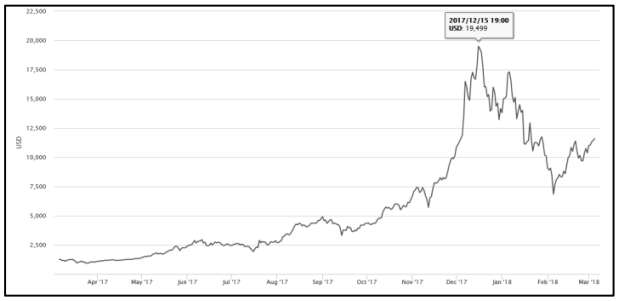
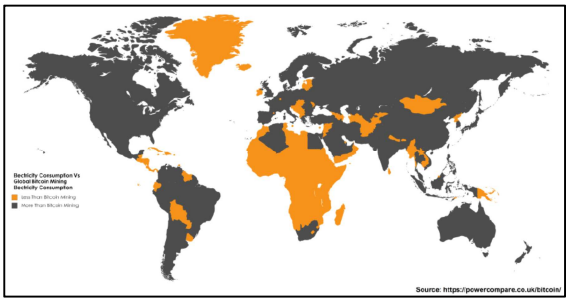
Le ***bitcoin : minage*** ou ***mirage*** **?**

La consommation énergétique monstrueuse du bitcoin

expliquée aux citoyens non spécialistes





par Daniel Leduc

Table des matières

1. Introduction 3
1.1. L'analogie des coffres-forts 5
2. Parenthèse au sujet du *hachage* 8
2.1. Un exemple très simpliste de *hachage*, pour illustrer le concept 8
2.2. Le *hachage* utilisé par le bitcoin 10
2.3. Le *hachage* comme passe-temps absurde 10
3. Le réseau bitcoin et la *chaîne de blocs* 11
3.1. Visite de la mine 12
3.2. À la recherche de la combinaison gagnante 13
3.3. Tous les autres ont travaillé "pour rien" 14
3.4. La récompense du mineur et la création de bitcoins 14
3.5. Puissance informatique (et électrique) et recherche de récompense 15
3.6. Le cercle vicieux de la *difficulté* 16
3.7. La *chaîne de blocs* 17
3.8. Le mauvais *mineur* 18
3.9. "Utilité" du *minage*: les guillemets enfins expliqués 18
4. La consommation énergétique du bitcoin 19
4.1. Estimations de consommation du réseau bitcoin 19
4.2. *Digiconomist*, la source omniprésente d'estimations 20
4.3. La consommation d'énergie du bitcoin comparée à celle de VISA 20
4.4. Quelques autres exemples concrets 21
4.5. Critiques de *Digiconomist* et extrapolations farfelues 21
4.6. Une autre approche pour "se faire une tête" au sujet des estimations 22
5. Quelques fausses conceptions voulant justifier le bitcoin énergivore 24
5.1. Réseau d'échanges entre pairs et élimination des intermédiaires 24
5.2. Attrait d'un système monétaire parallèle, indépendant des banques, et illusion d'un système (largement) distribué 24
6. Conclusion: la pointe de l'iceberg ? 27
Annexe A: Estimations de consommation énergétique mondiale annuelle du bitcoin (autres que celles de *Digiconomist*) 28

1. Introduction

Le *bitcoin* est cette monnaie virtuelle qui fait les manchettes depuis quelques temps. Elle est l'objet d'une spéculation intense. Comme le montre le graphique ci-dessous[1], son cours a explosé en 2017, atteignant près de 20 000 $US en décembre: une véritable ruée vers l'or.

Or, ce système de monnaie virtuelle consomme une énorme quantité d'énergie. Les estimations de consommation sont telles que certaines personnes pourraient croire à un canular. Lorsque je tente de les sensibiliser à cette problématique environnementale, certains laissent paraître une perplexité légitime et veulent comprendre ce qui explique cette consommation effrénée.

Au fil de leurs questions qui se multiplient, j'ai parfois l'impression de me retrouver, bien malgré moi, dans la position de celui qui devrait justifier le concept de bitcoin. Or, je n'ai aucunement l'intention de prendre la défense du bitcoin: je veux plutôt le dénoncer.

Mon but n'ayant jamais été de comprendre complètement le bitcoin, je ne suis pas en mesure de l'expliquer complètement, ni de répondre à toutes les questions qu'on pourrait avoir à son sujet.

Vous ne trouverez donc pas ici, par exemple, de réponses aux questions pratiques suivantes:

> Comment puis-je acheter des bitcoins avec des dollars (ou vice-versa) ?
> Qu'est-ce qu'un *portefeuille* (*wallet*) ?
> Les transactions en bitcoins sont-elles confidentielles ? anonymes ?

[1] Source: https://blockchain.info/fr/charts/market-price

Pas plus d'ailleurs que des réponses aux questions plus philosophiques, telles que:

> Est-il problématique que cette monnaie soit intangible (sans support physique) ?
> Le bitcoin est-il un système pyramidal (stratagème de Ponzi) ?

J'ai concentré mes lectures sur la notion de *minage*, car c'est du minage que découle l'énorme consommation énergétique bitcoin. Et mon inquiétude à son sujet est ce qui m'a motivé à me renseigner et à rédiger ce document de vulgarisation.

J'ai découvert un système fascinant, non seulement d'un point de vue technologique, mais également d'un point de vue économique. (La bombe thermonucléaire est aussi un concept fascinant, dont la compréhension est très stimulante intellectuellement, ce qui n'implique pas pour autant que son existence soit souhaitable.)

J'ose croire que ce document, bien que relativement long, n'est pas très difficile à lire. Les concepts y sont présentés de façon simple et progressive, afin de rendre la compréhension du bitcoin accessible au citoyen, pas seulement au spécialiste.

La plupart des auteurs d'articles de vulgarisation sur le bitcoin parlent en paraboles, par exemple en écrivant que les "mineurs" sont récompensés pour résoudre des "puzzles", ou participent à une sorte de "loterie". Tout cela m'apparaissait incompréhensible et je restais sur ma faim. Les analogies et les images doivent aider à comprendre, au lieu de contribuer à entretenir le mystère.

Maintenant que j'ai saisi le fonctionnement du bitcoin, je comprends mieux pourquoi on utilise ces images. Je me suis efforcé d'expliquer le fonctionnement du système avec assez de détails pour aller au-delà de telles métaphores qui, à elles seules, ne clarifient rien, sans pour autant que la compréhension du présent document exige du lecteur une expertise particulière, qu'elle soit économique ou technologique. (Je ne suis pas un expert moi-même.)

Dans ce document, concentrez-vous sur la compréhension des notions qui vous sont présentées, au fur et à mesure qu'elles y apparaissent, sans trop vous demander à quoi elles servent. Si vous cherchez trop à comprendre immédiatement la raison d'être de chaque concept, vous essaierez de courir avant d'avoir appris à marcher, et vous trébucherez. Faites donc preuve de patience; cet état d'esprit vous permettra d'y voir plus clair, car la raison d'être de chaque concept émergera graduellement pour former un tout qui vous semblera – espérons-le – plus cohérent.

Voici donc ce que je peux tenter de vous expliquer, au meilleur de ma compréhension, et sans pouvoir exclure la possibilité d'avoir commis quelques erreurs, inexactitudes ou simplifications. Malgré ces éventuelles maladresses, je suis convaincu que:

- la lecture de ce qui suit peut vous permettre de mieux comprendre le bitcoin;
- mes conclusions quant à la consommation énergétique du bitcoin demeurent valides.

1.1. L'analogie des coffres-forts

Les billets de banque, contrairement aux pièces de monnaie, comportent un numéro de série qui les rend uniques. Si l'on disposait d'un système adéquat, on pourrait donc théoriquement documenter en détail toutes les transactions dans le cadre desquelles un billet de banque spécifique a changé de mains, depuis qu'il a été imprimé. C'est en quelque sorte ce qui se passe avec le bitcoin.

La *chaîne de blocs* (*blockchain* en anglais) est la technologie sur laquelle repose le fonctionnement du bitcoin. Chaque *bloc* documente une liste de transactions en bitcoins et les blocs sont liés entre eux pour former une chaîne qui contient tout l'historique des échanges de bitcoins depuis leur création.

Imaginons la *chaîne de blocs* comme une chaîne de coffres-forts, chacun d'eux contenant un cahier dans lequel est consignée une liste de transactions.

La combinaison permettant d'ouvrir un coffre-fort est inscrite sur sa porte. N'importe qui peut donc facilement ouvrir n'importe quel coffre-fort pour prendre connaissance des informations qui s'y trouvent. La combinaison inscrite sur la porte d'un coffre-fort identifie aussi celui-ci, un peu comme une adresse inscrite sur la porte d'une maison.

Dans le cahier contenu dans un coffre-fort, on inscrit aussi la combinaison permettant d'ouvrir un autre coffre-fort. Puisque les combinaisons sont inscrites sur les portes, cette information n'est pas tant utile pour ouvrir l'autre coffre-fort que pour permettre d'identifier quel est le coffre-fort précédent dans la chaîne. (C'est "l'adresse" de la prochaine porte à ouvrir dans la chaîne.)

Lorsqu'une personne veut transférer des bitcoins à une autre personne, le système vérifie d'abord qu'elle possède bien ces bitcoins et qu'elle ne les a pas déjà dépensés ailleurs. Reprenant l'analogie des billets de banque avec leurs numéros de série, le système s'assurera que ces bitcoins (comportant des "numéros de série" bien spécifiques) sont devenus antérieurement la propriété du payeur et qu'ils sont toujours en sa possession.

Supposons que Jean veuille transférer 3 bitcoins à Marie le 5 octobre pour lui acheter quelque chose. Il faut donc vérifier, en inspectant les cahiers de la chaîne de coffres-forts, que Jean possède bien ces mêmes 3 bitcoins, i.e. qu'on dispose d'une trace de leur transfert antérieur à Jean, et que la personne qui les avait transférés à Jean les avait bien reçus d'une autre personne, etc.

Dans certains cas, le cahier d'un coffre-fort ne contiendra aucune information concernant ces mêmes 3 bitcoins (avec le bon "numéro de série"), mais il permettra quand même d'identifier le coffre-fort précédent (par sa combinaison) et on pourra ainsi poursuivre la recherche. Ultimement, on retrouvera, dans l'un des coffre-forts, l'écriture documentant la création de ces 3 bitcoins au bénéfice de leur premier détenteur. On aura alors remonté toute la chaîne des transactions impliquant les échanges de ces trois mêmes bitcoins et constaté que rien ne cloche.

Cette vérification est relativement facile, puisque les combinaisons de tous les coffre-forts sont connues. La *chaîne de blocs* est en quelque sorte un livre grand ouvert et consultable par tous.

Le modèle de coffre-fort utilisé a par contre une caractéristique bien spéciale: sa combinaison dépend de son contenu. Elle changera, si on modifie quoi que ce soit dans le cahier que contient le coffre-fort (qu'il s'agisse du montant d'une transaction, ou encore de la combinaison du coffre-fort précédent).

Voyons maintenant comment un nouveau coffre-fort est créé et ajouté à la chaîne.

Personne ne connaît d'avance la combinaison qui permet d'ouvrir un nouveau coffre-fort. La seule façon d'y parvenir, c'est d'essayer diverses combinaisons, jusqu'à ce qu'on en trouve une qui fonctionne. Ces multiples essais sont ce qu'on appelle le *minage* et ceux qui s'adonnent à cette activité sont naturellement appelés les *mineurs*.

On accumule d'abord, dans un nouveau cahier, un bloc d'informations au sujet de plusieurs nouvelles transactions (par exemple, le transfert de 3 bitcoins de Jean à Marie). On y inscrit aussi la combinaison du dernier coffre-fort qui a été rattaché à la chaîne.

On fait ensuite de multiples copies de ce document, chacune ne différant des autres que par le nom du mineur auquel elle est destinée. On place ces copies dans autant de coffre-forts identiques, lesquels ne font pas encore partie de la chaîne. Puisque chaque copie contient le nom (unique) du mineur auquel elle est destinée, chacun de ces nouveaux coffres-forts aura donc une combinaison différente.

On insère aussi une récompense dans chacun de ces nouveaux coffres-forts, on les verrouille et on remet à chaque mineur le coffre-fort qui lui est attribué. Chaque mineur doit alors chercher, par essais et erreurs, une combinaison permettant d'ouvrir son coffre-fort. Le premier qui y parvient a accès à sa récompense et inscrit la combinaison qu'il a trouvée sur la porte de son coffre-fort. La récompense est un nombre de bitcoins et c'est ainsi, par le processus de minage, que sont créés de nouveaux bitcoins.

Le cycle de minage est alors complété. Le coffre-fort du mineur gagnant fait désormais partie de la chaîne des coffres-forts dont on connaît la combinaison. Puis, le cycle de minage recommence: la combinaison qui a permis au mineur gagnant d'ouvrir son coffre-fort est inscrite dans un nouveau cahier, avec une nouvelle liste de transactions, dont on fait de multiples copies placées dans de nouveaux coffres-forts, etc.

À chaque cycle, les nouveaux coffres-forts des mineurs "perdants", jamais ouverts, disparaissent, avec la récompense et la copie du nouveau cahier qu'ils contenaient (disons que ces autres nouveaux coffres-forts, à défaut d'avoir pu être rattachés à la chaîne, se transforment en citrouilles).

Supposons que Jean veuille tricher en falsifiant le document relatant sa transaction avec Marie. Il ouvre un coffre-fort qui fait déjà partie de la chaîne et inscrit, dans le document qui s'y trouve, qu'il a transféré à Marie 2 bitcoins (plutôt que 3) le 5 octobre. Jean croit donc disposer à nouveau de 1 bitcoin qu'il avait déjà détenu et qu'il vient de voler à Marie; il entrevoit la possibilité de dépenser une deuxième fois ce même bitcoin en le transférant à quelqu'un d'autre en échange d'un bien ou d'un service[2].

[2] Supposons, pour simplifier la situation, que Marie n'avait encore dépensé aucun des bitcoins reçus de Jean.

Mais cette altération du contenu du document entraîne une modification de la combinaison du coffre-fort correspondant.

Une fois qu'il aura trouvé, par essais et erreurs, cette nouvelle combinaison, il devra l'inscrire dans le document du coffre-fort suivant, à la place de l'ancienne combinaison qui y avait déjà été inscrite. Ce changement au document du coffre-fort suivant entraînera lui-même un changement de combinaison de celui-ci et Jean devra se lancer à la recherche de cette nouvelle combinaison. Et ainsi de suite.

Pendant que Jean fait tout ce travail, une armée de mineurs s'affaire à trouver la combinaison de nouveaux coffres-forts et à les ajouter au bout de la chaîne. Cette armée de mineurs parviendra collectivement à trouver une nouvelle combinaison de coffre-fort bien plus rapidement que Jean ne peut le faire seul. Jean ne parviendra donc jamais à déverrouiller assez rapidement tous les coffres-forts de la chaîne pour falsifier tour à tour les documents qu'ils contiennent et à rattraper les mineurs au bout de la chaîne. Les efforts démesurés que Jean devrait consacrer à dissimuler son méfait lui rendront la tâche impossible. Et si, par ailleurs, Jean avait la possibilité de déployer de tels efforts, il serait bien plus payant pour lui de les consacrer à miner "honnêtement", afin de toucher les récompenses associées à de nouveaux coffres-forts qu'il parviendrait à ouvrir; il n'aurait pas intérêt à utiliser une telle habileté pour tricher, car ce serait moins payant.

Comme toute analogie, celle-ci a ses limites et pourrait, sous certains aspects, ne pas "coller" parfaitement à la réalité du bitcoin. Mais c'est l'analogie qui me semble la plus utile et la plus proche du fonctionnement réel du bitcoin. Les fameuses "énigmes" ou "calculs complexes" que doivent résoudre les mineurs sont simplement ces combinaisons de coffres-forts qu'ils doivent trouver par essais et erreur.

On pourrait raffiner l'analogie en précisant, par exemple, que chaque coffre-fort peut être déverrouillé par plus d'une combinaison. Moins il y a de combinaisons permettant d'ouvrir un coffre-fort, plus il est *difficile* d'en trouver une qui fonctionne. Cette notion de *difficulté* est un concept fondamental du *minage*.

Cette analogie permet aussi d'introduire un autre concept. Il est évident que la recherche par essais et erreurs d'une combinaison permettant d'ouvrir un coffre-fort représente beaucoup de travail; une fois trouvée, une telle combinaison, affichée sur la porte du coffre-fort (et dans le cahier du prochain coffre-fort), constitue une *preuve de* ce *travail*.

2. Parenthèse au sujet du *hachage*

Avant de discuter du bitcoin proprement dit, il faut ouvrir une (relativement longue) parenthèse et parler de notions de *cryptographie* ou de *hachage*. C'est un détour nécessaire et qui en vaut la peine, pour enfin dissiper le voile de mystère entourant le fonctionnement du bitcoin et aussi pour comprendre pourquoi on le qualifie de *cryptomonnaie*.

Le *hachage* est un traitement informatique par lequel certaines informations (nombres, messages, etc.) sont combinées d'une façon complexe pour donner un code numérique de longueur fixe qu'on appelle *empreinte* ou "*haché*" (*hash* ou *hashcode* en anglais).

2.1. Un exemple très simpliste de *hachage*, pour illustrer le concept

Voici un exemple très simpliste de mon cru. Supposons qu'on associe à chaque lettre d'un message un nombre correspondant à sa position dans l'alphabet (A = 1, B = 2, C = 3, etc.), puis qu'on additionne ces nombres pour donner un code numérique.

On pourrait dire que le message "ABACA" (c'est le nom d'un bananier des Philippines) correspond au code numérique 8:

A:	1
B:	2
A:	1
C:	3
A:	1
Somme:	8

On applique ainsi une "recette" (un *algorithme*, en terminologie informatique) qui décrit comment obtenir un code numérique (8) à partir d'une information donnée ("ABACA").

La même recette pourrait être appliquée à un message beaucoup plus long que le seul mot "ABACA". Elle pourrait par exemple être appliquée au contenu de tout un livre.

Imaginons un livre de 250 pages, comportant 2 000 lettres chacune (oublions, pour simplifier, la présence d'espaces blancs, de ponctuation, etc.), qui comporterait donc 500 000 lettres.

Dans ma "recette", la valeur maximale associée à chaque lettre serait 26 (pour la lettre Z, vingt-sizième de l'alphabet). La valeur maximale de notre code numérique, obtenu en appliquant la même "recette" à un tel livre, serait 13 000 000 (250 x 2 000 x 26), si le livre ne comportait que des pages remplies de Z (ce qui serait très endormant…).

On peut donc envisager qu'un code numérique de huit chiffres (en notation décimale) puisse être suffisant pour servir d'*empreinte* aussi bien pour un seul mot ("ABACA": 00 000 008) que pour un livre complet ("ZZZZ….ZZZ" sur 250 pages: 13 000 000).

Si, de façon plus réaliste, notre livre comportait une variété de lettres (toutes les autres lettres ayant une "valeur" inférieure à celle de Z), il aurait pour empreinte un autre nombre (peut-être, par exemple, 02 873 129 ou 07 229 438, ou toute autre valeur qui dépendrait de son contenu spécifique).

On pourrait ainsi combiner toutes les lettres contenues dans un livre pour obtenir un code numérique "unique". En effet, si on apportait des changements au contenu du livre et qu'on répétait le processus, on obtiendrait vraisemblablement un code numérique différent.

En utilisant une "recette" plus complexe et sophistiquée que la recette primitive de mon exemple ci-dessus, on pourrait faire en sorte qu'il soit très peu probable que deux ensembles de données différents (par exemple deux livres distincts) correspondent au même code numérique, i.e. à la même *empreinte*. Par exemple, à deux livres qui ne différeraient, ne serait-ce que d'un seul caractère, correspondraient des codes différents.

On ne peut pas, à partir du code numérique obtenu, connaître tout le contenu des données qui en sont à l'origine: on ne pourrait pas connaître l'histoire racontée dans le livre à partir de son *empreinte*, tout comme on ne pourrait pas déduire que c'est le mot "ABACA" qui est à l'origine de l'*empreinte* 00 000 008, si la seule information dont on disposait était ce code numérique.

Par contre, pour savoir si deux livres ont un contenu identique, il serait beaucoup plus facile de comparer leurs empreintes respectives, plutôt que de comparer les deux livres page par page, ligne par ligne et caractère par caractère.

L'empreinte constitue, en quelque sorte, un résumé très compact du contenu du livre, qu'on pourrait appeler aussi sa "signature", en ce sens qu'elle est (autant que possible) unique[3].

Les livres qu'on pourrait cryptographier ainsi ne sont pas nécessairement des romans. Il pourrait tout aussi bien s'agir de livres comptables, dans lesquels on aurait inscrit les détails de transactions. Par exemple: à telle date, telle personne a fait un virement (paiement) de tant de bitcoins à telle autre personne.

Est-ce que tout ce qui précède vous semble clair ? Sinon, relisez cette section avant de passer à la section suivante.

[3] Ma "recette" très primitive décrite ci-dessus ne permettrait pas de garantir un tel résultat avec une grande probabilité. Par exemple, les mots "ABACA" et "ACABA" correspondraient à la même empreinte de 0 000 0008. Encore une fois, cette "recette" est simpliste et n'a d'autre prétention que celle de vous aider à comprendre le concept général.

2.2. Le *hachage* utilisé par le bitcoin

En réalité, le traitement de *hachage* du bitcoin est beaucoup plus complexe que dans l'exemple simpliste donné ci-dessus. Par exemple, en utilisant la *fonction de hachage* SHA-256 (un *algorithme* plus sophistiqué que ma "recette"), on obtiendra, à partir du message "Bonjour, monde!0", l'*empreinte* suivante :

a9efd73638806846d0495fb92e2deba6e2e1ad5bc453e28e5fdc1334c97c21a8.

Il s'agit à première vue d'un très long code (de 64 caractères), qui semble (et qui est) plus complexe que le message d'origine "Bonjour, monde!0". Mais quand on pense qu'on pourrait aussi "résumer", avec un code de la même longueur, le contenu d'un livre de 250 pages, on en conçoit mieux l'utilité.

Je ne connais pas les détails par lesquels la fonction de hachage SHA-256 nous permet d'obtenir un tel code. Les curieux peuvent chercher sur internet (sur Wikipedia ou ailleurs). Il me suffit de savoir que c'est très complexe, et que ces algorithmes, contrairement à ma recette primitive, sont conçus pour minimiser la probabilité de *collision* (i.e. la probabilité que la même empreinte corresponde à deux ensembles de données-sources différentes).

Malgré la complexité du calcul, c'est un traitement qui peut être effectué très rapidement par un ordinateur.

2.3. Le *hachage* comme passe-temps absurde

Supposons maintenant que vous vous lanciez un petit défi.

Vous ajoutez un nombre à la fin du message (par exemple: "Bonjour, monde!**0**") et vous le soumettez à un ordinateur qui peut calculer l'empreinte correspondante en utilisant la fonction de hachage SHA-256.

Puis, vous changez le nombre ajouté au message ("Bonjour, monde!**1**","Bonjour, monde!**2**", etc.) et vous soumettez tour à tour à l'ordinateur ces messages modifiés pour obtenir leurs empreintes respectives.

Supposons maintenant que votre but soit d'obtenir une empreinte qui débute par un certain nombre de zéros. (Cet objectif peut vous sembler absurde et inutile, mais considérez néanmoins cette activité comme un passe-temps agréable et persévérez…)

Il n'y a pas moyen de prévoir quel genre de modification à votre message vous permettrait d'obtenir un tel résultat. Vous devrez donc procéder par essais et erreurs. Ça vous rappelle les coffres-forts ?

Vous pourriez être très chanceux et tomber sur une telle empreinte au premier essai. Mais vous pourriez aussi devoir réessayer pendant très longtemps, en changeant à chaque fois le nombre ajouté à la fin de “Bonjour, monde!”, avant de tomber sur une telle empreinte.

Et vous pouvez sans doute imaginer que ce serait d’autant plus difficile que vous souhaiteriez obtenir un plus grand nombre de zéros consécutifs au début de votre empreinte.

Voici un exemple tiré de l’article *Preuve de travail* sur Wikipedia[4], dont je me suis inspiré dans ce qui précéde:

Il est demandé à un processeur de réaliser une preuve de travail consistant à coder une variation de "Bonjour, monde!" en utilisant la fonction de hachage SHA-256 jusqu'à trouver une empreinte qui débute par 4 zéros. La variation consiste à ajouter un nombre à la fin de la chaîne de caractères. Le processeur devra réaliser 33 681 tentatives pour réussir.

"Bonjour, monde!0" : a9efd73638806846d0495fb92e2deba6e2e1ad5bc453e28e5fdc1334c97c21a8
"Bonjour, monde!1" : f767b47fd98fab25d08bd155c42708b434ac86bfa8d8b95b1457146e86b728e5
"Bonjour, monde!2" : fad41d13e759487a3d70a09c66c3e8ae8e9803f1fadba5411e039c35ac01f8b9
…
…
"Bonjour, monde!33678" : c8c15f22d9c2a9ce84f6c8ca5d5943e3bbc2d39758474c3d969c17359e6cf212
"Bonjour, monde!33679" : d109eb920aef296041c7b878eea20f1abc8fb957ea59bdf130d1dcd810722c2a
"Bonjour, monde!33680" : 0000abebe9c6554c85176b8e9f9f3f4ed9b7e8dc856a7b5cb9177bf7b22e1871

Même avec un ordinateur qui se chargerait de calculer pour vous l’empreinte de chaque message que vous lui soumettriez, essayez de vous imaginer le temps requis pour soumettre une question semblable 33 681 fois de suite à votre ordinateur (en supposant que vous le fassiez interactivement, “à la main”).

Tout ça doit vous sembler de plus en plus absurde... Mais tout ce qui compte, c’est que vous ayiez compris les notions jusqu’ici, sans nécessairement comprendre leur finalité.

3. Le réseau bitcoin et la *chaîne de blocs*

La longue parenthèse concernant le *hachage* étant enfin fermée, nous entrons maintenant dans le vif du sujet.

Comme on l’a vu à la section 1.1, le bitcoin repose sur une technologie sous-jacente, la *chaîne de blocs* (plus communément appelée *blockchain*).

[4] https://fr.wikipedia.org/wiki/Preuve_de_travail

Le réseau bitcoin relie entre eux des *noeuds* (*nodes* en anglais). Il s'agit d'ordinateurs qui participent, de diverses manières, au fonctionnement du système.

Certains de ces *noeuds* jouent un rôle particulier et sont appelés *mineurs*. (On appelle aussi *mineurs* les individus ou organisations qui possèdent ces ordinateurs et les utilisent à cette fin).

On peut résumer comme suit[5] le processus de minage:

1. Les détails des nouvelles transactions sont diffusés à tous les *noeuds*.
2. Chaque *mineur* rassemble ces informations pour former un *bloc*.
3. Chaque *mineur* travaille pour trouver un code de *preuve de travail* pour son *bloc*.
4. Quand un *mineur* trouve une *preuve de travail*, il diffuse son *bloc* à tous les *noeuds*.
5. Les *noeuds* récepteurs valident les transactions du *bloc* et acceptent le *bloc* seulement si toutes ses transactions sont valides.
6. Les *mineurs* expriment leur approbation du *bloc* en se mettant à travailler sur le prochain *bloc*, lequel incorporera l'*empreinte* du *bloc* accepté.

(Pas clair ? Pas grave! Les explications suivent…)

Ce processus constitue un cycle d'environ 10 minutes, au terme duquel un nouveau *bloc* est ajouté à la *chaîne de blocs*.

Le résumé ci-dessus mentionne la notion de *preuve de travail* (*proof-of-work*). Notez bien que l'article de Wikipedia cité précédemment (avec l'exemple "Bonjour, monde!") portait précisément sur ce concept.

3.1. Visite de la mine

Qu'est-ce que tout cela signifie ? Mettez-vous maintenant dans la peau d'un mineur et enfilez votre casque: on va descendre dans la mine pour voir ça de plus près…

Vous recevez du réseau bitcoin des informations au sujet des transactions en bitcoins les plus récentes (celles des 10 dernières minutes, en gros).

Vous combinez toutes ces informations en un *bloc*, lequel documente une liste de transactions. Un *bloc* est en quelque sorte une page du grand livre comptable que constitue la *chaîne de blocs*. Puis vous vous attelez à la tâche d'obtenir, en soumettant ce *bloc* à la fonction de hachage, une empreinte qui débute par un certain nombre de zéros.

[5] Il s'agit d'une traduction libre d'un extrait de la version anglaise de l'article *Bitcoin network* de Wikipedia (section *Process*) https://en.wikipedia.org/wiki/Bitcoin_network.

3.2. À la recherche de la combinaison gagnante

Vous procédez comme nous l'avons décrit plus tôt, sauf que cette fois-ci, au lieu du message "Bonjour, monde!", ce que vous cryptographiez, c'est un bloc d'informations documentant une liste de transactions en bitcoins, à laquelle vous ajoutez un nombre quelconque (comme celui qui était ajouté au message "Bonjour, monde!"). Vous modifiez ce nombre répétitivement, tant que vous n'obtenez pas une empreinte débutant par le nombre souhaité de zéros.

(Ce nombre, que vous faites varier au fil de vos diverses tentatives, s'appelle le *nonce*, en terminologie bitcoin. Retenez le terme, car je l'utiliserai plus loin, mais ne me demandez pas pourquoi on l'appelle ainsi: je ne le sais pas.)

Lorsque vous obtenez une empreinte respectant le critère (comportant le nombre de zéros initiaux souhaités), vous avez en quelque sorte trouvé une solution au problème sur lequel vous travailliez.

Comme je le mentionnais en introduction, divers documents de vulgarisation, articles, etc. font référence à des "puzzles", à des "énigmes" ou des "devinettes" que les mineurs de bitcoins doivent résoudre. Cette façon de présenter les choses semble bien mystérieuse, mais c'est peut-être la meilleure façon que bien des gens ont trouvée de décrire le processus décrit ci-dessus, sans entrer dans les détails.

Comme dans une énigme, il y a effectivement une réponse difficile à trouver et, à défaut de pouvoir la deviner, on y consacre énormément de puissance de calcul, un peu comme si on tentait d'ouvrir un coffre-fort en essayant successivement toutes les combinaisons possibles.

On parle souvent aussi d'une loterie, une autre analogie qui met l'accent sur le fait qu'il s'agit en quelque sorte d'un concours, avec un numéro gagnant inconnu a priori (un *nonce* qui permet d'obtenir une *empreinte* avec le bon nombre de zéros initiaux).

Pour des informations données (une liste de transactions spécifiques en bitcoins), il existe possiblement plusieurs solutions (plusieurs empreintes commençant par le nombre souhaité de zéros), chacune correspondant à une valeur de *nonce* différente.

À moins d'être très chanceux (ce qui est possible, mais peu probable), cela vous prendra beaucoup de calculs avant de trouver une solution acceptable (peut-être 33 681 essais, comme dans l'exemple "Bonjour, monde!", peut-être moins, peut-être plus). Cette solution qui fonctionne, vous donnant le nombre souhaité de zéros initiaux, constituera une pépite d'or, pour reprendre l'analogie du minage.

Vous vous empressez alors de diffuser cette information aux autres mineurs, à travers le réseau bitcoin: "J'en ai trouvé une!". Et vous leur soumettez la solution que vous avez trouvée: la liste de transactions bitcoins sur laquelle vous avez travaillé, avec le *nonce* qui vous a permis de trouver votre solution, ainsi que votre solution elle-même (l'*empreinte* commençant par tous ces zéros tant convoités). Le tout (en y ajoutant aussi certaines autres informations) constituera, pourvu qu'il soit validé par les autres *mineurs*, un *bloc* de la *chaîne de blocs*.

3.3. Tous les autres ont travaillé "pour rien"

Les autres mineurs, qui n'ont pas encore trouvé de solution, reçoivent votre message. Ils vérifient alors votre solution, en appliquant la fonction de hachage au *bloc* que vous leur avez soumis, pour s'assurer qu'ils obtiennent bien la même *empreinte* que vous.

C'est une vérification facile, car ils n'ont à appliquer la recette de la fonction de hachage qu'une seule fois, en utilisant la valeur de *nonce* que vous leur avez communiquée à même votre bloc.

C'est un peu comme si la preuve de la solution était inscrite sur un papier, conservé dans une boîte fermée à clef. Le mineur gagnant présente aux autres sa solution en leur fournissant également une clef (le *nonce*) pour ouvrir la boîte et prendre connaissance de la preuve. Il est beaucoup plus facile et rapide d'ouvrir cette boîte, une fois qu'on a la clef, que de passer du temps à chercher la clef dans la noirceur de la mine….

(On peut aussi faire une analogie intéressante avec le sudoku: il faut consacrer passablement de temps et d'efforts pour solutionner une grille de sudoku, mais une personne à qui vous soumettez votre solution pourra la vérifier rapidement avec beaucoup moins d'efforts.)

Les autres mineurs réalisent alors que votre solution est valide. Dans cette course pour rechercher une solution, vous êtes le gagnant, et tous les autres mineurs sont perdants. Ils abandonnent leur recherche d'une solution pour le bloc courant et se lancent avec vous à la recherche d'une solution pour le prochain bloc.

On voit ici à quel point le réseau bitcoin est inefficace. Tous les mineurs font simultanément des calculs similaires, très intensifs, mais tous ces efforts seront vains, sauf ceux déployés par le seul mineur gagnant. Le nombre de *mineurs* de bitcoins dans le monde est très difficile à estimer, mais certaines sources indiquent qu'il y en aurait plusieurs dizaines de milliers[6]. En tout temps, tous, sauf un, font ces calculs "inutilement"[7].

3.4. La récompense du mineur et la création de bitcoins

Mais qu'est-ce qui motive donc les mineurs à s'engager dans une telle course ?

Une récompense (un certain nombre de nouveaux bitcoins) est rattachée à chaque bloc pour lequel une solution est trouvée. À l'heure actuelle, on parle d'une récompense de 12.5 bitcoins par bloc *miné*, ce qui peut valoir facilement plus de 100 000 $US, au cours actuel du bitcoin (début 2018).

---

[6] Le blog suivant estime que le nombre de mineurs a varié entre environ 20 000 et 80 000 entre avril 2013 et avril 2014.: https://organofcorti.blogspot.ca/2014/05/165-estimating-number-of-bitcoin-miners.html#!/2014/05/165-estimating-number-of-bitcoin-miners.html.
Voir aussi: https://bravenewcoin.com/news/number-of-bitcoin-miners-far-higher-than-popular-estimates

[7] On comprendra plus loin pourquoi j'utilise ces guillemets, lorsque j'expliquerai la raison d'être de ces calculs.

Dans ce système, c'est ainsi que de nouveaux bitcoins sont créés. On compare cette création de bitcoins à l'impression de nouveaux billets de banque par une banque centrale, ou à la coulée de nouveaux lingots d'or à partir de matière aurifère extraite d'une vraie mine.

Ces nouveaux bitcoins que le système attribue au mineur gagnant constituent la première transaction de la liste incorporée à chaque nouveau bloc. Évidemment, seuls les bitcoins de récompense du bloc gagnant sont réellement créés. Les blocs inachevés des autres mineurs partent en fumée, avec la transaction potentiellement créatrice de bitcoins qu'ils comportaient.

Aucun mineur ne gagne à tous les coups, mais la récompense associée aux blocs gagnants doit être suffisamment importante pour compenser tous les coûts encourus (par exemple l'électricité consommée), incluant les coûts associés aux blocs minés sans succès. Sinon, le *minage* n'aurait aucun sens économique et personne n'aurait intérêt à *miner*. Statistiquement, il faut qu'un mineur puisse gagner assez souvent pour que le jeu en vaille la chandelle.

Il existe de nombreux regroupements (*pools*) de mineurs qui mettent leur puissance de calcul en commun pour gagner ces récompenses. Un groupe de mineurs peut collectivement *miner* des blocs gagnants plus fréquemment; les récompenses ainsi obtenues sont partagées entre les participants, au prorata de la puissance de calcul qu'ils ont chacun contribuée.

Je ne comprends pas comment cette approche pourrait permettre à un mineur individuel d'augmenter ses revenus de minage, mais il est clair que la participation à un *pool* peut lui permettre à tout le moins de régulariser ses revenus: un mineur individuel membre d'un *pool* obtiendra plus souvent de petits montants (fractions de récompenses), au lieu de gagner rarement de plus gros montants (récompenses entières de 12.5 bitcoins).

3.5. Puissance informatique (et électrique) et recherche de récompense

Compte tenu des explications ci-dessus, vous pouvez imaginer que plus un mineur déploie de moyens pour rechercher une solution, plus il aura de chances d'être le premier à en trouver une et à gagner la récompense qui s'y rattache.

Le réseau bitcoin a été mis sur pied en 2009. À l'époque, un individu pouvait miner des bitcoins avec son ordinateur personnel ou avec du matériel informatique spécialisé plus performant. Aujourd'hui, ce n'est plus possible. Ce ne sont plus que des organisations qui ont les moyens de se procurer tout le matériel informatique nécessaire. On parle de *mines* ou de *fermes* de bitcoins (des entrepôts remplis d'étagères sur lesquelles sont entassés jusqu'au plafond des ordinateurs spécialisés), ou encore les *pools* de mineurs évoqués plus tôt.

Un seul ordinateur ne consomme pas énormément d'électricité. Mais un entrepôt bourré d'ordinateurs en consomme beaucoup. Au Québec, les mineurs professionnels de bitcoins cherchent notamment à s'installer dans des usines désaffectées, par exemple dans d'anciennes usines de pâtes et papiers[8].

[8] http://www.lapresse.ca/affaires/economie/quebec/201802/22/01-5154978-matane-veut-transformer-une-papeterie-en-mine-de-bitcoins.php

Ces usines sont vastes et déjà pourvues d'installation électriques de grande capacité, autrefois utilisées pour alimenter de grosses machines, et aujourd'hui capables d'alimenter tous ces ordinateurs.

Bien sûr, une entreprise qui dispose de tels moyens a un avantage certain sur un individu qui ne dispose que d'un seul ordinateur. On se doute bien qu'elle aura bien plus de chances que le mineur individuel d'être la première à trouver une solution pour un nouveau bloc de la chaîne.

Une ferme de bitcoins en Chine[9]

3.6. Le cercle vicieux de la *difficulté*

Mais il y a un autre facteur qui rend nécessaire tout ce matériel informatique dernier cri ultra-performant, dans ce que de nombreux auteurs qualifient de "course aux armements".

La *difficulté* du minage augmente avec le temps (un peu comme il devient graduellement plus difficile de trouver des pépites d'or dans un gisement, au fur et à mesure que les pépites les plus faciles à trouver en ont déjà été extraites). Au fil du temps, le système bitcoin exige, comme solutions valides, des empreintes de blocs comportant de plus en plus de zéros initiaux.

Tous les 2 016 blocs (au bout d'environ 14 jours, puisque le minage de chaque bloc prend environ 10 minutes), la *difficulté* est ajustée en fonction de la performance récente du réseau, en vue de maintenir à 10 minutes la durée moyenne de minage des blocs. De cette façon, le système s'adapte automatiquement à la puissance totale de calcul disponible sur le réseau. Entre le 1er mars 2014 et le 1er mars 2015, le nombre moyen de *nonces* que les mineurs ont dû essayer avant de créer un nouveau bloc a augmenté de 16.4 trillions[10] à 200.5 trillions.[11]

C'est un cercle vicieux. Si les mineurs commencent à utiliser du matériel informatique plus performant, des solutions sont trouvées plus rapidement (en moins de 10 minutes) pour chacun des blocs. Le système réagira alors en augmentant le niveau de *difficulté* du minage (le nombre de zéros exigés au début d'une empreinte). Les mineurs auront alors tendance à se munir de matériel plus performant (et donc plus énergivore) pour s'attaquer à ce niveau de difficulté accru.

---

[9] Cette photo est tirée d'un article intéressant du magazine *Spectrum* de l'*Institute of Electrical and Electonics Engineers* (IEEE): https://spectrum.ieee.org/computing/networks/why-the-biggest-bitcoin-mines-are-in-china

[10] Un *trillion* (*quintillion* en anglais) est un milliard de milliards (10^{18}).

[11] Ce paragraphe est une traduction libre d'un extrait de la version anglaise de l'article *Bitcoin* de Wikipedia (https://en.wikipedia.org/wiki/Bitcoin). Cette information n'apparaissait pas dans la version française.

3.7. La *chaîne de blocs*

La cryptographie (*hashing*) est une technologie habituellement utilisée pour assurer la confidentialité de certaines informations. Par exemple, les mots de passe des utilisateurs sur un ordinateur ou sur un site internet sont conservés sous forme cryptographiée.

Vous avez peut-être entendu dire que le bitcoin permettait d'effectuer des transactions de façon anonyme. Mais dans le système bitcoin, tous ces calculs cryptographiques (*hashing*) ne servent même pas à assurer l'anonymat ou la confidentialité des transactions. Le mystère s'épaissit. À quoi servent-ils donc, alors ?

Pourquoi se donner tant de mal ? Pourquoi les mineurs doivent-ils accomplir un travail aussi *difficile* afin de pouvoir fournir, pour chaque bloc, une empreinte valide qui constitue la *preuve de* ce *travail* ? Travaille-t-on simplement *pour pouvoir prouver qu'on a travaillé* ?

On a jusqu'ici beaucoup parlé des *blocs* de la *chaîne de blocs*, sans s'attarder vraiment à la *chaîne* elle-même. Pourquoi parle-t-on d'une *chaîne*, et qu'est-ce qui relie entre eux les maillons que sont les *blocs* individuels ?

On a vu plus haut que chaque *bloc* contient:

- des informations concernant une liste de transactions en bitcoins;
- la valeur de *nonce* qui, combinée à ces informations, a permis d'obtenir une *empreinte* constituant une solution valide;
- l'*empreinte* elle-même qui constitue cette solution valide;
- "certaines autres informations".

Parmi ces "autres informations", chaque bloc contient aussi l'*empreinte* du bloc précédent. Les blocs sont ainsi liés entre eux pour former la *chaîne de blocs*. Chaque bloc contient donc:

- une partie explicite de l'historique des transactions en bitcoins: la liste des nouvelles transactions incorporées à ce bloc;

- une partie implicite de l'historique des transactions en bitcoins, puisqu'il contient l'empreinte du bloc précédent, laquelle constitue un "résumé" ou une "signature" de la liste des transactions associées explicitement au bloc précédent.

Le bloc précédent contient lui-même un "résumé" des transactions associées à son prédécesseur, et ainsi de suite. Ces hachages successifs d'informations, constituées elles-mêmes en partie de hachages antérieurs, font boule de neige: chaque *bloc* porte ainsi la trace de toutes les transactions en bitcoins précédentes, depuis l'origine du système. L'historique des transactions est raconté dans cet immense "livre comptable" qu'est la *chaîne de blocs*. Et l'historique des transactions antérieures à chacun des *blocs* est aussi résumé dans chacun de ceux-ci, un peu comme des poupées russes s'emboîtent les unes dans les autres.

À toutes les 10 minutes, l'empreinte-solution qui est trouvée pour le nouveau *bloc* qu'on va ajouter à la *chaîne* est en quelque sorte le "résumé" de toute la chaîne de blocs constituée jusque-là.

3.8. Le mauvais *mineur*

Si un mineur mal intentionné, dans une tentative de fraude, essayait d'altérer une information contenue dans un des blocs de la chaîne, il devrait recalculer l'empreinte du bloc, puisqu'il en aurait changé les données. L'empreinte ne serait plus la même et ne débuterait vraisemblablement plus par le nombre requis de zéros. Il faudrait alors que le mineur fautif cherche par essais et erreur, en modifiant le *nonce*, une empreinte qui constituerait une nouvelle solution valide pour ce bloc altéré: il devrait le *miner* à nouveau.

L'empreinte étant incluse comme une donnée du bloc suivant, l'empreinte du bloc suivant devrait être recalculée à son tour de la même façon, et ainsi de suite. Pendant qu'une armée de mineurs travaille d'arrache-pied à créer le prochain bloc de la chaîne, notre mineur fautif devrait, à partir d'un bloc antérieur altéré, tenter de reconstituer seul tous les blocs déjà incorporés à la chaîne, en aval du bloc altéré.

L'ensemble des mineurs, avec la puissance de calcul totale du réseau, ajoute à la chaîne un bloc valide à toutes les 10 minutes. Un fraudeur qui aurait à sa disposition, par exemple, 10% de la puissance de calcul totale du réseau, aurait besoin de 10 fois plus de temps (100 minutes) pour recréer un seul bloc. Pendant ce temps, les autres mineurs, disposant des 90% restants de la puissance de calcul du réseau, auraient déjà ajouté au moins 9 nouveaux blocs valides à la chaîne. Le tricheur n'arriverait donc jamais à rattraper les autres mineurs au bout de la chaîne pour compléter son méfait et effacer les traces de celui-ci.

3.9. "Utilité" du *minage*: les guillemets enfins expliqués

On affirmait plus haut que tous les mineurs perdants avaient effectué des calculs "inutilement".

On peut s'être demandé pourquoi autant de travail est nécessaire pour créer un nouveau bloc ? Pourquoi exiger tant de calculs qui ressemblent a priori à un passe-temps absurde ? À qui profite ce travail ? N'est-il pas complètement vain et son exigence n'est-elle pas totalement arbitraire ?

Si j'ai réussi à vulgariser assez bien ce que je comprends du bitcoin, il devrait vous apparaître maintenant évident que toute cette charge de travail est un aspect fondamental du système, visant à rendre insurmontable, pour un "tricheur", la tâche consistant à trafiquer toute la chaîne pour en altérer l'historique.

La charge de calcul énorme associée à la *chaîne de blocs* n'est pas un aspect accidentel ou qu'un effet secondaire: il s'agit bien d'une propriété voulue et inhérente au concept, car c'est ce qui vise à garantir l'intégrité des transactions[12]. Alors c'est à cela que "servent" tous ces calculs, toutes ces "énigmes" si difficiles à résoudre.

[12] Le système bitcoin comporte une vulnérabilité qualifiée "d'attaque des 51%". Si une majorité de mineurs se liguaient pour commettre une fraude en altérant la chaîne de blocs, ils pourraient en théorie y parvenir. Cette possibilité n'est pas que théorique, puisqu'un regroupement (*pool*) de mineurs a déjà constitué une majorité (sans nécessairement avoir eu d'intention malveillante), puis a volontairement réduit son influence afin de ne pas compromettre le système.

4. La consommation énergétique du bitcoin

4.1. Estimations de consommation du réseau bitcoin

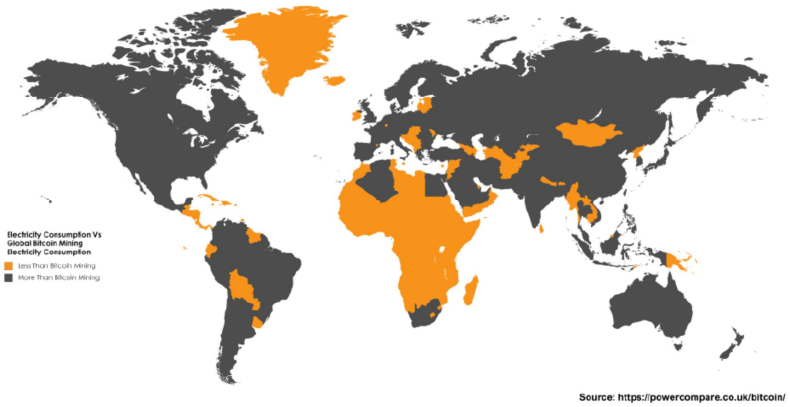
La performance du matériel informatique utilisé par le bitcoin est exprimée en *hashes* (*empreintes*) par seconde (H/s). Au moment d'écrire ces lignes (7 mai 2018), la puissance de calcul totale du réseau bitcoin est estimée[13] à 28 990 958 831 GH/s (près de 29 trillions ou, si vous voulez, plus de 29 milliards de milliards de calculs par seconde).

Personne ne sait réellement exactement combien d'énergie consomme le réseau bitcoin pour effectuer tous ces calculs. Les estimations existantes sont basées sur des hypothèses et ne peuvent donner qu'un ordre de grandeur.

L'estimation la plus connue est le *Bitcoin Energy Consumption Index*, tenu à jour sur le blog *Digiconomist*[14]: la consommation électrique mondiale annuelle du réseau bitcoin y était estimée à **31 térawatts-heures**[15] **(TWh)** au début de décembre 2017 et à **65 TWh** en date du 6 mai 2018.

Pour avoir une idée de la quantité d'énergie que cela représente, il suffit de savoir que les exportations totales nettes d'électricité d'Hydro-Québec (vers l'Ontario, le Nouveau-Brunswick, l'État de New-York, la Nouvelle-Angleterre et ailleurs) s'élevaient à 32.6 TWh en 2016[16].

Un site internet britannique[17] compare cette estimation à la consommation nationale de tous les pays et indique quels pays ont une consommation annuelle inférieure à la consommation annuelle mondiale du réseau bitcoin: en mars 2018, il indiquait que 159 pays consomment chacun moins d'électricité que le bitcoin, comme l'indique la carte ci-contre.



[13] Source: https://blockchain.info/fr/stats (page consultée le 2018/05/07).

[14] https://digiconomist.net/bitcoin-energy-consumption

[15] Un térawatt-heure (10^{12} Wh) équivaut à un milliard de kilowatts-heures (kWh).

[16] http://www.hydroquebec.com/developpement-durable/energie-environnement/marches-exportation.html

[17] https://powercompare.co.uk/bitcoin/

4.2. *Digiconomist*, la source omniprésente d'estimations

Lorsqu'on tente de se renseigner au sujet de la consommation d'énergie du bitcoin, on constate, en lisant attentivement les articles et en remontant aux sources, que la très grande marjorité des estimations citées sur internet (notamment dans des média réputés) proviennent directement ou indirectement de *Digiconomist.* C'est malsain, puisqu'il n'est pas souhaitable de se fier à une source unique.

J'ai donc cherché d'autres sources d'informations à ce sujet et j'ai trouvé diverses études[18], pour la plupart universitaires, qui avancent des estimations plus conservatrices, typiquement dans une fourchette de **1 à 10 TWh par année**. C'est "moins énorme" que 31 ou 65 TWh par année, mais c'est quand même énorme.

Fait intéressant, une de ces estimations provient d'un entrepreneur du bitcoin.[19] On ne pourra sans doute pas l'accuser d'être biaisé en défaveur du bitcoin et de chercher à gonfler son estimation pour donner mauvaise réputation au bitcoin. Il admet que le bitcoin consomme beaucoup d'énergie, mais affirme que cela en vaut la peine. Sa dernière estimation, en date du 11 janvier 2018, s'élève à **18.40 TWh** (valeur la plus probable), à l'intérieur d'une fourchette de **14.19 TWh** à **27.47 TWh**.

4.3. La consommation d'énergie du bitcoin comparée à celle de VISA

Digiconomist compare l'efficacité énergétique des transactions bitcoin (850 kWh / transaction) avec celles des transactions de cartes de crédit VISA (169 kWh par 100 000 transactions ou 0.00169 kWh / transaction)[20]. Une transaction bitcoin consommerait donc en moyenne environ un demi-million de fois plus d'électricité qu'une transaction VISA!

Même si on choisissait de supposer que *Digiconomist* surestime la consommation du réseau bitcoin par un facteur de dix, en se fiant plutôt à des estimations plus conservatrices publiées dans diverses études universitaires, on concluerait quand même qu'une transaction bitcoin consomme près de 50 000 fois plus d'électricité qu'une transaction VISA.

Des défenseurs du bitcoin critiquent cette comparaison en soutenant qu'un réseau de cartes de crédit ne peut fonctionner seul et doit s'appuyer sur un réseau bancaire pour former un système complet de paiement. Il s'agit là d'un argument très juste. Mais la prise en compte de cette réalité ne viendra certainement pas gonfler l'estimation de consommation d'une transaction impliquant à la fois un réseau de cartes de crédit et le réseau bancaire au point de le rendre comparable à celui d'une transaction bitcoin.

---

[18] L'Annexe A présente une liste des autres sources d'informations que j'ai trouvées, avec leurs estimations.

[19] Voir https://bitcoinmagazine.com/articles/op-ed-bitcoin-miners-consume-reasonable-amount-energy-and-its-all-worth-it/ et, **pour ses estimations les plus récentes**, http://blog.zorinaq.com/bitcoin-electricity-consumption/.

[20] Voir https://digiconomist.net/bitcoin-energy-consumption (page consultée le 2018/05/07)

Les objections des défenseurs du bitcoin à une telle comparaison ne doivent pas nous faire perdre de vue qu'on ne débat pas de la différence entre ce qui est *énorme* et ce qui est *raisonnable*, mais bien de la différence entre ce qui est *énorme* et ce qui est *moins énorme*.

4.4. Quelques autres exemples concrets

Les térawatts-heures demeurent abstraits pour bien des gens: ramenons donc les comparaisons à l'échelle humaine. Selon *Digiconomist*, chaque transaction en bitcoins consommerait en moyenne 850 kilowatts-heures (kWh).

Concrètement, l'énergie consommée par une seule transaction permettrait à une Tesla modèle S équipée d'une batterie de 100 kWh de parcourir plus de 5 000 km![21]

Et l'énergie consommée par quarante-sept (47) transactions comblerait amplement, pour une année entière, tous les besoins énergétiques d'une résidence unifamiliale moyenne au Québec[22].

4.5. Critiques de *Digiconomist* et extrapolations farfelues

Sans entrer dans les détails, sachez que certains critiquent l'approche de *Digiconomist* et remettent en question le bien-fondé de sa méthodologie.

Par ailleurs, certaines publications s'appuient sur les estimations de *Digiconomist* pour avancer des extrapolations complètement insensées. Par exemple, le magazine *Newsweek* affirmait en décembre 2017 que, si la tendance se maintient, le réseau bitcoin pourrait consommer, à la fin de 2020, autant d'électricité que le monde entier[23].

Je doute fort qu'on double, d'ici 2020, le nombre de centrales électriques de la planète pour alimenter le réseau bitcoin, ou alors qu'on consacre au réseau bitcoin toute la capacité mondiale actuelle de production d'électricité, ce qui ne nous laisserait que les bougies pour nous éclairer et les poêles à bois pour nos besoins de chauffage.

---

[21] Source: https://www.tesla.com/fr_CA/models : autonomie de 594 km pour le modèle S 100D, à 20°C et 100 km/h; 850 kWh / 100 kWh x 594 km = 5 049 km

[22] Source: http://energie.hec.ca/eeq/ (page 35): un tel ménage moyen consomme 142 GJ par année (données de 2014); or, 1 kWh = 3.6 MJ, donc 47 x 850 kWh = 47 x 850 x 3.6 MJ = 143 820 MJ = 144 GJ.

[23] http://www.newsweek.com/bitcoin-mining-track-consume-worlds-energy-2020-744036

Des extrapolations aussi absurdes sont déplorables, puisqu'elles minent (sans jeu de mots) la crédibilité de ceux qui souhaitent susciter une prise de conscience de la consommation énergétique du bitcoin.

J'espère avoir su faire la part des choses en examinant diverses estimations qui circulent sur internet.

Mais je n'aurais pas su dire a priori qui, de *Digiconomist* ou de ses détracteurs, a raison. Les critiques dont j'ai pris connaissance et le statut de source d'information quasi-unique de *Digiconomist* m'ont fait douter. J'ai donc voulu confirmer autrement qu'une si grande consommation d'énergie était plausible.

4.6. Une autre approche pour "se faire une tête" au sujet des estimations

Peut-on se fier aux estimations qui circulent, si personne ne sait vraiment combien d'énergie consomme le réseau bitcoin ?

Comment savoir qu'il ne s'agit pas d'une autre "fausse nouvelle" ?

Pour dissiper ce doute, examinons des informations bien réelles provenant d'Hydro-Québec.

La moyenne annuelle des surplus d'électricité d'Hydro-Québec est évaluée à 10 TWh pour la période 2017-2026[24] .

Hydro-Québec estime par ailleurs que, si elle devait donner suite à toutes les demandes d'électricité que lui font des entreprises de l'industrie du bitcoin, tous ses surplus y passeraient[25]. Hydro-Québec estime donc qu'elle pourrait trouver preneurs, parmi les *mineurs* ou *fermes* de bitcoins, pour 10 TWh par année.

Hydro-Québec mentionne aussi des projets de *fermes* de bitcoins qui pourraient requérir une puissance aussi élevée que 300 mégawatts[26] (MW), ce qui représente 2.6 TWh par année[27]. Tous ces projets ne seraient pas forcément aussi importants. Mais Hydro-Québec a déjà reçu une centaine[28] de demandes d'approvisionnement de *mineurs* de bitcoins

[24] http://www.ledevoir.com/economie/511863/hydro-quebec-anticipe-que-la-diminution-de-ses-importants-surplus-d-electricite

[25] https://lactualite.com/actualites/2018/02/15/hydro-quebec-pourrait-augmenter-les-tarifs-des-exploitants-de-cryptomonnaies/

[26] http://ici.radio-canada.ca/nouvelle/1085808/cryptomonnais-bitcoins-hydro-quebec-reponse-maire-matane

[27] La puissance est, par définition, la quantité d'énergie qu'on peut fournir (ou consommer) dans un intervalle de temps donné. Sur une période d'un an, l'énergie, exprimée en watts-heures (Wh), est le produit de la puissance, exprimée en watts (W), par 365 x 24 heures.

[28] http://ici.radio-canada.ca/nouvelle/1085808/cryptomonnais-bitcoins-hydro-quebec-reponse-maire-matane

Si, par exemple, cent *fermes* de bitcoins avaient chacune besoin, en moyenne, d'une puissance de "seulement" 11.4 MW (beaucoup moins que 300 MW), la demande totale d'électricité qui en découlerait correspondrait bien à une énergie de 10 TWh par année[29] , soit aux surplus d'Hydro-Québec.

Si Hydro-Québec reçoit de telles demandes, la consommation énergétique énorme du bitcoin n'est sans doute pas une légende urbaine.

Par ailleurs, s'il est possible que des mineurs de bitcoins puissent avoir la capacité de consommer 10 TWh par année au Québec seulement, il n'est pas difficile de croire que la consommation annuelle mondiale d'électricité du bitcoin puisse se chiffrer à plusieurs dizaines de TWh.

Cette analyse très simple me semble donc donner de la crédibilité aux estimations déjà mentionnées de *Digiconomist* :

au 2 décembre 2017: **31 TWh**

au 6 mai 2018:[30] **65 TWh**

[29] 100 mineurs x 11.4 MW/mineur x 365 jours x 24 heures/jour = 10 000 000 MWh ou 10 TWh

[30] https://digiconomist.net/bitcoin-energy-consumption

5. Quelques fausses conceptions voulant justifier le bitcoin énergivore

5.1. Réseau d'échanges entre pairs et élimination des intermédiaires

Quand on fait un virement bancaire, on paie un certain montant à une autre personne, par l'intermédiaire d'une banque, laquelle fait un traitement informatique qui consiste à vérifier que le payeur dispose de fonds suffisants, débiter son compte bancaire du montant de la transaction et créditer d'un même montant le compte bancaire de la personne qui reçoit le paiement. En principe, ce n'est rien de très compliqué.

Ce traitement informatique comporte une séquence d'opérations bien définies qui ne sont effectuées qu'une seule fois par transaction, par un seul intervenant, la banque (à moins bien sûr que plus d'une banque soit impliquée dans la transaction, auquel cas le processus se complexifie, mais quand même pas beaucoup).

On lit souvent que le réseau bitcoin constitue un système d'échange entre pairs (*peer-to-peer*), qui ne nécessite pas l'intervention d'une tierce partie responsable d'assurer l'intégrité de la transaction. Ce serait, selon ses partisans, l'un des avantages du bitcoin.

Je fais une toute autre lecture de la situation. Il me semble qu'au contraire, une transaction en bitcoins entraîne l'intervention non pas d'un seul ou de quelques intermédiaires, comme dans le système bancaire, mais bien de milliers d'intermédiaires, les *mineurs*.

Tous ces intermédiaires font des calculs similaires, très lourds et tout à fait redondants, lesquels n'ont aucune utilité en soi. Leur utilité pour le réseau bitcoin découle de leur simple volume monstrueux, qui rendrait une fraude difficile, voire impossible, à moins de disposer d'une puissance de calcul astronomique.

Le système bancaire repose sur la confiance (ou fiducie) placée dans des intermédiaires comme les banques. On lit parfois que, dans le système bitcoin, la notion de confiance est remplacée par le concept de *preuve de travail*.

5.2. Attrait d'un système monétaire parallèle, indépendant des banques, et illusion d'un système (largement) distribué

Certaines personnes, bien que préoccupées par la consommation énergétique du bitcoin, hésitent à rejeter ce nouveau système auquel est associée la perspective de nous affranchir du système bancaire.

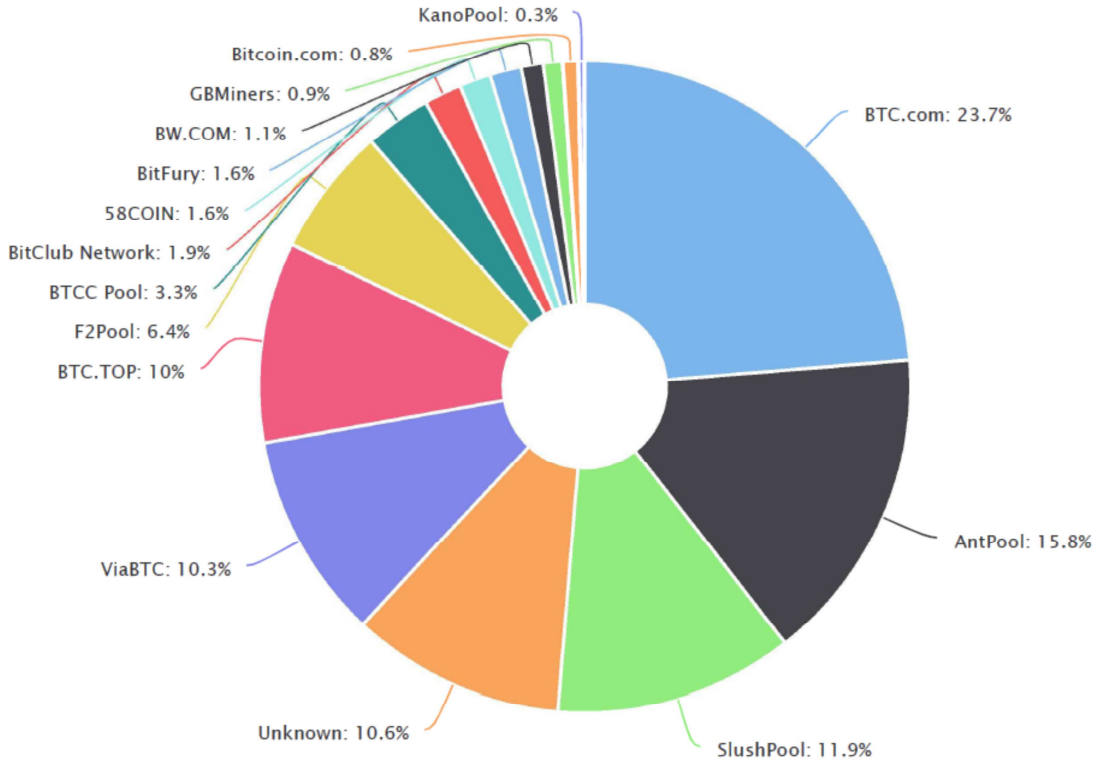
Les banques et autres acteurs du système financier ne sont pas toujours populaires et peuvent être perçus comme des institutions parasites qui exploitent honteusement les individus: "elles *veulent notre bien* et vont tout faire pour l'avoir".

L'augmentation et la multiplication des frais de services des banques, la réduction des services eux-mêmes, les faibles intérêts qu'elles consentent sur les dépôts des épargnants et la rémunération considérable de leurs dirigeants ne sont pas étrangers à une telle perception.

L'image de l'individu qui mine des bitcoins dans son sous-sol, de façon tout à fait indépendante, sans qu'une banque ne puisse venir exiger sa part du gâteau, est bien sympathique. Elle évoque l'utopie d'une démocratisation par laquelle tout le pouvoir financier serait transféré des institutions aux individus, lesquels coopéreraient dans un système conçu pour eux et opéré par eux.

C'est peut-être ce qu'il était encore permis de rêver aux premiers temps du bitcoin (en 2009). Mais la réalité d'aujourd'hui et de demain est tout à fait différente. Le bitcoin n'est pas la "banque du peuple". Ce système, avec les ressources de minage de plus en plus inabordables qu'il requiert, concentre l'influence et les profits entre les mains d'un nombre de plus en plus restreint d'intervenants, en particulier des entreprises privées (les *fermes*), disposant de moyens financiers substantiels, et les *pools* de mineurs.

Le graphique ci-dessous[31] illustre la distribution de la puissance de calcul parmi les *pools* les plus connus. On voit bien à quel point cette puissance de calcul est largement concentrée dans moins d'une dizaine de *pools* dans le monde.



[31] Source: https://blockchain.info/pools (image téléchargée le 2018/03/04).

Les *pools* chinois contrôleraient par ailleurs plus des deux tiers de la puissance mondiale de calcul du réseau bitcoin.[32]

Ces joueurs dominants peuvent par exemple influencer la prise de décisions concernant l'évolution du système bitcoin, avec toutes les implications que cela pourrait avoir pour les diverses parties prenantes (incluant les petits mineurs individuels, s'ils existent encore).

Alors ce système, de moins en moins décentralisé, ne ressemble pas une coopérative de *hackers* joviaux. C'est un système opéré et contrôlé par de très gros joueurs qui s'activent dans un univers parallèle échappant à tout contrôle, avec l'inaction complaisante ou indifférente de la plupart des gouvernements, sauf peut-être ceux de la Chine et de la Corée du Sud, qui commencent à s'inquiéter des impacts économiques et environnementaux du bitcoin.

Je ne m'étendrai pas davantage sur le sujet, car l'objet de ce document est d'expliquer la consommation d'énergie du bitcoin, et non d'énumérer les autres problématiques qui lui sont associées, par ailleurs largement documentées.

Mais cette parenthèse m'apparaissait importante, car les préoccupations environnementales de certaines personnes sont tempérées par une vision romantique de "banque du peuple" qu'il est important de déboulonner.

[32] *Essor des monnaies virtuelles en Chine: les autorités entre défiance et accompagnement* , document du Ministère de l'économie et des finances de la République française, daté du 26 octobre 2017 (https://www.tresor.economie.gouv.fr/Ressources/17989_essor-des-monnaies-virtuelles-en-chine-les-autorites-entre-defiance-et-accompagnement)

6. Conclusion: la pointe de l'iceberg ?

Le bitcoin, avec sa consommation effrénée d'énergie, n'est peut-être que la pointe de l'iceberg d'une nouvelle problématique environnementale majeure, en ce sens qu'il ne constitue que la première application répandue de la technologie de la *chaîne de blocs*.

On recense déjà des dizaines, voire des centaines d'autres cryptomonnaies basées sur la *chaîne de blocs*[33]. (Bien sûr, le bitcoin demeure la plus connue et la plus importante.)

Et les applications envisagées ne se limitent pas aux cryptomonnaies. Au-delà des transactions monétaires associées à celles-ci, les informations qui pourraient être incorporées à des *chaînes de blocs* pour devenir inaltérables vont des documents contractuels aux données de traçabilité des aliments, en passant par des systèmes de messagerie sécurisée, de bulletins de vote électroniques, de passeports, de paiements de droits d'auteurs, etc.[34]

De plus en plus d'entreprises du secteur financier et même d'autres secteurs s'intéressent donc à cette technologie et à ses autres applications potentielles, ce qui n'augure rien de bon pour l'environnement.

Par ailleurs, d'autres technologies développées pour les cryptomonnaies, moins énergivores, seraient en développement. Une autre approche, la *preuve d'enjeu* (*proof of stake*), pourrait éventuellement remplacer la *preuve de travail* associé au *minage.* Selon cette approche, les *mineurs* seraient remplacés par des *foreurs*, et le système délèguerait à un seul *foreur* la responsabilité de *forer* un nouveau bloc. On comprend comment cela pourrait réduire la consommation d'énergie, puisqu'avec le *minage*, des dizaines de milliers de *mineurs* font des calculs semblables simultanément. Certains émettent toutefois des doutes quant à la robustesse de cette approche, en comparaison avec celle du minage.

S'il est possible de rendre les cryptomonnaies moins énergivores, tant mieux. Mais il faudrait alors encore se demander si cette approche a une efficacité énergétique acceptable, compte tenu de ses bénéfices éventuels pour la société. Et nous n'en sommes pas là, puisque c'est toujours le *minage* qui prévaut actuellement et qui prévaudra encore dans un avenir prévisible.

De plus en plus d'acteurs économiques conventionnels (banques, grandes firmes comptables, etc.), qui ne sont ni anonymes ni marginaux, s'intéressent aujourd'hui à la technologie de la *chaîne de blocs* et consacrent des ressources à l'étude de celle-ci, par peur de manquer un train dans lequel tous leurs semblables pourraient embarquer.

Où ce train mènera-t-il la planète ?

---

[33] Wikipedia en recense un nombre surprenant: https://en.wikipedia.org/wiki/List_of_cryptocurrencies.

[34] Voir notamment l'article *How could blockchain be used in the enterprise?* de *Computerworld UK*: https://www.computerworlduk.com/galleries/security/how-could-blockchain-be-used-the-enterprise-3628558/

Annexe A: Estimations de consommation énergétique mondiale annuelle du bitcoin (autres que celles de *Digiconomist*)

Les publications énumérées ci-dessous présentent des valeurs de puissance, d'énergie, ou bien des deux. Lorsque seules des valeurs de puissance étaient indiquées, j'en ai déduit les valeurs d'énergie consommée pendant un an;[35] ces valeurs d'énergie calculées sont présentées en rouge pour indiquer qu'il ne s'agit pas de valeurs explicitement incluses dans les documents cités.

Date	Auteur(s)	Organisation	Puissance estimation inférieure (MW)	Puissance estimation supérieure (MW)	Énergie estimation inférieure (TWh)	Énergie estimation supérieure (TWh)	Titre de la publication (hyperlien)
2014/06/26	O'Dwyer, Karl J. Malone, David	Hamilton Institute, National University of Ireland Maynooth	100 (0.1 GW)	10 000 (10 GW)	0.88	87.60	*Bitcoin Mining and its Energy Footprint* (http://karlodwyer.com/publications/pdf/bitcoin_KJOD_2014.pdf)
septembre 2016	Valfells, Sveinn Egilsson, Jón Helgi	Flux, Ltd. Faculté d'économie, Université d'Islande	160		1.40		*Minting Money with Megawatts* (http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7547426)
2017/03/10	Bevand, Marc	entrepreneur du domaine des cryptomonnaies	1 620	3 136	14.19	27.47	*Electricity consumption of Bitcoin: a market-based and technical analysis* **(voir les estimés du 11 janvier 2018)** (http://blog.zorinaq.com/bitcoin-electricity-consumption/) *Op Ed: Bitcoin Miners Consume A Reasonable Amount of Energy — And It's All Worth It* **(avec estimés antérieurs)** (https://bitcoinmagazine.com/articles/op-ed-bitcoin-miners-consume-reasonable-amount-energy-and-its-all-worth-it/)
2017/03/20	Hileman, Garrick Rauchs, Michel	Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School	232	462	2.03	4.05	*Global Cryptocurrency Benchmarking Study* (https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf)
mai 2017	Vranken, Harald	Faculté de gestion, science et technologie, Université ouverte (*Open Universiteit*) des Pays-Bas	100	500	0.88	4.38	*Bitcoin mining and sustainability: OU scientist internationally in the spotlight* (https://www.ou.nl/en/-/bitcoin-mining-en-duurzaamheid-ou-wetenschapper-internationaal-in-de-belangstelling)

[35] Pour convertir une puissance (exprimée en MW) en énergie consommée pendant un an (exprimée en MWh), il suffit de la multiplier par 365 x 24. On divise ensuite le résultat par 1 000 000 pour passer de MWh à TWh.