est d'investir dans du matériel plus performant. Mais à long terme ceci augmente les coûts de production pour tout le monde via le mécanisme d'ajustement de la difficulté.

- Un sur-investissement délibéré de la part des mineurs. Un tel comportement n'est pas économiquement rationnel, sauf si les mineurs espèrent secrètement en tirer un profit qui irait au delà de la vente des bitcoins minés. Dans un marché traditionnel, ceci s'apparenterait à une stratégie de vente à perte pour éliminer la concurrence. Nous reviendrons sur cette hypothèse plus loin.

3.10. Erreur n°10 : Bitcoin n'a pas de frais de transaction

En réalité, le protocole Bitcoin prévoit le versement de commissions : Chaque transaction peut contenir un "pourboire" à verser au mineur qui réussira à l'inclure la transaction dans la *blockchain*. Le réseau exige un pourboire obligatoire (autrement dit, une commission) sur les transactions inhabituelles qui ressemblent à des attaques par *flooding*. Il n'y a pas de frais obligatoires sur les transactions ordinaires, mais les pourboires incitent les mineur à traiter les transactions plus rapidement. D'après certaines estimations, les pourboires représentent environ 0,3 % du volume ([BLOCKCHAININFO_STATS]).

Lorsque la masse monétaire approchera de son plafond, les pourboires deviendront la principale source de financement du minage. En attendant, les mineurs sont rémunérés essentiellement par l'inflation. D'après certaines estimations, les mineurs reçoivent un flux de bitcoins correspondant à environ 4 % du volume des transactions ([BLOCKCHAININFO_STATS]).

3.11. Erreur n°11 : Les bitcoins sont intrinsèquement rares, comme l'or

D'après ses promoteurs, Bitcoin est comparable à l'or physique puisque par construction, le minage ne peut pas produire plus de 21 millions de bitcoins. Cependant :

- Comme certains utilisateurs confient la gestion de leur portefeuille à des tiers de confiance qui gèrent les comptes indépendamment de la *blockchain*, Bitcoin n'est pas totalement immunisé contre le système de réserves fractionnaires décrié par ses partisans, ni l'or-papier d'ailleurs. Cette pratique peut accroître la masse monétaire bien au delà de la base monétaire.

- Ce qui est rare n'est pas nécessairement cher. L'or ne tire pas sa valeur de sa seule rareté, mais aussi des qualités qui le différencient de tous les autres métaux. Les bitcoins sont certes rares, mais il y a déjà une cinquantaine d'autres monnaies virtuelles [http://altcoins.com/] dotées de qualités similaires. Si l'usage des monnaies virtuelles se généralise et si leur valeur de marché réussit à dépasser les coûts d'émission, des taux de change s'établiront entre Bitcoin et ses concurrents en fonction leurs popularités respectives et de leurs qualités techniques. Par exemple, une monnaie virtuelle capable de garantir à la fois l'anonymat et la non traçabilité supplanterait certainement Bitcoin pour certains usages. Inversement, une monnaie virtuelle suffisamment digne de confiance pour qu'au moins un état lui donne cours légal serait adoptée par le grand public plus facilement que Bitcoin.

- La rareté des bitcoins n'est pas gravée dans le marbre, ni dans les lois mathématiques. Ce n'est rien de plus qu'une convention. Si la communauté Bitcoin décide un jour qu'il est dans l'intérêt général d'augmenter la base monétaire, cela pourra être fait facilement. Cela pourrait se produire si Bitcoin devient populaire et si les nouveaux utilisateurs estiment que les premiers arrivés (devenus minoritaires) bénéficient d'un avantage indu. En pratique il suffirait qu'une très large majorité des mineurs adopte une nouvelle version du protocole. Les mineurs y seraient probablement favorables puisque leurs perspectives économiques s'en trouveraient améliorées. Dans le système actuel, la réduction planifiée des récompenses de minage les condamne à disparaître.

3.12. Erreur n°12 : Bitcoin est déflationnaire

En faisant abstraction du système de réserves fractionnaires et de la concurrence des autres monnaies virtuelles, il est vrai que la base monétaire de Bitcoin finira par croître plus lentement que l'économie, puis par décroître au fur et à mesure que des utilisateurs perdent leurs clés privées. Cependant :

- Ceci ne garantit pas que le pouvoir d'achat d'un bitcoin va augmenter. À terme la valeur de Bitcoin en tant que moyen de paiement, qu'unité de compte ou que réserve de valeur sera déterminée par son utilité réelle.

- En août 2014, la base monétaire de Bitcoin croit encore à un rythme de 13 % par an.

3.13. Erreur n°13 : Le réseau Bitcoin est résilient.

En pratique Bitcoin n'est ni plus ni moins résilient que le réseau Internet. Comme toutes les bases de données distribuées et répliquées, il est vulnérable à un partitionnement (ou morcellement) du réseau : Si gouvernement décide d'isoler sa population du reste de l'Internet, alors deux versions de la *blockchain* se développent indépendamment l'une de l'autre, et les attaques par contrefaçon (*double-spending*) deviennent triviales.

Les promoteurs de Bitcoin suggèrent que la cohérence de la *blockchain* pourrait être préservée par divers moyens, y compris en attachant des cartes mémoire à des pigeons voyageurs si nécessaire. Cependant, nous avons vu qu'un fonctionnement en temps réel est indispensable pour détecter rapidement les attaques par contrefaçon et confirmer les transactions sous un délai raisonnable.

À défaut, le protocole Bitcoin restaurera automatiquement la cohérence après un épisode de partitionnement : Lorsque la connectivité est rétablie, seule la branche la plus longue de la *blockchain* survit. Les transactions confirmées sur la branche isolée sont invalidées et doivent être soumises à nouveau au réseau. Elles finiront par être enregistrées, sous réserve qu'une attaque par contrefaçon n'ait pas été perpétrée dans l'intervalle.

Dans le mondes des bases de données, on résout parfois le problème du partitionnement à l'aide de mécanismes d'arrêt automatique : Dès qu'un noeud soupçonne qu'un autre est défaillant ou injoignable, il le met hors service, par exemple en coupant son alimentation électrique. Si le mécanisme est suffisamment rapide, la probabilité de destruction mutuelle est faible. Cette approche est adoptés lorsque la cohérence des données est plus importante que la disponibilité du service. Le comportement de Bitcoin en cas de partitionnement s'en approche : Comme le fragment isolé du réseau voit sa puissance de calcul chuter brutalement, les délais de confirmation vont s'y allonger et les transactions vont s'exécuter au ralenti.

Ainsi, les utilisateurs soumis à un régime dictatorial, qui sont ceux qui ont le plus besoin d'une monnaie alternative fiable, sont ceux qui souffriraient le plus d'une attaque contre Bitcoin ciblant le réseau.

3.14. Erreur n°14 : La compétition entre les mineurs garantit la sécurité de Bitcoin

C'est l'hypothèse fondatrice de Bitcoin en tant que système décentralisé sans tiers de confiance. À l'origine le réseau Bitcoin était constitué d'ordinateurs personnels faisant la course au minage pendant leur temps libre. Mais les mineurs ont rapidement compris qu'ils pouvaient augmenter leur retour sur investissement en se rassemblant en coopératives (*pools*). Cette pratique s'éloigne du modèle sans tiers de confiance car les membres d'un *pool* doivent se faire confiance entre eux et faire confiance à leur leader.

Mi août 2014, le plus grand *pool* contrôlait 29 % de la puissance de calcul, deux *pools* contrôlaient 51 %, et les sept plus grands *pools* contrôlaient 75 % ([BLOCKCHAININFO_POOLS]). Notons que ces chiffres sont tirés de déclarations spontanées. Il est difficile de détecter d'éventuelles collusions secrètes entre des *pools*.

Revenons sur le seuil de six confirmations (soit 1 h) traditionnellement considéré comme suffisant pour déclarer une transaction irrévocable. Ce seuil garantissait un risque de fraude inférieur à 0,1 % sous l'hypothèse historique qu'aucun noeud ne contrôlerait jamais plus de 10 % de la puissance de calcul. Maintenant qu'un *pool* contrôle 30 %, le risque de fraude avec six confirmations est passé de 0,1 % à

18 %. Pour ramener le risque à 0,1 %, il faudrait attendre 25 confirmations, soit 4 h (source : [BITCOIN], page 8).

3.15. Erreur n°15 : Une attaque par contrefaçon ne peut pas être rentable

Il est vrai qu'un attaque massive par contrefaçon exigerait une puissance de calcul considérable. Une telle attaque ébranlerait la crédibilité de Bitcoin et réduirait donc la valeur marchande du butin et de l'investissement en matériel. Cependant :

- Des organisations diverses pourraient espérer tirer profit de la destruction de Bitcoin. C'est une question d'analyse de rentabilité.
- L'investissement en matériel ne serait pas déprécié par l'attaque s'il pouvait être réutilisé dans le cadre d'une autre monnaie virtuelle utilisant la même fonction de hachage.

3.16. Erreur n°16 : La sécurité de Bitcoin ne dépend pas de tiers de confiance

En oubliant le problème des mineurs en situation de monopole, on peut en effet dire que Bitcoin ne fait à aucun moment intervenir des tiers de confiance. Bitcoin est vraisemblablement la première monnaie virtuelle dotée de cette propriété.

Cependant, tout ceci suppose que le protocole et les règles du minage sont fixées pour l'éternité. Or Bitcoin continue à évoluer, et certaines règles ne peuvent être changées qu'à l'unanimité. En pratique les décisions sont prises informellement par une communauté d'intervenants aux intérêts parfois contradictoires :

- **Les mineurs .** On pourrait penser qu'ils sont attachés à Bitcoin pour le long terme à cause de leurs investissements en infrastructure, mais n'oublions pas que leur matériel devient obsolète en 6 mois. Néanmoins, les mineurs s'opposeraient vraisemblablement à toute modification du protocole qui rendrait instantanément leurs ASICs obsolètes.
- **Les bureaux de change .** En tant qu'entreprises s'adressant aux utilisateurs finaux, avec des investissements marketing importants, ils sont probablement attachés Bitcoin à plus long terme que les mineurs. Les bureaux de change interagissent avec le système bancaire traditionnel et avec les régulateurs financiers. Par exemple, les bureaux de change installés aux États-Unis sont indubitablement des *money service businesses*. S'il fallait choisir entre la protection de la vie privée et le respect de la réglementation financière, les grands bureaux de change choisiraient certainement la voie réglementaire. La plupart des bureaux de change enregistrent d'ores et déjà l'identité de leurs utilisateurs. Certains vont jusqu'à refuser de traiter des bitcoins provenant de services peu recommandables tels que les jeux d'argent non autorisés.
- **Les développeurs .** Il existe une implémentation de référence pour le protocole Bitcoin, gérée par une petite équipe de développeurs auxquels les utilisateurs font confiance pour corriger tous les problèmes. En août 2010 [https://en.bitcoin.it/wiki/Incidents#CVE-2010-5139] et en mars 2013 [https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki], des *bugs* logiciels ont provoqué des duplications de la *blockchain*, et ce sont les développeurs qui ont désigné la *blockchain* canonique. Notons que ceci a eu pour effet d'invalider rétroactivement les transactions enregistrées sur les autres versions de la *blockchain*.
- **Les commerçants (y compris les travailleurs rémunérés en bitcoins) .** À long terme ce sont eux qui détermineront l'utilité, et donc la valeur marchande, des bitcoins. Mais la plupart des commerçants ne sont pas réellement attachés à Bitcoin pour le long terme. Ils se satisfont de recevoir les paiements en devises traditionnelles par l'intermédiaire de tiers de confiance qui gèrent les détails techniques des transactions Bitcoin, tant que les commissions sont inférieures à celles des paiements par carte de crédit.

3.17. Erreur n°17 : Les mineurs, agissant dans leur intérêt propre, empêcheront collectivement l'apparition d'un monopole à 51 %

La théorie classique postule qu'un agent économique disposant de ressources de minage fera un choix rationnel entre les deux options suivantes :

- Rejoindre le plus grand *pool*, et accepter ainsi la responsabilité de pousser un peu plus le système vers un scénario catastrophique de monopole à 51 %.
- Rejoindre un *pool* plus petit, et subir immédiatement un retour sur investissement plus faible.

Le choix optimal dépend du coût subjectif du scénario de monopole à 51 %. L'histoire suggère que les marchés s'en préoccupent peu, sinon les taux de change se seraient effondrés en janvier 2014 lorsqu'un *pool* bien connu s'est approché du seuil fatidique, et à nouveau en juin 2014 lorsqu'il a récidivé malgré ses promesses antérieures [https://bitcoinfoundation.org/2014/06/centralized-mining/].

Voir aussi : dilution de la responsabilité et tragédie des biens communs.

3.18. Erreur n°18 : Bitcoin a atteint une masse critique, il ne peut plus disparaître

D'après les chiffres de la Section 3.7, « Erreur n°7 : En tant que devise et que système de traitement des paiements, Bitcoin a des frais de fonctionnement faibles », pour doubler la puissance de calcul (et contrôler ainsi la moitié du total) il suffit d'investir 140 millions d'USD en matériel et de dépenser 554 000 USD par jour de fonctionnement. Le coût d'une telle attaque sera réduit si l'organisateur réussit simultanément à éjecter quelques gros *pools* du réseau, par exemple au moyen d'un déni de service, ou en sabotant leur alimentation électrique, ou simplement à l'aide d'une ordonnance légale.

L'organisateur pourrait alors s'approprier 100 % des bitcoins nouvellement créés, soit 25 par période de 10 min (août 2014). Si les taux de change restent stables, l'attaque serait rentabilisée en quatre mois.

Ces montants seraient très abordables pour une coalition de banques ou de gouvernements désireux de saper la crédibilité de Bitcoin. Les paris coûteux ne sont pas rares dans le monde de la finance.

3.19. Erreur n°19 : Même si Bitcoin disparaît, la "technologie des *blockchains*" survivra.

À chaque fois que Bitcoin perd en popularité, ses défenseurs détournent le discours vers la "technologie des *blockchains*". Il est vrai que des services de notarisation mondiaux, décentralisés, dignes de confiance et peu coûteux seraient utiles, notamment dans les régions politiquement instables. Et tant que la *blockchain* de Bitcoin existera, des services parasites pourront y enregistrer tous types de transactions non financières presque gratuitement.

Malheureusement, une *blockchain* ne peut pas être à la fois digne de confiance et peu coûteuse. Si les mineurs de Bitcoin dépensent 250 millions d'USD par an (estimation en août 2014), c'est uniquement parce que cela leur rapporte davantage sous la forme de bitcoins nouvellement créés. Une *blockchain* dédiée par exemple à la notarisation de transactions immobilières ne pourrait pas récompenser ses mineurs de la même façon.

Par ailleurs, un service de notarisation n'a aucun intérêt sans un mécanisme coercitif associé. La *blockchain* de Bitcoin est son propre mécanisme coercitif, puisque les bitcoins n'ont aucune existence en dehors d'elle. Mais comment une *blockchain* pourrait-elle traiter des litiges relatifs à une transaction immobilière ? Et qui déciderait quelle *blockchain* a le dernier mot pour chaque type de transaction ?

4. Comment l'email est devenu centralisé

Bitcoin ambitionne de remplacer les devises traditionnelles d'une façon qui rappelle le bouleversement du courrier postal par l'email.

SMTP, le protocole qui définit l'email tel que nous le connaissons aujourd'hui, fonctionne de façon décentralisée et point-à-point : N'importe qui peut publier des lignes MX dans le DNS de sorte que son courrier soit acheminé directement jusqu'à sa station de travail personnelle. C'était pratique courante à la fin des année 1980.

Mais l'administration d'un serveur exposé à Internet est une corvée peu gratifiante. C'est pourquoi les services informatiques des universités et des grandes entreprises ont fini par prendre en charge l'email de leurs milliers d'utilisateurs. Puis vers la fin des années 1990 le grand public a découvert Internet et les FAI ont commencé à gérer plusieurs millions de comptes email chacun. Avançons jusqu'en 2014 : Gmail a 500 millions d'utilisateurs, Outlook.com (Hotmail) en a plus de 400 millions, et Yahoo Mail en a quelques centaines de millions également.

Ceci montre que la plupart des utilisateurs acceptent beaucoup de sacrifices en échange d'un service gratuit et facile à utiliser.

5. Comment la cryptographie asymétrique est devenue centralisée

Lors de sa (re)découverte en 1977, la cryptographie asymétrique fût présentée comme une révolution qui allait permettre aux individus de communiquer en toute sécurité sans dépendre de clés secrètes fournies par un tiers de confiance.

Presque 40 ans plus tard, le modèle décentralisé dit "toile de confiance" de PGP n'a toujours pas été adopté par le grand public, et tous les systèmes d'exploitation font confiance à quelques centaines d'autorités de certification dont certaines, pour des raisons diverses, ont failli à leur rôle en émettant de faux certificats pour des domaines Internet tels que google.com, yahoo.com et microsoft.com.

Ceci montre, une fois encore, que la plupart des utilisateurs ne sont pas disposés à s'impliquer activement dans la gestion de problématiques de sécurité.

6. L'avenir de Bitcoin

6.1. Première étape : Centralisation du minage

Nous avons vu que d'un point de vue économique, un mineur n'a aucun intérêt à rester sous le seuil de 51 %. La centralisation est quasiment déjà réalisée : il ne manque plus qu'une poignée de main en coulisses entre les leaders de quelques gros *pools*. Des émissaires de l'industrie du minage "représentant 30 % de la puissance de hachage mondiale" se rencontreraient déjà dans des réunions privées [http://www.coindesk.com/private-china-meeting-bitcoin-mining-industry-leaders/].

Les promoteurs libertariens de Bitcoin devraient se réjouir que ce parfait exemple de capitalisme non régulé engendre un monopole naturel en seulement quelques années.

Que se passera-t-il lorsqu'un *pool* revendiquera ouvertement son statut de monopole ?

- Bitcoin ne disparaîtra pas du jour au lendemain. Le monopole n'abusera pas immédiatement de son pouvoir. Il se contentera de faire vivre l'écosystème Bitcoin comme un dictateur éclairé, recevant 100 % des nouveaux bitcoins. La plupart des utilisateurs de s'apercevront de rien.
- Le monopole sera même en mesure d'améliorer la qualité du service, par exemple en confirmant les transactions sans délai et en garantissant la détection des tentatives de contrefaçon.

D'un autre côté :

- Bitcoin ne pourra plus prétendre être un système décentralisé et sans tiers de confiance. Ceci rebutera les utilisateurs, maintenant très minoritaires, qui l'avaient adopté pour des raisons idéologiques.
- Le monopole constituera un point de défaillance centralisé. Même s'il souhaite pérenniser le système, divers acteurs pourront le contraindre à agir contre son intérêt, ou le convaincre de céder le contrôle en empochant un beau bénéfice.
- À ce stade le système *proof-of-work* n'aura plus vraiment d'utilité. Néanmoins, pour protéger son statut, le monopole devra continuer à investir dans du matériel et à gaspiller de l'électricité. Le monopole finira donc par proposer des modifications à apporter au protocole, avec pour effet d'entériner définitivement son rôle d'autorité centrale.

À plus long terme, au fur et à mesure que le minage devient moins rentable, le monopole essaiera de profiter de sa situation de diverses façons :

- Les utilisateurs constateront que leurs transactions s'exécutent plus rapidement lorsqu'ils proposent un pourboire plus élevé.
- Le monopole pourra également offrir des accès prioritaires, des accords d'interconnexion et d'autres services à valeur ajoutée aux grands acteurs de l'écosystème Bitcoin.
- Ou encore, le monopole changera les règles, par exemple en relevant le plafond de la masse monétaire au delà de 21 millions.

6.2. Seconde étape : Centralisation de la gouvernance

Les utilisateurs finiront par s'apercevoir que Bitcoin ne tient plus ses promesses. Ceci arrivera rapidement si le mineur en situation de monopole est amené à prendre des décisions sur des sujets controversés tels que :

- choix entre anonymat et respect des réglementations financières ;
- gestion d'une liste noire des bitcoins volés ;
- permettre ou non le remboursement des bitcoins volés ou perdus (après leur mise sur liste noire) ;
- autoriser ou non les jeux d'argent et les services de blanchiment ;
- définition d'un délai de prescription pour les bitcoins qui ont transité par une adresse douteuse ;
- comment traiter les ordonnances légales, telles que les saisies d'actifs en bitcoins.

À ce stade la communauté des utilisateurs voudra que quelqu'un prenne les choses en main. La fondation Bitcoin [https://bitcoinfoundation.org] sera un candidat naturel, mais une coalition de bureaux de change aurait peut-être encore plus de poids face au mineur en situation de monopole. Plusieurs solutions seront envisagées :

- *Checkpointing* périodique de la *blockchain*. Malheureusement le *checkpointing* décentralisé est une forme de consensus distribué, c'est à dire le problème que la *blockchain* était censée résoudre. Cette approche exigerait donc probablement une forme de centralisation.
- Interdire aux mineurs de dépasser une certaine fraction de la puissance de calcul (par exemple 10 %). Ceci impliquerait qu'une autorité centrale les mette sous tutelle, afin d'éviter les collusions en coulisses.
- Rendre le système de consensus de la *blockchain* plus démocratique, par exemple "une voix par personne physique" au lieu de "une voix par gigahash/s". Ceci impliquerait un registre des utilisateurs, donc la fin de l'anonymat.

- Adopter une fonction de hachage moins favorable aux ASICs afin de revenir au concept initial "un vote par ordinateur". Ceci favoriserait toujours les mineurs disposant d'électricité bon marché, et encouragerait le retour des *botnets*.

- Abandonner le mécanisme *proof-of-work* pour son concurrent, *proof-of-stake*. Ceci pourrait encourager les utilisateurs à mettre leurs avoirs en commun dans des banques.

- Choisir périodiquement de nouveaux mineurs au hasard, comme dans la stochocratie. Mais ceux-ci pourraient être tentés de vendre leur privilège au plus offrant.

Voir aussi : Prohibited changes [https://en.bitcoin.it/wiki/Prohibited_changes], Hardfork Wishlist [https://en.bitcoin.it/wiki/Hardfork_Wishlist].

La plupart de ces solutions diviseraient profondément la communauté Bitcoin. Et le simple fait de devoir prendre des mesures si drastiques ébranlerait la crédibilité de Bitcoin et des monnaies virtuelles en général. C'est pourquoi l'issue la plus vraisemblable est qu'il ne se passera rien de tout cela. Le contrôle de Bitcoin restera partagé entre le monopole de minage et l'autorité de gouvernance, chacun ayant le pouvoir de détruire le système si l'autre abuse de ses pouvoirs. Trois des développeurs principaux ont d'ailleurs déjà la possibilité d'envoyer des messages d'urgence à tous les utilisateurs [https://en.bitcoin.it/wiki/Alerts].

L'autorité de gouvernance définira la politique, le montant des commissions, les conditions d'utilisations. Le monopole de minage assurera l'intendance. Les gouvernements n'auront aucun mal à leur faire respecter leurs réglementations financières.

On peut espérer que tous les acteurs se mettront d'accord pour abandonner le système *proof-of-work* coûteux et devenu inutile.

À ce stade le réseau Bitcoin commencera à ressembler à l'écosystème VISA/MasterCard, mais avec davantage de flexibilité et des conditions d'accès moins contraignantes. Notons qu'avec des mesures techniques de sécurité appropriées (carte à puce) et une régulation antitrust efficace, le coût de fonctionnement d'un système de paiement international par carte de crédit peut dès aujourd'hui être réduit à 0,3 % [http://www.europarl.europa.eu/news/en/news-room/content/20140219IPR36454/html/MEPs-back-cap-on-card-payment-fees]. Bitcoin et les autres monnaies virtuelles devront faire mieux pour survivre.

6.3. Long terme

La centralisation provoquera-t-elle la mort de Bitcoin ? Probablement pas. Internet a réellement besoin d'un système de paiement adapté aux nouveaux usages (*programmable money*). Pour de nombreuses applications, les utilisateurs acceptent de renoncer aux droits de recours attachés aux cartes de crédit, en échange d'une simplicité d'utilisation accrue et de coûts réduits.

Bitcoin, affaibli par la centralisation, sera-t-il remplacé par une autre monnaie virtuelle ? Pas forcément. Au fur et à mesure que la réglementation éloignera Bitcoin de l'économie souterraine, d'autres monnaies virtuelles s'approprieront ce marché. Mais pour les applications grand public, même si Bitcoin est loin d'être parfait, il a prouvé son utilité et il bénéficie de la prime au premier entrant sur un marché où l'effet de réseau est puissant. Les micropaiements et les transactions hors ligne seront gérés par des tiers de confiance, dont le pouvoir restera limité tant que le coeur du système restera autonome (du moins en théorie).

7. Solutions pour éviter la centralisation

7.1. Quotas de minage

Est-il possible d'éviter la centralisation ? Pas sans renoncer à au moins une des propriétés fondamentale de Bitcoin.

Dans cette section nous suggérons que l'introduction de quotas de minage est peut-être la moins mauvaise des solutions.

Des quotas pourraient par exemple être attribués pays par pays sur la base du PIB ou d'un critère reflétant l'influence politique (les détails sont laissés à l'imagination du lecteur).

L'idée de quotas n'est pas aussi incompatible avec l'esprit de Bitcoin qu'on pourrait le penser. Après tout, il y a déjà des quotas de production au coeur de Bitcoin : pas plus de 25 bitcoins par 10 min (en août 2014). Le but n'est pas de contrôler qui est autorisé à faire tourner des ASICs, mais de décentraliser le contrôle sur les critères d'ajout des transactions à la *blockchain*. Il ne serait pas gênant que tous les pays choisissent de délocaliser le travail de hachage en Chine ou en Islande, à condition qu'ils préparent leurs blocs eux-mêmes et indépendamment les uns des autres.

Pourquoi attribuer des quotas aux nations plutôt que, par exemple, aux individus ou aux entreprises ? Parce que les nations sont naturellement en compétition, et la défiance mutuelle est exactement ce qu'il faut pour éviter la centralisation. Chaque nation organiserait sa part du travail de minage et ferait usage des bitcoins minés à sa façon ; ainsi une grande variété de tendances politiques et de modèles de société seraient représentés. Si toutes les nations venaient à s'unir sous l'autorité d'un gouvernement mondial avec une réglementation financière commune, le sort de Bitcoin serait le dernier des soucis de ses partisans.

Le DNS est également décentralisé en domaines de premier niveau nationaux (plus quelques domaines transnationaux) qui ont chacun leur propre politique d'attribution des noms. Ceci élargit la liberté de choix des utilisateurs.

7.1.1. Avantages d'un système de quotas

- Des quotas résoudraient le problème du monopole à 51 % qui est la principale vulnérabilité de Bitcoin et le déclencheur potentiel d'un processus de centralisation complète.
- Les quotas sont une solution familière pour les marchés souffrant de la tragédie biens communs.
- Des quotas pourraient freiner à la course à la puissance de calcul entre les mineurs, réduisant ainsi le coût écologique du minage.
- Par construction, le minage est de toute façon une partie de l'écosystème Bitcoin qui a vocation à devenir insignifiante. 62 % de la base monétaire cible a déjà été minée.

7.1.2. Avantages d'un système de quotas nationaux

- Des quotas nationaux protégeraient Bitcoin contre l'excès de réglementation, car ils obligeraient les états à se mettre d'accord s'ils souhaitent contrôler ce qui se passe au niveau de la *blockchain*.
- L'idée de superviser le minage respecte la tradition historique selon laquelle les états veulent maîtriser l'émission des monnaies, mais ne se préoccupent pas tant que cela des transactions au quotidien.
- Le fait d'impliquer les gouvernements contribuerait à légitimer Bitcoin aux yeux du grand public.

7.1.3. Inconvénients d'un système de quotas

- Le minage indépendant et anonyme à petite échelle deviendrait impossible. Mais il n'est de toute façon déjà plus rentable. Autrement dit, des quotas pérenniseraient l'accès libre et équitable au système de transactions, mais en contrepartie le minage deviendrait un oligopole fermé.
- Idéalement, le contrôle des quotas de minage devrait être réalisé de façon décentralisée, sans tiers de confiance. Ceci nécessite un consensus pour modifier tous les logiciels. En pratique, il suffirait probablement de convaincre les bureaux de change, et le reste de l'industrie Bitcoin suivrait.
- Il n'est pas prouvé qu'il soit possible de faire respecter des quotas de minage de façon décentralisée.

- Les mineurs devraient révéler la structure de leur capital et plus généralement être beaucoup plus transparents qu'aujourd'hui. Mais nous pensons que la réglementation et la transparence sont inéluctables.
- Nous avons émis l'hypothèse (Section 3.9, « Erreur n°9 : La hausse récente du taux de change traduit forcément une forte demande pour les bitcoins ») que le sur-investissement dans le minage est peut-être une des causes de la bulle actuelle (2013-2014) plutôt que seulement sa conséquence, à cause du mécanisme contre-intuitif de régulation de la masse monétaire de Bitcoin. Des quotas ralentiraient la tendance au sur-investissement, conduisant probablement à une baisse des cours. Bitcoin n'est peut-être pas encore suffisamment mature pour atteindre une valeur de marché stable et déconnectée des coûts de minage.
- Les quotas de minage n'empêchent pas la centralisation de la gouvernance, qui pourrait être déclenchée non seulement par l'émergence d'un monopole de minage, mais aussi par divers autres scénarios de crise.

7.2. Généralisation : les oligopoles à défiance maximale

L'idée de quotas nationaux prolonge naturellement l'analogie qui présente bitcoin comme une ressource naturelle rare et le minage comme une activité comparable à l'industrie minière. Mais nous sommes conscients que la communauté Bitcoin pourrait la rejeter pour des raisons idéologiques. Dans cette section nous proposons un raisonnement aboutissant à une solution plus générale.

Reprenons au début. Bitcoin ambitionne de fournir un système de paiement sans tiers de confiance. Un livre comptable de toutes les transactions, géré de façon décentralisée, permettrait d'atteindre ce but. Les résultats théoriques sur le problème des généraux byzantins indiquent qu'un consensus distribué sur le contenu de ce livre peut être atteint si et seulement si la proportion de participants malhonnêtes est plafonnée.

Malheureusement, comme Bitcoin prétend aussi garantir l'anonymat, les participants ne sont pas bien définis. Bitcoin doit donc recourir à une métrique externe, décentralisée et raisonnablement équitable pour répartir les droits de décision. C'est à cela que sert le système *proof-of-work*. D'où l'affirmation que "les utilisateurs de Bitcoin votent avec leur puissance de calcul".

Nous avons déjà mentionné des alternatives telles que *proof-of-stake* et la sélection aléatoire. Mais dans tous ces systèmes, la centralisation apparait inévitablement parce que les votes peuvent être achetés. Lorsqu'un mineur rejoint un *pool*, tout se passe comme si il vendait son droit de regard sur le choix des transactions à valider.

La centralisation n'est pas intrinsèquement mauvaise (au contraire, elle peut générer des économies d'échelle). La concentration du pouvoir ne devient dangereuse que lorsque des seuils sont franchis, aboutissant par exemple à la tyrannie de la majorité. Avec un oligopole stable de trois *pools* de même taille, Bitcoin serait sûr et efficace. Malheureusement on sait que les oligopoles ont tendance à se transformer en cartels.

Comme les lois antitrust sont difficilement applicables *a posteriori* dans un système ouvert, décentralisé et anonyme, nous proposons plutôt d'organiser délibérément l'oligopole de façon à minimiser le risque de collusions. D'où l'idée d'oligopoles à défiance maximale. De ce point de vue, adopter des quotas nationaux de minage revient à reconnaître que plusieurs siècles de guerres et de compétition économique ont structuré le monde en un oligopole d'entités qui ne se font pas confiance : les nations.

8. Remerciements

Merci à Stéphane Gourichon pour ses commentaires sur une version antérieure de ce document.

9. Post-scriptum

- Le minage est toujours centralisé, mais les *pools* n'approchent plus du seuil des 50 %. La distribution du hachage est stable, avec un *pool* aux alentours de 30 % et les deux suivants totalisant environ 30 % également. Inutile de dire que cette situation est trop parfaite pour résulter d'un équilibre naturel de marché.

- La gouvernance consensuelle de Bitcoin a volé en éclats suite à des débats sur des détails techniques :

  - La ré-implémentation de la fonction *Replace By Fee (RBF)* [https://en.bitcoin.it/wiki/Transaction_replacement], qui rappelle que les transactions Bitcoin ne peuvent pas être instantanées.

  - La controverse sur la taille maximale des blocs [https://en.bitcoin.it/wiki/Block_size_limit_controversy], qui soulève un dilemme intéressant pour la crédibilité de Bitcoin : D'un côté, si le *status quo* est maintenu, alors Bitcoin ne pourra pas passer à l'échelle et concurrencer les systèmes de paiement existants. D'un autre côté, si la taille des blocs est augmentée, alors les utilisateurs comprendront que les règles ne sont pas immuables (y compris, potentiellement, celles qui fixent le plafond de la masse monétaire et qui garantissent la nature décentralisée de Bitcoin).

  Plusieurs acteurs tentent de prendre le contrôle de Bitcoin.

- Des institutions financières annoncent leur intérêt pour la "technologie des *blockchains*" et envisagent de créer des *blockchains* privées. Mais sans minage décentralisé, une *blockchain* n'est rien de plus qu'un service de notarisation très conventionnel. Au mieux, des *blockchains* privées permettront à des institutions concurrentes de se contrôler mutuellement, comme envisagé dans la Section 7.2, « Généralisation : les oligopoles à défiance maximale ».

Bibliographie

[BITCOIN] *Bitcoin: A Peer-to-Peer Electronic Cash System* . Satoshi Nakamoto. https://bitcoin.org/bitcoin.pdf.

[BLOCKCHAININFO_STATS] *Bitcoin Statistics* . http://blockchain.info/stats.

[BLOCKCHAININFO_CHARTS] *Bitcoin Charts* . http://blockchain.info/charts.

[BLOCKCHAININFO_POOLS] *Bitcoin Hashrate Distribution* . http://blockchain.info/pools.

[BITCOINIT_MYTHS] *Myths - Bitcoin* . https://en.bitcoin.it/wiki/Myths.