21 Leçons

Enseignements tirés de ma chute dans le terrier du lapin Bitcoin

Gigi

21 Leçons
Enseignements tirés de ma chute dans le terrier du lapin Bitcoin
Seconde édition. Version 0.3.12, git commit `8e70090`.

Traduit de l'anglais par Antho / @PrplSknk

a. `https://creativecommons.org/licenses/by-sa/4.0`

Dédié à ma femme, à mon enfant, ainsi qu'à tous les enfants du monde. Puisse Bitcoin vous soutenir et vous apporter la vision d'un futur qui vaille la peine de s'engager.

Avant-propos

Certains appellent ça une expérience mystique. D'autres appellent ça Bitcoin.

J'ai rencontré Gigi pour la première fois dans un de mes foyers spirituels – Riga, Lettonie – patrie de la conférence *The Baltic Honeybadger*, où les plus fervents fidèles de Bitcoin accomplissent un pèlerinage annuel. Après une profonde conversation autour d'un déjeuner, le lien que Gigi et moi avions tissé était aussi immuable qu'une transaction Bitcoin traitée quelques heures plus tôt lorsque nous nous sommes salués.

Mon autre foyer spirituel, Christ Church à Oxford où j'ai eu le privilège d'étudier pour mon MBA, est le lieu où m'est apparue la révélation « terrier du lapin ». Comme Gigi, j'ai transcendé les sphères économiques, techniques et sociales afin de laisser Bitcoin m'envelopper spirituellement. Après avoir « acheté haut » pendant la bulle de novembre 2013, j'ai dû tirer des enseignements très difficiles de l'interminable et destructeur marché baissier de trois ans qui s'ensuivit. Ces 21 leçons m'auraient particulièrement bien aidé à ce moment-là. La plupart sont simplement des vérités naturelles qui, pour le néophyte, sont assombries par un film opaque et fragile. Cependant, d'ici la fin de ce livre, cette façade volera en éclats.

Par une nuit très claire de la fin août 2016 à Oxford, quelques semaines seulement après le piratage de la plateforme d'échange Bitfinex, j'ai fait une halte contemplative au Master's Garden de Christ Church. C'était une période compliquée et j'étais sur le point de craquer psychologiquement et émotionnellement après ce qui m'a paru une éternité de torture. Pas pour les pertes financières, non, mais bien à cause du vide spirituel écrasant

que je ressentais, isolé dans ma vision du monde. Si seulement un livre comme celui-ci avait existé à l'époque, j'aurais pu me rendre compte que je n'étais pas seul. Le Master's Garden est un endroit particulier à mes yeux et aux yeux de beaucoup avant moi au cours des siècles. C'est ici qu'un certain Charles Dodgson, professeur de mathématiques à Christ Church, remarqua l'une de ses jeunes élèves, Alice Liddell, fille du doyen. Dodgson, plus connu sous son nom de plume Lewis Carroll, s'est inspiré d'Alice et du Master's Garden ; et par la magie de ce vénérable gazon, j'ai plongé mon regard dans le crypto-abîme, qui me l'a ardemment rendu, étouffant toute arrogance, giflant mon orgueil en plein visage. J'étais enfin en paix.

21 Leçons vous embarque pour un véritable voyage vers Bitcoin, non seulement philosophique, technologique et économique, mais aussi spirituel.

En se plongeant plus profondément dans la philosophie sobrement exposée dans 7 des 21 Leçons, avec assez de temps et de réflexion, il est possible d'aller jusqu'à comprendre l'origine de toute chose. Ses 7 leçons sur l'économie rendent compte, en des termes simples, de la façon dont nous sommes à la merci d'un petit groupe de chapeliers fous et comment ils ont réussi à nous mettre des œillères dans la tête, dans le cœur et à l'âme. Les 7 leçons sur la technologie décrivent la beauté et la perfection technologiquement darwinienne de Bitcoin. En tant que bitcoiner non technique, ces leçons apportent une étude pertinente sur la nature fondamentalement technologique de Bitcoin et, de fait, sur la nature de la technologie elle-même.

Dans cette expérience éphémère que nous appelons la vie, nous vivons, nous aimons et nous apprenons. Mais qu'est-ce que la vie sinon une suite chronologique d'événements ?

Parvenir au sommet de la montagne Bitcoin n'est pas chose aisée. C'est truffé de faux sommets, le terrain est très accidenté et les crevasses sont omniprésentes, prêtes à vous engloutir. Après

la lecture de ce livre, vous comprendrez que Gigi est le sherpa Bitcoin ultime. Je lui en serai toujours reconnaissant.

Hass McCook
29 novembre 2019

« Voudriez-vous me dire, s'il vous plaît, quel chemin je dois prendre pour m'en aller d'ici ? »

« Cela dépend beaucoup de l'endroit où tu veux aller. »

« Peu m'importe l'endroit… »

« En ce cas, peu importe la route que tu prendras. »

– Lewis Carroll, *Alice au pays des merveilles*

Table des matières

À propos de ce livre (... et de son auteur)

Il s'agit d'un livre un peu particulier. Mais bon, Bitcoin est aussi une technologie un peu particulière, donc un livre particulier à propos de Bitcoin est sans doute adapté. Je ne sais pas vraiment si je suis un mec particulier (j'aime bien penser que je suis un mec *normal*) mais l'histoire de ce livre, et de comment j'en suis venu à devenir auteur, mérite d'être racontée.

Premièrement, je ne suis pas auteur. Je suis ingénieur. Je n'ai pas étudié les lettres. J'ai appris le code et comment coder. Deuxièmement, je n'ai jamais eu l'intention d'écrire un livre, encore moins un livre sur Bitcoin. Bon sang, ce n'est même pas ma langue maternelle. [1] Je suis juste un gars qui a attrapé le virus Bitcoin. Gravement.

Qui suis-*je* alors pour écrire un livre sur Bitcoin ? Bonne question. En bref, la réponse est simple : je suis Gigi et je suis un bitcoiner.

Mais le développement est un peu plus nuancé.

Je viens de l'informatique et du développement logiciel. Dans une vie antérieure, j'étais dans une équipe de recherche qui tentait d'apprendre à penser et à réfléchir à des ordinateurs, entre autres choses. Dans une vie encore plus ancienne, j'écrivais des logiciels de traitement automatisé de passeports et d'autres trucs du même style, ce qui est encore plus effrayant. Je m'y connais

1. La raison pour laquelle j'écris ce livre en anglais, c'est que mon cerveau fonctionne d'une manière bizarre. Dès que ça devient technique, il passe tout seul à l'anglais.

un peu en informatique et en réseaux, donc j'imagine que j'ai quelques longueurs d'avance pour comprendre l'aspect technique de Bitcoin. En revanche, comme j'essaie de le souligner dans ce livre, cet aspect technique ne représente qu'une petite partie de l'animal qu'est Bitcoin. Et chacune de ses parties est importante.

Ce livre a vu le jour grâce à une seule question toute bête : *« Qu'avez-vous appris de Bitcoin ? »*. J'ai tenté d'y répondre d'un simple tweet. Puis le tweet est devenu tempête de tweets. Cette tempête s'est transformée en article. L'article a évolué en trois articles. Trois articles sont devenus 21 leçons. Et 21 leçons ont engendré ce livre. Du coup, je suppose que je suis juste nul pour résumer ma pensée en un seul tweet.

« Pourquoi écrire ce livre ? », me direz-vous. À nouveau, deux réponses : une courte et une longue. La courte, c'est que je devais le faire. J'étais (et suis toujours) *possédé* par Bitcoin. Il ne cesse de me fasciner. Je ne peux m'arrêter de penser à lui et aux implications qu'il aura dans nos sociétés. La réponse longue, c'est que je crois que Bitcoin est l'invention la plus importante de notre époque et que la nature de cette invention doit être comprise par le plus grand nombre. Bitcoin reste l'un des phénomènes les plus mal compris du monde actuel et ça m'a pris des années pour réaliser pleinement le sérieux de cette technologie extraterrestre. Comprendre ce qu'est Bitcoin et comment il va transformer nos sociétés est une expérience marquante. J'ai l'espoir de faire germer dans votre tête les graines qui pourraient vous conduire à cette prise de conscience.

Dans l'ordre des choses, bien que ce passage soit intitulé « *À propos de ce livre (… et de son auteur)* », ce livre, qui je suis et ce que j'ai fait n'ont pas vraiment d'importance. Je suis juste un nœud du réseau, à la fois littéralement *et* métaphoriquement. De toute façon, vous ne devriez pas croire ce que je dis. Comme nous, bitcoiners, aimons le répéter : faites vos propres recherches.

Et par-dessus tout : ne vous fiez pas, vérifiez.

J'ai fait mes recherches au mieux afin de vous permettre, cher lecteur, de vous plonger dans de nombreuses ressources. En plus des notes et des citations de ce livre, j'essaie de garder à jour une liste de contenu sur 21lessons.com/rabbithole et sur bitcoin-resources.com, qui recense également plein d'autres morceaux choisis, livres, podcasts, qui vous aideront à comprendre ce qu'est Bitcoin.

En résumé, c'est juste un livre qui parle de Bitcoin, écrit par un bitcoiner. Bitcoin n'a pas besoin de ce livre, et vous n'avez sans doute pas besoin de ce livre pour comprendre Bitcoin. Je pense que vous comprendrez Bitcoin dès que *vous* serez prêt et je crois aussi que vos premières fractions d'un bitcoin vous trouveront dès que vous serez prêt à les recevoir. Par essence, chacun obtiendra ₿itcoin exactement au bon moment. Dans l'intervalle, Bitcoin existe et c'est bien suffisant. [2]

2. Beautyon, *Bitcoin is. And that is enough.* [8]

Préface

S'enfoncer dans le terrier du lapin Bitcoin est une expérience bizarre. Comme tant d'autres, j'ai l'impression que ces deux dernières années passées à étudier Bitcoin m'ont plus appris que deux décennies d'éducation classique.

Ces leçons forment la quintessence de ce que j'ai découvert. D'abord publié comme une série d'articles intitulée *« Ce que Bitcoin m'a enseigné »*, ce qui suit peut être vu comme la troisième édition de la série d'origine.

À l'instar de Bitcoin, ces leçons sont évolutives. Je compte revenir dessus régulièrement, en publiant plus tard des mises à jour et du contenu supplémentaire.

Contrairement à Bitcoin, les futures versions de ce projet ne seront pas nécessairement rétro-compatibles. Certaines leçons pourront être complétées, d'autres seront retravaillées voire même remplacées.

Bitcoin est un professeur intarissable, c'est pour cela que je ne considère pas ces leçons comme exhaustives ou définitives. Elles sont le reflet de mon propre périple au cœur du terrier. Il existe bien d'autres leçons à tirer, de fait chaque personne qui entrera dans le monde de Bitcoin en retirera des connaissances différentes.

J'espère que vous trouverez une utilité à ces leçons et que leur apprentissage par la lecture vous paraîtra moins pénible et douloureux que je ne l'ai parfois vécu par l'expérience.

21 Leçons

« Ma pauvre Alice, ce que tu peux être sotte ! » se répondit-elle. « Comment pourrais-tu apprendre des leçons ici ? C'est tout juste s'il y a assez de place pour toi, et il n'y en a pas du tout pour un livre de classe ! »

– Lewis Carroll, *Alice au pays des merveilles*

Introduction

> *« Mais je ne veux pas aller parmi les fous, » fit remarquer Alice. « Impossible de faire autrement, » dit le Chat ; « nous sommes tous fous ici. Je suis fou. Tu es folle. » « Comment savez-vous que je suis folle ? » demanda Alice. « Tu dois l'être, » répondit le Chat, « autrement tu ne serais pas venue ici. »*
>
> – Lewis Carroll, *Alice au pays des merveilles*

En octobre 2018, Arjun Balaji posait cette question innocente : *Qu'avez-vous appris de Bitcoin ?* Après avoir essayé d'y répondre en un court tweet, et avoir lamentablement échoué, j'ai compris que ce que j'avais retenu était bien trop riche pour répondre en quelques mots, voire même répondre tout court.

Ces connaissances que j'ai acquises, évidemment, concernent Bitcoin - ou tout du moins lui sont liées. Cependant, bien que certains rouages de Bitcoin soient expliqués ici, les leçons qui suivent ne sont pas une justification du fonctionnement ou de la nature de Bitcoin. Elles pourront néanmoins aider à explorer certains aspects satellites de Bitcoin comme les questions philosophiques, les réalités économiques ou les innovations technologiques.

Les *21 leçons* sont groupées par sept, formant ainsi trois chapitres. Chacun de ces chapitres observe Bitcoin sous une lumière précise, récoltant les enseignements à tirer de l'examen sous différents angles de cet étrange réseau.

Le chapitre 1 explore les enseignements philosophiques de Bitcoin. L'interaction entre immuabilité et changement, le concept de rareté véritable, l'Immaculée Conception de Bitcoin, le problème de l'identité, la contradiction entre réplication et localité, la force de la liberté d'expression et les limites du savoir.

Le chapitre 2 s'intéresse aux enseignements économiques de Bitcoin. Des leçons sur la méconnaissance financière, l'inflation, la valeur, l'argent, son histoire, les réserves fractionnaires des banques ainsi que la manière dont Bitcoin réintroduit la monnaie saine d'une façon rusée et détournée.

Le chapitre 3 présente certaines leçons acquises en examinant la technologie de Bitcoin. Pourquoi les nombres renferment-ils une force, des remarques sur la confiance, pourquoi donner l'heure demande du travail, comment une progression lente et

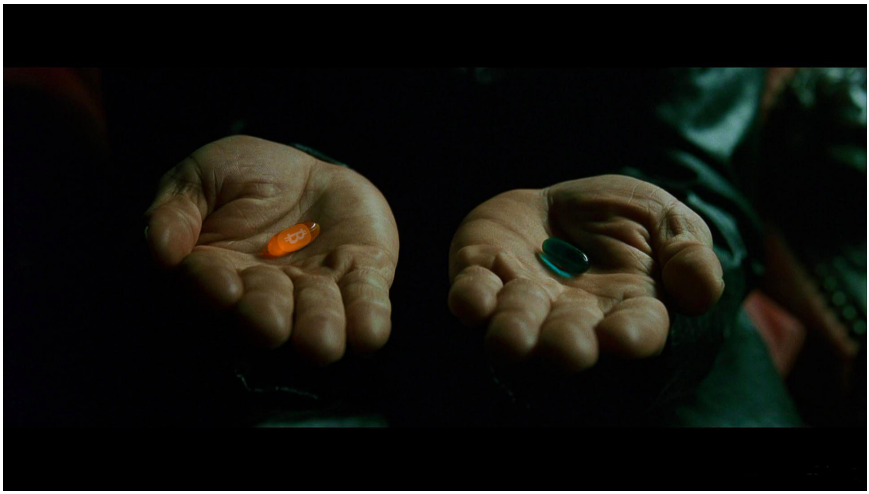
prudente est une fonctionnalité et pas un bug, ce que l'invention de Bitcoin peut nous apprendre sur la vie privée, pourquoi les cypherpunks écrivent-ils du code (et non des lois) et quelles métaphores pourraient être utiles pour imaginer l'avenir de Bitcoin.

Chaque leçon contient plusieurs citations et liens au fil du texte. Si une idée vaut la peine d'être creusée, vous pouvez suivre les liens vers le contenu pertinent dans les notes de bas de page ou la bibliographie.

Bien que quelques connaissances préalables sur Bitcoin puissent aider, j'ai bon espoir que ces leçons pourront être assimilées par tout lecteur curieux. Malgré les liens qui peuvent exister entre elles, chaque leçon devrait se suffire à elle-même et pouvoir être lue indépendamment. J'ai accordé une attention particulière à éviter le jargon technique, malgré cela quelques termes spécifiques à certains domaines restent inévitables.

Je souhaite que mon récit puisse donner l'envie à d'autres personnes de gratter le vernis et d'examiner certaines des questions les plus profondes qu'amène Bitcoin. Ma propre inspiration émane d'une multitude d'auteurs et de créateurs de contenu à qui je voue une éternelle gratitude.

Enfin, et surtout : en écrivant tout ceci mon but n'est pas de vous convaincre de quoi que ce soit. Mon but est de vous amener à penser, de vous montrer que Bitcoin représente bien plus que ce que l'on croit. Je ne peux même pas vous dire ce qu'est Bitcoin ou ce qu'il va vous apprendre. Vous allez devoir le découvrir par vous-même.



Souvenez-vous : je n'offre que la vérité. Rien de plus.

« C'est ta dernière opportunité. Tu ne pourras pas rebrousser chemin. Si tu choisis la bleue, tout s'arrête. Tu te réveilles dans ton lit et tu crois ce que bon te semble. Si tu prends la rouge[3], tu restes aux Pays des Merveilles et je t'emmène au tréfonds du terrier. »

– Morpheus

3. la *orange*

Première partie

Philosophie

Philosophie

> *La Souris la regarda avec curiosité (Alice crut même la voir cligner l'un de ses petits yeux), mais elle ne répondit rien.*
> – Lewis Carroll, *Alice au pays des merveilles*

Si l'on regarde Bitcoin en surface, on pourrait conclure qu'il est lent, inefficace, inutilement redondant et excessivement paranoïaque. Si l'on observe Bitcoin d'un esprit curieux, on pourrait bien découvrir que les choses ne sont pas ce qu'elles paraissent au premier coup d'œil.

Bitcoin a le chic pour mettre vos présomptions sens dessus dessous. Régulièrement, juste au moment où vous alliez retrouver votre zone de confort, Bitcoin viendra à nouveau fracasser vos certitudes comme un éléphant dans un magasin de porcelaine.

Bitcoin est l'enfant de nombreuses disciplines. Tout comme des moines aveugles examinant un éléphant, chaque personne qui approche cette nouvelle technologie le fait sous un angle particulier. Par conséquent, chacun arrivera à différentes conclusions sur la nature de la bête.

Les leçons qui suivent présentent certaines idées préconçues que Bitcoin a fracassées ainsi que les conclusions auxquelles je suis arrivé. Des questions philosophiques à propos de l'immuabilité, de la rareté, de la localité et de l'identité sont abordées au cours des quatre premières leçons. Chaque partie se compose de sept leçons.

FIGURE 0.1. – Moines aveugles examinant le taureau Bitcoin

Partie I – Philosophie :

1. Immuabilité et changement
2. La rareté de la rareté
3. Réplication et localité
4. Le problème de l'identité
5. L'Immaculée Conception
6. La force de la liberté d'expression
7. Les limites du savoir

La leçon 5 s'intéresse à la façon dont l'histoire de Bitcoin est non seulement fascinante mais aussi absolument essentielle à un système sans responsables. Les deux dernières leçons de ce chapitre couvriront la force de la liberté d'expression et les limites de notre savoir individuel, auxquelles la profondeur étonnante du terrier du lapin Bitcoin fait écho.

J'espère que vous trouverez l'univers Bitcoin aussi pédagogique, fascinant et amusant que je l'ai trouvé et que je le trouve encore. Je vous invite à suivre le lapin blanc et à explorer les tréfonds du terrier. Maintenant, accrochez-vous à votre montre à gousset, sautez et profitez de la descente.

1. Immuabilité et changement

> *« Je me demande si on m'a changée pendant la nuit ? Voyons, réfléchissons : est-ce que j'étais bien la même quand je me suis levée ce matin ? Je crois me rappeler que je me suis sentie un peu différente. Mais, si je ne suis pas la même, la question qui se pose est la suivante : Qui diable puis-je bien être ? Ah, c'est là le grand problème ! »*
>
> – Alice

Bitcoin est fondamentalement difficile à décrire. C'est un *truc nouveau*, donc chaque tentative de comparaison à des concepts antérieurs – y compris l'appeler or numérique ou Internet de l'argent – est condamnée à ne pas pouvoir rendre compte de son entièreté. Quelle que soit votre analogie favorite, il y a deux aspects de Bitcoin réellement essentiels : la décentralisation et l'immuabilité.

On peut voir Bitcoin comme un contrat social automatisé [1]. Le logiciel est juste une des pièces du puzzle, de sorte que vouloir changer Bitcoin en changeant le logiciel est absolument futile. Il faudrait pour cela convaincre l'ensemble du réseau d'adopter les changements, ce qui tient plus de l'effort psychologique que de l'effort d'ingénierie.

Ce qui suit peut sembler absurde au départ, comme tant d'autres choses dans ce domaine, mais je crois fermement en la

1. Hasu, Unpacking Bitcoin's Social Contract [32]

vérité de cette maxime : ce n'est pas vous qui changerez Bitcoin, c'est Bitcoin qui vous changera.

> « Bitcoin nous changera plus que nous ne le changerons. »
>
> – Marty Bent [2]

Ça m'a pris un bon moment pour comprendre la profondeur de cette phrase. Après tout, comme Bitcoin est juste un logiciel et qu'il est entièrement libre, on peut simplement changer les choses à volonté, non ? Faux. *Totalement* faux. Sans surprise, l'inventeur de Bitcoin le savait parfaitement.

> « La nature de Bitcoin est telle qu'une fois sortie la version 0.1, les concepts essentiels étaient gravés dans le marbre pour le restant de ses jours. »
>
> – Satoshi Nakamoto [3]

De nombreuses personnes ont tenté de modifier la nature de Bitcoin. Elles ont toutes échoué jusqu'à présent. Bien qu'il existe une étendue infinie de forks et d'altcoins, le réseau Bitcoin continue sa route, exactement comme à la mise en ligne du prenier nœud. Les altcoins n'importent pas sur le long terme. Les forks finiront par mourir de faim. Ce qui importe c'est Bitcoin. Tant que notre compréhension fondamentale des mathématiques et/ou de la physique ne change pas, le ratel Bitcoin continuera de s'en moquer.

2. Tales From the Crypt [10]
3. Message du forum BitcoinTalk : 'Re : Transactions and Scripts. . .' [56]

> « Bitcoin est le premier exemple d'une nouvelle forme de vie. Il vit et respire sur internet. Il vit car il est capable de payer des gens pour le maintenir en vie. [...] Il ne peut être changé. On ne peut le contredire. On ne peut l'altérer. On ne peut le corrompre. On ne peut l'arrêter. [...] Si une guerre nucléaire détruisait la moitié de la planète, il continuerait à vivre, intact. »
>
> – Ralph Merkle [4]

Le cœur de Bitcoin battra plus longtemps que tous les nôtres.

Comprendre tout ça m'a fait changer bien plus que ne le feront les précédents blocs de Bitcoin. Ma préférence temporelle a été modifiée, ma compréhension de l'économie, mes opinions politiques et bien plus encore. Mince, ça change même le régime alimentaire des gens [5]. Si tout ça vous semble dingue, vous êtes au bon endroit. Tout ceci est dingue en effet ; et c'est pourtant ce qui se passe.

Bitcoin m'a appris qu'il ne changerait pas. C'est moi qui changerai.

4. DAOs, Democracy and Governance, [44]
5. Inside the World of the Bitcoin Carnivores, [58]

2. La rareté de la rareté

> *« Cela suffit comme cela... J'espère que je ne grandirai plus... »*
>
> – Alice

Généralement, le progrès technologique semble rendre les choses plus abondantes. Ce qui était auparavant un produit de luxe devient accessible à de plus en plus de gens. Bientôt, nous vivrons tous comme des rois. C'est déjà le cas pour la plupart d'entre nous. Comme l'écrivait Peter Diamandis dans Abundance [23] : « La technologie est un mécanisme de libération des ressources. Elle peut rendre abondant ce qui était rare. »

Bitcoin, en tant que technologie avancée, casse cette tendance et crée une nouvelle ressource authentiquement rare. Certains avancent même que c'est l'une des ressources les plus rares de l'univers. L'offre ne peut pas grossir, quels que soient les efforts déployés pour y parvenir.

> « Il n'y a que deux choses véritablement rares : le temps et Bitcoin. »
>
> – Saifedean Ammous [1]

Paradoxalement, ceci se produit par un mécanisme de réplication. Les transactions sont diffusées, les blocs se propagent, le registre distribué est – vous l'avez deviné – distribué. Mais ce ne sont que des mots savants pour désigner la copie. Bon sang, Bitcoin se réplique même tout seul sur autant d'ordinateurs que possible, en incitant les gens à exécuter des nœuds complets et à miner de nouveaux blocs.

1. Présentation sur The Bitcoin Standard [2]

Toute cette réplication œuvre magnifiquement de concert en vue de produire de la rareté.

En ces temps d'abondance, Bitcoin m'a appris ce qu'était la véritable rareté.

3. Réplication et localité

> *Ensuite résonna une voix furieuse, celle du Lapin, en train de crier : « Pat ! Pat ! Où es-tu ? »*
> – Lewis Carroll, *Alice au pays des merveilles*

Si l'on met de côté la mécanique quantique, la localité au sein du monde physique n'est pas un problème. La question *« Où se trouve X ? »* trouve une réponse sensée, peu importe si X est une personne ou un objet. Dans le monde numérique, la question du *où* est déjà délicate en soi mais on peut potentiellement y répondre. Sans rire, où sont situés vos e-mails ? « Le cloud » serait une mauvaise réponse, c'est juste l'ordinateur de quelqu'un d'autre. Pourtant, si vous vouliez situer chaque stockage contenant une copie de vos e-mails, en théorie, vous pourriez.

Avec Bitcoin, la question du « où » est *vraiment* délicate. Où sont situés vos bitcoins, exactement ?

> « J'ai ouvert les yeux, regardé autour de moi et j'ai posé l'inévitable, la sempiternelle, la tristement banale question postopératoire : 'Où suis-je ?' »
>
> – Daniel Dennett [1]

C'est un double problème : d'abord, le registre distribué l'est par réplication totale, ce qui signifie que le registre est partout. Deuxièmement, les bitcoins n'existent pas. Pas seulement physiquement, non, *techniquement* aussi.

1. Daniel Dennett, *Where Am I ?* [21]

Bitcoin gère un ensemble de transactions sortantes non-dépensées, sans jamais devoir mentionner une quelconque entité représentant un bitcoin. L'existence d'un bitcoin se déduit en observant cet ensemble de transactions, tout en désignant comme bitcoin chaque entrée totalisant 100 millions d'unités de base.

> « Où est-il pendant le transfert, à ce moment ? [...] Premièrement, il n'y a pas de bitcoins. Il n'y en a simplement pas. Ils n'existent pas. Il y a des entrées dans un registre qui est partagé [...] Il n'existent dans aucun lieu physique. Le registre lui existe partout, en gros. La géographie n'a pas de sens ici ; ça ne vous aidera pas à définir votre politique. »
>
> – Peter Van Valkenburgh [2]

Par conséquent, que détenez-vous vraiment lorsque vous dites *« j'ai un bitcoin »*, s'ils n'existent pas ? Eh bien, vous vous souvenez de tous ces mots étranges que le portefeuille que vous utilisez vous a forcé à écrire ? Ce que vous détenez ce sont justement ces mots sorciers : une formule magique [3] qui sert à ajouter des entrées dans le registre public ; les clés qui permettent de « déplacer » des bitcoins. À toutes fins utiles, c'est pour ça que vos clés privées *sont* vos bitcoins. Si vous vous dites que j'invente tout ça, n'hésitez pas à m'envoyer vos clés privées.

Bitcoin m'a appris que la localité était une histoire complexe.

2. Peter Van Valkenburgh dans le podcast *What Bitcoin Did*, épisode 49 [73]

3. The Magic Dust of Cryptography : Comment l'information numérique change notre société [30]

4. Le problème de l'identité

« Qui es-tu ? » lui demanda-t-elle.
– Lewis Carroll, *Alice au pays des merveilles*

Nic Carter, en hommage à Thomas Nagel qui posait cette même question à propos des chauve-souris, a écrit un excellent article sur la question : quel effet cela fait-il d'être un bitcoin ? Il y montre remarquablement qu'en général, les blockchains publiques et ouvertes, et Bitcoin plus particulièrement, souffrent du même dilemme que le bateau de Thésée [1] : quel Bitcoin est le vrai Bitcoin ?

> « Observez par exemple comment les éléments de Bitcoin font preuve de peu de persistance. L'ensemble du code source a déjà été retravaillé, modifié et étendu tant et si bien qu'il ne ressemble que difficilement à sa version d'origine. [...] Les archives de qui possède quoi, le registre lui-même, est virtuellement la seule caractéristique persistante du réseau [...] Afin d'être vraiment perçu sans responsable, il faut tourner le dos à cette solution simple qui consiste à ce qu'une entité puisse désigner une chaîne comme étant la chaîne légitime. »
>
> – Nic Carter [2]

Il semble que le progrès technologique nous force sans arrêt à prendre au sérieux ces considérations philosophiques. Un jour

1. Dans la métaphysique de l'identité, le bateau de Thésée est une expérience de pensée qui soulève la question de savoir si un objet dont toutes les parties ont été remplacées reste fondamentalement le même objet. [98]
2. Nic Carter, *Quel effet cela fait-il d'être un bitcoin ?* [19]

ou l'autre, les voitures autonomes feront face au dilemme du tramway de façon bien réelle, ce qui les obligera à prendre des décisions d'ordre éthique sur quelles vies comptent et quelles vies ne comptent pas.

Les cryptomonnaies, particulièrement depuis le premier hard-fork litigieux, nous forcent à réfléchir et à se mettre d'accord sur la métaphysique de l'identité. Il est intéressant de constater que les deux meilleurs exemples que nous avons connu jusqu'à présent ont mené à deux réponses différentes. Le premier août 2017, Bitcoin se sépara en deux camps. Le marché décida que la chaîne inchangée était le Bitcoin originel. Un an plus tôt, le 25 octobre 2016, Ethereum se séparait en deux camps. Le marché décidait que la chaîne *modifiée* était l'Ethereum originel.

Aussi longtemps que ces réseaux de transfert de valeur existeront, pour peu qu'ils soient correctement décentralisés, les questions posées par le *bateau de Thésée* devront sans cesse trouver des réponses.

Bitcoin m'a appris que la décentralisation entrait en contradiction avec l'identité.

5. L'Immaculée Conception

> *« Leur tête a disparu, [...] » répondirent les soldats.*
> – Lewis Carroll, *Alice au pays des merveilles*

Ça parle à tout le monde lorsqu'une belle histoire donne lieu à une naissance. Celle de Bitcoin est fascinante et ses détails sont plus importants qu'on pourrait le croire à première vue. Qui est Satoshi Nakamoto ? Était-ce une seule personne ou un groupe ? Était-ce un homme ou une femme ? Un extraterrestre qui aurait voyagé dans le temps, ou une intelligence artificielle avancée ? Sans tenir compte des théories absurdes, nous ne le saurons sans doute jamais. Et ça a toute son importance.

Satoshi a choisi de rester anonyme. Il a fait germer la graine de Bitcoin. Il est resté dans le coin suffisamment longtemps pour s'assurer que le réseau ne connaîtrait pas une mort prématurée. Et il s'est évaporé.

Ce qui peut sembler une étrange pirouette à propos de l'anonymat est en réalité une chose cruciale pour qu'un système soit vraiment décentralisé. Pas de contrôle centralisé. Pas d'autorité centrale. Pas d'inventeur identifié. Personne à poursuivre, à torturer, à faire chanter ou à extorquer. L'Immaculée Conception d'une technologie.

> « L'une des meilleures choses que Satoshi ait faites a été de disparaître. »
>
> – Jimmy Song [1]

1. Jimmy Song, *Pourquoi Bitcoin est différent* [67]

Depuis la naissance de Bitcoin, des milliers d'autres cryptomonnaies ont été créées. Aucun de ces clones ne partage l'histoire de sa naissance. Si vous voulez remplacer Bitcoin, vous allez devoir transcender cette histoire. Dans une guerre d'idées, le récit impose la survie.

> « L'or a d'abord été travaillé sous forme de bijoux et utilisé pour le troc il y a plus de 7000 ans. L'éclat captivant de l'or l'a mené à être considéré comme un cadeau des dieux. »
>
> Austrian Mint [2]

Comme l'or il y a bien longtemps, Bitcoin pourrait être perçu comme un cadeau des dieux. Mais contrairement à l'or, les origines de Bitcoin sont très humaines. Et cette fois, nous connaissons les dieux du développement et de la maintenance : des gens du monde entier, anonymes ou pas.

Bitcoin m'a appris que le narratif était important.

2. The Austrian Mint, *Gold : The Extraordinary Metal* [46]

6. La force de la liberté d'expression

> *« Je te demande pardon ! » dit la Souris très poliment, mais en fronçant le sourcil. « Tu as dit quelque chose ? »*
> – Lewis Carroll, *Alice au pays des merveilles*

Bitcoin est une idée. Une idée qui, dans sa forme actuelle, est la manifestation de rouages purement alimentés par du texte. Tous les aspects de Bitcoin sont du texte : le livre blanc, c'est du texte. Le logiciel qui s'exécute sur les nœuds, c'est du texte. Le registre, c'est du texte. Les transactions, ce sont du texte. Les clés publiques et privées, ce sont du texte. Tous les aspects de Bitcoin sont du texte, en conséquence ils sont équivalents à de la parole.

> « Le Congrès n'adoptera aucune loi relative à l'établissement d'une religion, ou à l'interdiction de son libre exercice ; ou pour limiter la liberté d'expression, de la presse ou le droit des citoyens de se réunir pacifiquement ou d'adresser au Gouvernement des pétitions pour obtenir réparations des torts subis. »
>
> – Premier amendement de la Constitution des États-Unis

Bien que la bataille finale des Crypto Wars [1] n'ait pas encore été livrée, il sera extrêmement difficile de criminaliser une idée, qui plus est une idée basée sur l'échange de messages écrits. Chaque fois qu'un gouvernement tente d'interdire du texte ou de

1. Les *Crypto Wars* est le nom officieux des tentatives par les États-Unis et les gouvernements alliés de saboter le chiffrement des données. [26] [78]

la parole, nous glissons sur le chemin de l'absurdité qui mène inévitablement aux abominations telles que les nombres illégaux [2] et les nombres premiers illégaux [3].

Tant que quelque part dans le monde, l'expression restera libre comme dans *liberté*, Bitcoin sera inarrêtable.

> « Il n'y a aucun moment lors d'une transaction où Bitcoin ne cesse d'être du *texte*. Ce n'est *que du texte*, tout le temps. [...] Bitcoin, c'est du *texte*. Bitcoin, c'est de la *parole*. Il ne peut pas être réglementé dans un pays libre tel que les États-Unis qui possède des droits inaliénables garantis et un premier amendement qui retire explicitement le droit de publier du contrôle du gouvernement. »
>
> – Beautyon [4]

Bitcoin m'a appris que dans une société libre, la liberté d'expression et le logiciel libre étaient inarrêtables.

2. Un nombre illégal est un nombre qui représente une information qu'il est interdit de posséder, prononcer, diffuser ou transmettre dans une juridiction légale donnée.[84]

3. Un nombre premier illégal est un nombre premier qui représente une information dont la possession ou la distribution est interdite dans une quelconque juridiction légale. L'un des premiers nombres premiers illégaux fut découvert en 2001. Lorsqu'interprété d'une façon particulière, il décrit un programme informatique qui permet de contourner le système de gestion des droits numériques sur les DVD. La distribution d'un tel programme aux États-Unis est illégale selon le Digital Millennium Copyright Act. Un nombre premier illégal est une sorte de nombre illégal.[85]

4. Beautyon, *Pourquoi l'Amérique ne peut réglementer Bitcoin* [7]

7. Les limites du savoir

« Plus bas, encore plus bas, toujours plus bas. Est-ce que cette chute ne finirait jamais ? »
– Lewis Carroll, *Alice au pays des merveilles*

S'embarquer dans Bitcoin est une expérience humiliante. Je croyais que je savais des trucs. Je pensais que j'étais instruit. Au minimum, je tenais ce que j'avais appris en informatique pour acquis. J'ai étudié pendant des années, alors je dois à peu près tout savoir sur les signatures numériques, le hachage, le chiffrement, la sécurité opérationnelle et les réseaux, non ?

Faux.

C'est difficile d'étudier tous les fondamentaux qui rendent le fonctionnement de Bitcoin possible. C'est limite impossible de tous les comprendre en profondeur.

« Personne n'a atteint le fond du terrier du lapin Bitcoin. »

– Jameson Lopp [1]

Ma liste de livres à lire ne cesse de s'agrandir bien plus vite que je ne suis capable de la faire fondre. La liste de documents et d'articles à lire est virtuellement infinie. Il y a bien plus de podcasts sur tous ces sujets que je ne pourrais jamais en écouter. C'est réellement humiliant. En plus, Bitcoin continue d'évoluer et il est presque impossible de suivre le rythme de l'innovation

1. Jameson Lopp, tweet du 11 novembre 2018 [41]

FIGURE 7.1. – Le terrier du lapin Bitcoin n'a pas de fond.

qui s'accélère. La poussière soulevée par la première couche du réseau n'a même pas encore fini de retomber, que des gens ont déjà construit la seconde et travaillent sur la troisième.

Bitcoin m'a appris que je savais très peu sur presque tout. Il m'a appris que ce terrier de lapin n'avait pas de fond.

Deuxième partie

Économie

Économie

> *« Un grand rosier se dressait près de l'entrée du jardin ; il était tout couvert de roses blanches, mais trois jardiniers s'affairaient à les peindre en rouge. Ceci sembla très curieux à Alice… »*
>
> – Lewis Carroll, *Alice au pays des merveilles*

L'argent ne pousse pas sur les arbres. C'est idiot de croire ça et nos parents ont fait en sorte de nous l'inculquer en le répétant comme un mantra. Nous sommes encouragés à utiliser judicieusement l'argent, à ne pas le dépenser inconsidérément et à l'épargner quand tout va bien pour les mauvais moments. Après tout, l'argent ne pousse pas sur les arbres.

Bitcoin m'a plus appris sur l'argent que ce que j'aurais jamais cru devoir savoir. Grâce à lui, j'ai été forcé d'explorer l'histoire de l'argent, du secteur bancaire, diverses écoles de pensée économique et bien d'autres choses. La quête pour la compréhension de Bitcoin m'a mené sur une multitude de chemins et je tente d'en explorer certains au long de ce chapitre.

Dans les sept premières leçons j'ai abordé certaines questions philosophiques qui entourent Bitcoin. Les sept suivantes se pencheront plutôt sur l'argent et l'économie.

Partie II – Économie :

8. La méconnaissance financière
9. L'inflation
10. La valeur
11. L'argent
12. L'histoire et le déclin de la monnaie
13. La folie des réserves fractionnaires
14. Une monnaie saine

À nouveau, je ne pourrai qu'effleurer la surface. Bitcoin est non seulement ambitieux, mais il couvre aussi profondément un large spectre de domaines, rendant impossibles à balayer tous les sujets pertinents en une seule leçon, un seul essai, article ou livre. Je doute même que ce soit tout simplement possible.

Bitcoin est une nouvelle forme de monnaie, qui rend l'étude de l'économie primordiale à sa compréhension. S'agissant de la nature humaine et des interactions entre agents économiques, l'économie est sans doute l'une des pièces les plus grandes et les plus floues du puzzle Bitcoin.

À nouveau, ces leçons explorent diverses choses que Bitcoin m'a apprises. Elles sont un reflet de ma chute dans le terrier du lapin. N'ayant pas de formation en économie, je suis clairement en-dehors de ma zone de confort et je suis tout à fait conscient que ma compréhension est potentiellement incomplète. Je ferai de mon mieux pour présenter ce que j'ai retenu, au risque même de passer pour un idiot. Après tout, je cherche toujours à répondre à la question : *« Qu'avez-vous appris de Bitcoin ? »*

Après sept leçons observées sous l'angle de la philosophie, passons à l'angle de l'économie pour en examiner sept de plus. Tout ce que j'ai à vous offrir cette fois, c'est un cours d'économie. Terminus : *une monnaie saine.*

8. La méconnaissance financière

> *« Et la dame pensera que je suis une petite fille ignorante ! Non, il vaudra mieux ne rien demander ; peut-être que je verrai le nom écrit quelque part. »*
> – Lewis Carroll, *Alice au pays des merveilles*

L'une des choses qui m'a le plus frappé, c'est la quantité de finance, d'économie et de psychologie nécessaire à la compréhension de ce qui semble, à première vue, un système purement *technique* – un réseau informatique. Pour paraphraser un petit gars aux pieds poilus : « Il est fort dangereux, Frodon, d'étudier Bitcoin. On lit le livre blanc et si l'on ne regarde pas où l'on met les pieds, on ne sait pas jusqu'où cela peut nous mener. »

Pour comprendre un nouveau système monétaire, il faut apprendre à connaître l'ancien. J'ai très vite réalisé que la quantité d'éducation financière reçue au sein du système scolaire était à peu près égale à *zéro*.

Comme un enfant, j'ai commencé à me poser bon nombre de questions : comment fonctionne le système bancaire ? Comment fonctionnent les marchés financiers ? Qu'est-ce que la monnaie fiduciaire ? Qu'est-ce que la monnaie *normale* ? Pourquoi existe-t-il autant de dette ? [1] Combien de monnaie est véritablement émise, et qui décide de ça ?

1. `https://www.usdebtclock.org/`

Après une légère panique face à l'ampleur de mon ignorance, je me suis senti rassuré lorsque j'ai constaté que j'étais en bonne compagnie.

> « C'est pas ironique que Bitcoin m'en ait appris plus sur la monnaie que toutes ces années à travailler pour des institutions financières ? ... y compris en ayant commencé dans une banque centrale »
>
> – Aaron [2]

> « J'ai plus appris sur la finance, l'économie, la technologie, la cryptographie, la psychologie, la politique, la théorie des jeux, la législation et moi-même pendant les trois derniers mois dans la crypto que mes trois années et demie d'université »
>
> – Dunny [3]

Deux exemples des nombreuses confessions que l'on trouve un peu partout sur Twitter [4]. Bitcoin, comme nous l'avons vu dans la Leçon 1, est un organisme vivant. Mises prétendait que l'économie aussi est vivante. Et nous le savons tous par expérience, le vivant est difficile à appréhender par nature.

> « Un système scientifique est simplement une étape atteinte dans la recherche indéfiniment continuée de la connaissance. Il est forcément affecté par l'imperfection inhérente à tout effort humain. Mais reconnaître ces faits ne signifie pas que la science économique de notre temps soit arriérée. Cela veut dire seulement qu'elle est chose vivante, et vivre implique à la fois imperfection et changement. »
>
> – Ludwig von Mises [5]

---

2. Aaron (`@aarontaycc`, `@fiatminimalist`), tweet du 12 déc. 2018 [45]
3. Dunny (`@BitcoinDunny`), tweet du 28 nov. 2017 [24]
4. Voir `http://bit.ly/btc-learned` pour plus de confessions Twitter.
5. Ludwig von Mises, *L'Action Humaine* [74]

On voit tous passer des articles sur diverses crises financières, en se demandant comment ces grands sauvetages fonctionnent et nous restons perplexes face à l'absence de responsable de ces milliers de milliards de dégâts. Je reste perplexe, mais au moins je commence à entrevoir ce qui se passe dans le monde de la finance.

Certaines personnes vont jusqu'à attribuer la méconnaissance générale de ces sujets à une méconnaissance plus systémique et délibérée. Tandis que l'histoire, la physique, la biologie, les maths et les langues font toutes partie de notre cursus, l'univers monétaire et financier n'est étonnamment abordé qu'en surface, voire pas du tout. Je me demande si les gens continueraient d'accroître la dette autant qu'ils le font si nous étions tous éduqués sur la gestion personnelle et les rouages de la monnaie et du crédit. Puis je réfléchis à combien de couches d'aluminium feraient un bon chapeau. Trois, probablement.

> « Ces crashs, ces sauvetages, ce ne sont pas des accidents. Et ce n'est pas non plus par accident qu'il n'y a pas d'éducation financière à l'école. [...] C'est prémédité. Comme avant la Guerre Civile où il était illégal d'instruire un esclave, nous n'avons pas le droit d'étudier la monnaie à l'école. »
>
> – Robert Kiyosaki [6]

Comme dans Le Magicien d'Oz, on nous demande de ne pas prêter attention à l'homme derrière le rideau. Contrairement au Magicien d'Oz, nous possédons maintenant une véritable sorcellerie [7] : un réseau de transfert de valeur, résistant à la censure, ouvert et sans frontières. Il n'y a pas de rideau et chacun peut en apprécier la magie [8].

---

6. Robert Kiyosaki, *Pourquoi les riches deviennent encore plus riches*[39]

7. `http://bit.ly/btc-wizardry`

8. `https://github.com/bitcoin/bitcoin`

Bitcoin m'a appris à regarder derrière le rideau et à surmonter ma méconnaissance financière.

9. L'inflation

> *« Ici, vois-tu, on est obligé de courir tant qu'on peut pour rester au même endroit. Si on veut aller ailleurs, il faut courir au moins deux fois plus vite que ça ! »*
>
> – La Reine Rouge

Tenter de comprendre l'inflation monétaire et comment un système désinflationniste tel que Bitcoin pourrait changer nos comportements a constitué le début de ma plongée dans l'économie. Je savais que l'inflation était le taux auquel la monnaie était nouvellement émise, mais je n'en savais pas beaucoup plus que ça.

Tandis que certains économistes prétendent que l'inflation est bonne, d'autres prétendent qu'une monnaie « dure » qui ne peut être facilement produite — comme nous avions durant la période de l'étalon-or — est indispensable à une économie saine. Bitcoin, avec son offre fixe de 21 millions, partage l'avis du second camp.

Habituellement, les effets de l'inflation ne sautent pas aux yeux. Selon le taux d'inflation (ainsi que d'autres facteurs), le délai entre la cause et la conséquence peut s'étendre sur plusieurs années. De plus, l'inflation touche certaines catégories plus que d'autres. Comme Henry Hazlitt le fait remarquer dans *L'Économie Politique en Une Leçon* : « L'art de la politique économique consiste à ne pas considérer uniquement l'aspect immédiat d'un problème ou d'un acte, mais à envisager ses effets plus lointains ; il consiste essentiellement à considérer les conséquences que cette politique peut avoir, non seulement sur un groupe d'hommes ou d'intérêts donnés, mais sur tous les groupes existants. »

L'une de mes révélations fut le moment où j'ai compris que l'émission monétaire — imprimer plus d'argent — était une activité économique *totalement* différente de toutes les autres activités économiques. Pendant que les vrais biens et services produisent de la vraie valeur pour les vrais gens, imprimer plus d'argent a l'exact effet contraire : on retire de la valeur à tous ceux qui détiennent cette monnaie dont la quantité augmente.

> « L'inflation en soi — c'est-à-dire la simple émission de plus de monnaie, avec pour conséquences la hausse des salaires et l'accroissement des prix — peut très bien avoir l'air de créer une demande supplémentaire. Mais si on raisonne en termes de production et d'échange des biens réels, il n'en est rien. »
>
> – Henry Hazlitt [1]

La force destructrice de l'inflation devient évidente dès qu'un peu d'inflation se change en *beaucoup*. Si la monnaie subit une hyperinflation, les choses tournent au vinaigre très rapidement [2]. Au fur et à mesure qu'une monnaie se désagrège, elle échouera à stocker la valeur à travers le temps et les gens se précipiteront pour mettre la main sur n'importe quel bien qui pourra y parvenir.

Une autre conséquence de l'hyperinflation, c'est que tout l'argent épargné par les gens durant leur vie va littéralement s'évaporer. L'argent liquide qui se trouve dans votre portefeuille sera toujours là, bien entendu. Mais ça ne sera effectivement plus que ça : du papier sans valeur.

La monnaie perd également de la valeur avec une inflation soi-disant « modérée ». C'est juste qu'elle arrive suffisamment

1. Henry Hazlitt, *L'Économie Politique en Une Leçon* [35]
2. `https://en.wikipedia.org/wiki/Hyperinflation`[83]

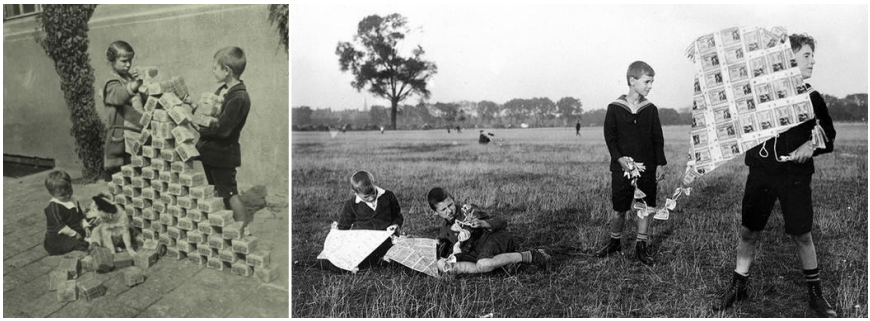


FIGURE 9.1. – Hyperinflation pendant la République de Weimar (1921-1923)

lentement pour que la plupart des gens ne s'aperçoivent pas de la baisse de leur pouvoir d'achat. Et dès lors que la planche à billets tourne, la quantité de monnaie peut être facilement accrue et ce qui était auparavant une inflation modérée peut se transformer par l'appui d'une simple bouton en une bonne dose d'inflation bien forte. Friedrich Hayek le faisait remarquer dans l'un de ses essais, l'inflation modérée mène généralement à l'inflation pure et simple.

> « Une inflation 'modérée' et stable ne peut pas nous aider — cela peut seulement mener à l'inflation totale. »
>
> – Friedrich Hayek [3]

L'inflation est particulièrement sournoise, puisqu'elle favorise ceux qui sont au plus près du procédé d'émission. Il faut du temps pour que la monnaie nouvellement émise circule et que les prix s'ajustent. Donc si vous avez la possibilité de mettre la main sur plus d'argent avant que celui des autres ne se dévalue, vous avez de l'avance sur la courbe d'inflation. C'est aussi pour ça que l'on peut voir l'inflation comme un impôt caché, car au

3. Friedrich Hayek, *Le chômage des années 80 et les syndicats* [33]

final ce sont les gouvernements qui en profitent tandis que tout le monde en paye le prix.

> « Je ne pense pas que cela soit une exagération de dire que l'Histoire est largement une histoire d'inflation, une inflation habituellement fabriquée par les gouvernements, pour le gain des gouvernements. »
>
> – Friedrich Hayek [4]

Jusqu'à présent, les devises contrôlées par les gouvernements ont toutes fini par être remplacées ou s'effondrer totalement. Peu importe la faiblesse du taux d'inflation, parler de croissance « stable » revient à parler de croissance exponentielle. Dans la nature comme en économie, tous les systèmes qui se développent de façon exponentielle devront se stabiliser sous peine de subir un effondrement catastrophique.

« Ça ne peut pas arriver dans mon pays », c'est probablement ce que vous vous dites. Ce n'est pas du tout ce que vous vous dites si vous vivez au Vénézuela, qui est en ce moment touché par l'hyperinflation. Avec un taux d'inflation supérieur à un million de pourcents, leur argent ne vaut plus rien. [75]

Ça pourrait encore prendre plusieurs années, ou ne pas toucher votre devise. Mais il suffit de jeter un coup d'œil à la liste des anciennes monnaies [5] pour voir que cela se produit invariablement, au cours d'un temps suffisamment long. Je me souviens avoir réellement utilisé toutes celles-ci : le schilling autrichien, le Deutsche mark, la lire italienne, le franc français, la livre irlandaise, le dinar croate, etc. Ma grand-mère a même utilisé la couronne austro-hongroise. Au fil du temps, les monnaies en

4. Friedrich Hayek, *La Bonne Monnaie* [34]
5. Voir *Liste des anciennes monnaies* sur Wikipedia. [91]

circulation [6] vont lentement mais sûrement se diriger vers leurs cimetières respectifs. Elles subiront une hyperinflation ou seront remplacées. Elles seront bientôt des monnaies anciennes. Nous les rendrons obsolètes.

> « L'Histoire a montré que les gouvernements cèdent immanquablement à la tentation de gonfler l'offre de monnaie. »
>
> – Saifedean Ammous [7]

Pourquoi Bitcoin est-il différent ? Contrairement aux monnaies imposées par les états, les biens monétaires qui ne sont pas réglementés par des gouvernements, mais par les lois de la physique [8], ont une tendance à la survie et même à maintenir leur valeur au fil du temps. Jusqu'à présent, le meilleur exemple est l'or qui, comme l'atteste le bien nommé *rapport or sur costume correct* [9], conserve sa valeur sur des centaines et même des milliers d'années. Il n'est peut-être pas parfaitement « stable » — un concept discutable dès le départ — mais la valeur qu'il renferme reste au moins dans les mêmes ordres de grandeur.

Lorsqu'un bien monétaire ou une devise conserve efficacement sa valeur à travers le temps et l'espace, il est perçu comme *fort*. Si à l'inverse il ne peut la maintenir, parce qu'il s'abîme ou gonfle facilement son offre, il est considéré comme *faible*. Le concept de dureté est essentiel à la compréhension de Bitcoin et mérite un examen détaillé. Nous y reviendrons dans la dernière leçon sur l'économie : la monnaie saine.

---

6. Voir *Liste des monnaies en circulation* sur Wikipedia [90]
7. Saifedean Ammous, *L'Étalon Bitcoin* [1]
8. Gigi, *La consommation énergétique de Bitcoin - Une nouvelle perspective* [29]
9. L'Histoire montre que le prix d'une once d'or est égal au prix d'un costume pour homme de bonne facture, selon le cabinet de conseil en investissement Sionna[42]

Alors que de plus en plus de pays souffrent d'hyperinflation, de plus en plus de gens devront affronter la réalité des monnaies fortes et faibles. Si nous avons de la chance, il se peut même que certaines banques centrales se trouvent forcées de réévaluer leurs politiques monétaires. Quoi qu'il arrive, la lucidité que m'a procuré Bitcoin s'avérera sans doute inestimable, quelle que soit l'issue.

Bitcoin m'a appris que l'inflation était un impôt caché et que l'hyperinflation était une catastrophe.

10. La valeur

> *« C'était le Lapin Blanc qui revenait en trottant lentement et en jetant autour de lui des regards inquiets comme s'il avait perdu quelque chose... »*
> – Lewis Carroll, *Alice au pays des merveilles*

La valeur est en quelque sorte paradoxale et il existe de multiples théories [1] qui tentent d'expliquer pourquoi nous donnons de la valeur à certaines choses plutôt qu'à d'autres. Les gens sont conscients de ce paradoxe depuis des millénaires. Comme Platon l'écrivait dans son dialogue avec Euthydème, nous estimons certaines choses parce qu'elles sont rares, pas seulement sur leur nécessité à notre survie.

> « Même, pour bien faire, vous avertiriez vos écoliers d'en user de la sorte, et de n'en parler qu'entre eux ou avec vous ; car la rareté, Euthydème, met le prix aux choses, et l'eau, comme dit Pindare, se vend à vil prix quoiqu'elle soit ce qu'il y a de plus précieux. »
>
> – Platon [2]

Ce paradoxe de la valeur [3] montre une chose intéressante à propos de nous autres, humains : il semblerait que nous estimions les choses sur une base subjective [4], tout en observant certains

1. Voir *Théorie de la valeur (économie)* sur Wikipédia [102]
2. Platon, *Euthydème* [60]
3. Voir *Paradoxe de l'eau et du diamant* sur Wikipedia[96]
4. Voir *Conception subjective de la valeur* sur Wikipedia [100]

critères raisonnés. Une chose peut nous être *précieuse* pour de nombreuses raisons, mais celles auxquelles nous accordons de la valeur partagent certains traits. Si cette chose se copie facilement ou qu'elle est naturellement abondante, nous ne l'estimons pas.

Apparemment, nous accordons de la valeur à quelque chose par sa rareté (l'or, les diamants, le temps), sa complexité ou sa quantité de travail nécessaire, son irremplaçabilité (une vieille photo d'un être cher), son utilité à permettre des choses autrement impossibles ou encore une combinaison de tout ça, comme les grandes œuvres d'art.

Bitcoin est tout ça à la fois : il est extrêmement rare (21 millions), de plus en plus dur à produire (la réduction des récompenses), impossible à remplacer (une clé privée perdue l'est à jamais) et nous permet de faire des choses plutôt utiles. C'est vraisemblablement le meilleur outil pour transférer de la valeur au-delà des frontières, il est virtuellement résistant à la censure et à la saisie, ce qui permet à n'importe qui de stocker sa valeur sans l'aval des banques et du gouvernement, pour ne citer qu'eux.

Bitcoin m'a appris que la valeur était subjective, mais pas arbitraire.

11. L'argent

« Quand j'étais jeune, . . .
j'ai bien entretenu la souplesse de mes muscles
en me frottant avec cette crème
– un shilling la boite ! –
Voulez-vous m'en acheter un lot ? »

– Le Sage

Qu'est-ce que l'argent ? On l'utilise tous les jours, pourtant il est étonnamment complexe de répondre à cette question. Nous en dépendons de toutes les manières possibles et imaginables et si nous en manquons nos vies deviennent très difficiles. Toutefois, nous réfléchissons rarement à cette chose qui fait prétendument tourner le monde. Bitcoin m'a contraint à répondre inlassablement à cette question : mais enfin c'est quoi, l'argent ?

Dans notre monde « moderne », la plupart des gens penseront probablement à des bouts de papier lorsqu'ils parleront d'argent, alors même qu'il n'est en majorité qu'un nombre sur un compte bancaire. Notre argent est déjà fait de un et de zéros, alors en quoi Bitcoin est-il différent ? Il l'est car en son sein, c'est un *type* de monnaie très différent de celle que l'on utilise habituellement. Pour le comprendre, nous allons devoir nous pencher sur ce qu'est la monnaie, comment elle a vu le jour et pourquoi l'or et l'argent ont été utilisés durant la majeure partie de l'histoire du commerce.

Les coquillages, l'or, l'argent, le papier, le bitcoin. En fin de compte, **la monnaie c'est ce dont les gens se servent**, peu importe son aspect et sa forme, ou l'absence de celles-ci.

L'argent est ingénieux, en tant qu'invention. Un monde sans argent s'en retrouverait compliqué à l'absurde : combien de poissons pour ces nouvelles chaussures ? Combien de vaches pour acheter une maison ? Qu'est-ce que je fais si je n'ai aucun besoin immédiat mais que je dois me débarrasser de mes pommes bien mûres ? Pas besoin d'être très imaginatif pour comprendre qu'une économie basée sur le troc serait terriblement inefficace.

Le truc excellent avec l'argent c'est qu'on peut l'échanger contre *n'importe quoi d'autre* – c'est une sacrée invention ! Tel que Nick Szabo [1] le résume brillamment dans *Shelling Out : The Origins of Money* [69], les êtres humains ont utilisé toutes sortes de choses en tant que monnaie : des perles de matériaux rares comme l'ivoire, des coquillages, des os spécifiques, divers types de bijoux, puis plus tard des métaux rares comme l'argent ou l'or.

> « En ce sens, il ressemble plus à un métal précieux. Au lieu que ce soit l'offre qui change afin de maintenir la valeur, celle-ci est prédéterminée et c'est la valeur qui change. »
>
> – Satoshi Nakamoto [2]

Tels les bons paresseux que nous sommes, nous ne passons pas trop de temps à réfléchir à ce qui marche. L'argent, pour la plupart d'entre nous, ça fonctionne très bien. Comme avec nos voitures ou nos ordinateurs, nous ne sommes obligés d'y penser que lorsqu'un de ces trucs tombe en panne. Les personnes qui ont vu leurs économies d'une vie s'évaporer avec l'hyperinflation savent très bien la valeur d'une monnaie forte, tout comme ceux qui ont vu leurs amis et famille disparaître à cause des atrocités de l'Allemagne nazie ou de l'Union Soviétique connaissent très bien la valeur de la confidentialité.

1. `http://unenumerated.blogspot.com/`
2. Satoshi Nakamoto, dans une réponse à Sepp Hasslberger [50]

Le problème avec l'argent, c'est qu'il est partout. Il représente la moitié de chaque transaction, ce qui confère un pouvoir considérable à ceux qui sont responsables de l'émission monétaire.

> « Étant donné que l'argent représente la moitié de chaque transaction commerciale et que des civilisations entières s'épanouissent et s'effondrent selon la qualité de leur monnaie, on parle ici d'un pouvoir incommensurable, un pouvoir qui est passé sous silence. C'est le pouvoir de tisser des mirages qui semblent vrais aussi longtemps qu'ils durent. C'est là le cœur du pouvoir de la Réserve Fédérale. »
>
> – Ron Paul [3]

Bitcoin retire ce pouvoir pacifiquement, puisqu'il met fin à l'émission monétaire sans recourir à la force.

L'argent a connu de multiples itérations. La plupart d'entre elles étaient bonnes. Elles amélioraient notre monnaie d'une façon ou d'une autre. En revanche, très récemment, ses rouages ont été corrompus. Aujourd'hui, la quasi-totalité de notre argent est fabriqué *de toutes pièces* par les pouvoirs en place. Pour comprendre comment nous en sommes arrivés là, j'ai dû étudier l'histoire de la monnaie et de son déclin consécutif.

Il reste encore à voir s'il faudra une série de catastrophes ou simplement un effort éducatif monumental pour réparer cette corruption. Je prie les dieux de la monnaie saine afin que ce soit le second.

Bitcoin m'a appris ce qu'était l'argent.

3. Ron Paul, *End the Fed* [57]

12. L'histoire et le déclin de la monnaie

> *« . . . ils avaient refusé de se rappeler les simples règles de conduite que leurs amis leur avaient enseignées : par exemple, qu'un tisonnier chauffé au rouge vous brûle si vous le tenez trop longtemps, ou que, si vous vous faites au doigt une coupure très profonde avec un couteau, votre doigt, d'ordinaire, se met à saigner ; et Alice n'avait jamais oublié que si l'on boit une bonne partie du contenu d'une bouteille portant l'étiquette : poison, cela ne manque presque jamais, tôt ou tard, de vous causer des ennuis. »*
> – Lewis Carroll, *Alice au pays des merveilles*

Beaucoup de personnes pensent que la monnaie est soutenue par de l'or, qui serait enfermé dans de grandes chambres fortes, protégées par d'épais murs. Ce n'est plus vrai depuis plusieurs décennies. Je ne suis pas certain de ce que j'en ai pensé quand je l'ai appris, puisque j'étais encore plus embêté, n'ayant potentiellement aucune compréhension de l'or, de l'argent papier ou même de pourquoi il faudrait le soutenir avec quelque chose, pour commencer.

Un des aspects de l'étude de Bitcoin est l'étude de la monnaie fiduciaire : ce que ça signifie, comment c'est apparu et pourquoi c'est peut-être pas la meilleure idée que nous ayons eu. Alors, qu'est-ce que la monnaie fiduciaire exactement ? Et comment en est-on arrivés à l'utiliser ?

Lorsque quelque chose est imposé par *décret*, ça veut sim-

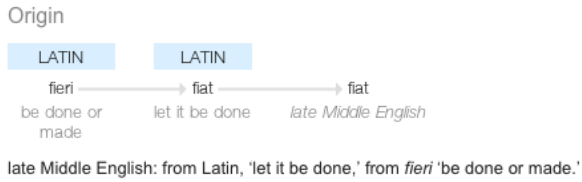


FIGURE 12.1. – fiat — 'Qu'il en soit ainsi'

plement dire c'est imposé par une autorisation ou une proposition officielle. Par conséquent, la monnaie fiduciaire est monnaie simplement parce que *quelqu'un* le décide. De nos jours, comme tous les gouvernements utilisent de la monnaie fiduciaire, ce quelqu'un c'est *votre* gouvernement. Malheureusement, vous n'êtes pas *libre* d'être en désaccord avec cette proposition de valeur. Vous vous apercevrez rapidement qu'elle est tout sauf non-violente. Si vous refusez d'utiliser cette monnaie papier pour mener vos affaires et payer vos impôts, les seules personnes avec qui vous pourrez parler économie seront vos compagnons de cellule.

La valeur de la monnaie fiduciaire ne découle pas de ses attributs intrinsèques. La qualité d'une catégorie donnée de monnaie fiduciaire n'est corrélée qu'à l'(in)stabilité politique et fiscale de ceux qui la font passer du rêve à la réalité. Sa valeur est décrétée, arbitrairement.

Jusqu'à récemment, deux sortes de monnaie étaient d'usage : la **monnaie de commodité**, faite de *choses* précieuses ; et la **monnaie représentative**, qui *représente* uniquement la chose précieuse, généralement par des jeux d'écriture.

Nous avons déjà abordé la monnaie de commodité plus haut. Les gens utilisaient des os, des coquillages et des métaux précieux comme monnaie. Plus tard, ce sont principalement des

FIGURE 12.2. – Pièce lydienne en électrum. Crédit photo CC-BY-SA Classical Numismatic Group, Inc.

pièces faites de ces métaux comme l'or ou l'argent qui furent utilisées. La plus vieille pièce qu'on ait trouvée jusqu'à aujourd'hui est faite d'un alliage naturel d'or et d'argent et a été frappée il y a plus de 2700 ans [1]. S'il y a de l'innovation dans Bitcoin, ce n'est pas le concept de pièce.

Il s'avère que la thésaurisation, ou hodling, pour reprendre le jargon moderne, est presque aussi vieille que les pièces elles-mêmes. Le plus ancien hodler de pièces était une personne qui a mis une centaine de celles-ci dans une jarre et l'a enterrée sous les fondations d'un temple, pour qu'on ne les retrouve qu'au bout de 2500 ans. Plutôt un bon stockage à froid si vous voulez mon avis.

L'un des inconvénients d'utiliser des pièces faites de métaux précieux est qu'elles peuvent être rognées, dépréciant de fait leur valeur. De nouvelles pièces peuvent être frappées à partir des copeaux, faisant gonfler l'offre de monnaie au fil du temps, dévaluant chaque autre pièce au passage. Les gens rabotaient

1. D'après l'historien grec Hérodote, contemporain du Ve siècle avant J.-C., les Lydiens furent le premier peuple à utiliser des pièces d'or et d'argent. [47]

FIGURE 12.3. – Pièces d'argent rognées à divers degrés.

littéralement tout ce qu'ils pouvaient de leurs dollars d'argent. Je me demande quel genre de pubs *Dollar Shave Club* faisait à l'époque.

Puisque la seule inflation que les gouvernements tolèrent est celle dont ils sont responsables, des efforts furent entrepris pour mettre un terme à cette guérilla de la dépréciation. Au jeu traditionnel du gendarme et du voleur, les rogneurs de pièces ont fait preuve d'imagination dans leurs procédés, forçant les « Maîtres de la Monnaie » à faire preuve d'encore plus d'imagination dans leurs contre-mesures. Isaac Newton, le physicien mondialement reconnu, auteur de *Principia Mathematica*, était l'un de ces maîtres. C'est à lui qu'on attribue l'ajout des stries sur la tranche des pièces que l'on peut toujours observer aujourd'hui. L'époque du rognage facile était révolue.

Même en gardant un œil sur les procédés de dépréciation des pièces [2], celles-ci faisaient encore face à d'autres problèmes. Elles

2. En plus du rognage, le grippage (secouer les pièces dans un sac et récupérer la poussière de métal qui s'est détachée) ainsi que le tamponnage (faire un trou au centre de la pièce et l'aplatir au marteau jusqu'à combler le trou) étaient les techniques de dépréciation les plus répandues. [92]

FIGURE 12.4. – Le 'dollar' originel. Saint Joachim est représenté avec sa robe et son chapeau de mage. Crédit photo CC-BY-SA Wikipedia utilisateur Berlin-George

sont encombrantes et pas très pratiques à transporter, surtout en cas de grands transferts de valeur. C'est pas vraiment faisable d'arriver avec un gros sac de dollars en argent chaque fois que vous voulez acheter une Mercedes.

En parlant de trucs allemands : l'origine du nom du *dollar* américain est une autre histoire intéressante. Le mot « dollar » est dérivé du mot allemand *Thaler*, l'abréviation de *Joachimsthaler* [101]. Un Joachimsthaler était une pièce frappée dans la ville de *Sankt Joachimsthal*. Thaler est simplement le raccourci pour désigner quelqu'un (ou quelque chose) qui vient de la vallée. Et puisque Joachimsthal était *la* vallée ou l'on produisait les pièces d'argent, les gens appelaient naturellement ces pièces des *Thaler*. Thaler (en allemand) a glissé vers daalders (en hollandais) puis finalement vers dollars (en anglais).

L'introduction de la monnaie représentative sonna le glas de la monnaie dure. Les certificats sur l'or furent introduits en 1863 et quinze ans après, le dollar d'argent fut lui aussi lentement mais

FIGURE 12.5. – Un dollar d'argent américain de 1928. 'Payable au porteur sur demande.' Crédit photo CC-BY-SA Collection numismatique nationale de l'institut Smithsonian

sûrement remplacé par un intermédiaire de papier : le certificat sur l'argent. [99]

Il aura ensuite fallu environ un demi-siècle après l'arrivée des certificats pour que ces morceaux de papier se changent en ce que nous connaissons de nos jours comme le dollar américain.

Notez que le dollar d'argent américain de 1928 dans la figure 12.5 porte toujours le nom de *certificat sur l'argent*, ce qui indique qu'il s'agit bien d'un document stipulant que l'on doit au porteur de ce bout de papier un peu de métal argenté. Il est intéressant de remarquer que le texte l'indiquant s'est vu rétrécir au fil du temps. La trace du mot *certificat* a fini par totalement disparaître, remplacée par la déclaration rassurante qu'il s'agit de billets de la réserve fédérale.

Nous l'avons évoqué plus haut, il s'est passé la même chose avec l'or. Dans sa majorité, le monde fonctionnait sur un étalon bimétallique [77], ce qui signifie que les pièces étaient principalement composées d'or et d'argent. C'était à n'en pas douter une avancée technologique d'avoir des certificats sur l'or, échan-

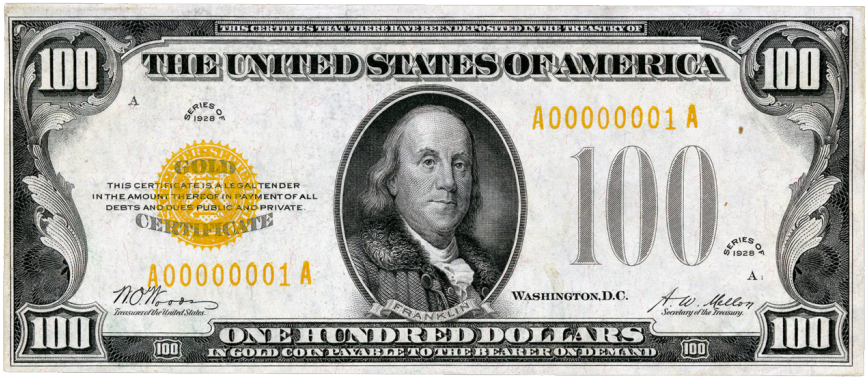


FIGURE 12.6. – Un certificat américain sur l'or de 100$ de 1928. Crédit photo CC-BY-SA Collection numismatique nationale, Musée National de l'Histoire américaine.

geables contre des pièces de ce même métal. Le papier est plus pratique, plus léger et puisqu'il est divisible arbitrairement en inscrivant simplement dessus un nombre plus petit, il est facile de le réduire en plus petites unités.

Afin de rappeler aux porteurs (utilisateurs) que ces certificats représentaient de l'or ou de l'argent bien réels, ils revêtaient une couleur évocatrice et l'indiquaient clairement en toutes lettres. Vous pouvez facilement lire ce message de haut en bas :

> « Il est certifié par la présente que cent dollars en pièces d'or, payables au porteur sur demande, ont été déposés au trésor des États-Unis d'Amérique. »

En 1963, les mots « PAYABLES AU PORTEUR SUR DEMANDE » furent retirés de tous les nouveaux billets. Cinq ans plus tard, il fut mis fin à la convertibilité des billets en or ou en argent.

Les mots qui rappelaient l'origine de la monnaie papier et l'idée qui l'accompagne furent supprimés. La couleur dorée dis-

FIGURE 12.7. – Un billet américain de vingt dollars de 2004 utilisé de nos jours. 'CE BILLET A COURS LÉGAL'

parut. Il ne restait plus que le papier et avec lui, pour le gouvernement, la possibilité d'en imprimer autant qu'il le voulait.

Ce tour de passe-passe long de plus d'un siècle fut achevé en 1971 par l'abolition de l'étalon-or. L'argent devint l'illusion que nous partageons tous dorénavant : la monnaie fiduciaire. Elle a de la valeur car quelqu'un, qui commande une armée et gère des prisons, a dit qu'elle en avait. On peut très clairement le lire sur chaque dollar en circulation aujourd'hui, « CE BILLET A COURS LÉGAL ». Autrement dit : il vaut quelque chose parce que c'est écrit dessus.

À ce propos, il y a une autre leçon intéressante sur les billets modernes qui se cache sous nos yeux. La deuxième ligne indique que le cours légal concerne « TOUTES LES DETTES, PUBLIQUES ET PRIVÉES ». J'ai été surpris par ce qui peut paraître une évidence pour les économistes : tout l'argent consiste en de la dette. J'en ai encore des migraines, je laisserai donc au lecteur la tâche d'étudier le lien entre l'argent et la dette.

Nous l'avons vu, l'or et l'argent ont été utilisés comme monnaie pendant des millénaires. Au fil du temps, les pièces d'or et d'argent furent remplacées par du papier. Celui-ci a lentement été accepté comme moyen de paiement. Cette adoption créa une illusion — l'illusion que le papier lui-même a de la valeur. Le coup de grâce fut de totalement rompre le lien entre la représentation et le réel : abolir l'étalon-or en convainquant tout le monde que c'est le papier qui est précieux.

Bitcoin m'a appris l'Histoire de la monnaie et le plus important tour de passe-passe dans l'Histoire de l'économie : la monnaie fiduciaire.

13. La folie des réserves fractionnaires

> *Hélas ! les regrets étaient inutiles ! Elle continuait à grandir sans arrêt, et, bientôt, elle fût obligée de s'agenouiller sur le plancher : une minute plus tard, elle n'avait même plus assez de place pour rester à genoux, et elle essayait de voir si elle serait mieux en se couchant, un coude contre la porte, son autre bras replié sur la tête. Puis, comme elle ne cessait toujours pas de grandir, elle passa un bras par la fenêtre, mit un pied dans la cheminée, et se dit : « À présent je ne peux pas faire plus, quoi qu'il arrive. Que vais-je devenir ? »*
> – Lewis Carroll, *Alice au pays des merveilles*

La valeur et la monnaie ne sont pas des sujets simples, particulièrement de nos jours. Le processus d'émission monétaire du système bancaire ne l'est pas plus et je ne peux m'empêcher de croire que c'est délibéré. Ce phénomène, que je n'avais jusqu'à présent rencontré que dans les papiers de recherche et les documents légaux, semble également courant dans les milieux financiers : rien n'est expliqué de façon simple, non pas parce que c'est réellement complexe, mais parce que la vérité est dissimulée sous des couches et des couches de jargon d'une complexité *apparente*. « Politique monétaire expansionniste, assouplissement quantitatif, relance fiscale de l'économie ». Le public hoche de la tête, hypnotisé par les mots savants.

Les banques à réserve fractionnaire et l'assouplissement quantitatif sont justement deux de ces mots sophistiqués, dissimulant

la réalité des choses en la présentant comme complexe et difficile à comprendre. Si vous deviez expliquer ça à un enfant, vous verriez rapidement la folie qu'ils renferment.

Godfrey Bloom l'a exprimé bien mieux que je ne pourrais jamais le faire, en s'adressant au Parlement Européen lors d'un débat commun :

> « [...] vous ne comprenez pas vraiment le concept de banque. Toutes les banques sont fauchées. La Santander, la Deutsche Bank, la Royal Bank of Scotland — elles sont toutes fauchées ! Et pourquoi elles sont fauchées ? Ce n'est pas une volonté divine. Ce n'est pas une espèce de tsunami. Elles sont fauchées parce qu'elles ont un système appelé 'réserves fractionnaires' qui leur permet de prêter de l'argent qu'elles n'ont même pas ! C'est un scandale orchestré par des malfaiteurs et ça fait trop longtemps que ça dure. [...] Il y a de la contrefaçon — qu'on appelle parfois assouplissement quantitatif — mais ça reste de la contrefaçon sous un autre nom. La création monétaire artificielle coûterait au simple quidam un long moment derrière les barreaux [...] et tant que l'on n'enverra pas les banquiers — et j'inclus ici les banquiers centraux et les politiques — en prison pour ce scandale cela continuera. »
>
> – Godfrey Bloom [1]

Permettez-moi de répéter le passage essentiel : les banques peuvent prêter de l'argent qu'elles ne possèdent pas.

Grâce au système de réserve fractionnaire, une banque a besoin de ne garder qu'une *fraction* de chaque dollar qu'elle reçoit. Ça se situe quelque part entre 0 et 10%, plutôt vers la limite inférieure d'ailleurs, ce qui n'arrange rien.

1. Débat commun sur l'union bancaire [17]

Prenons un exemple concret afin de mieux illustrer cette idée insensée : une fraction de 10% fera l'affaire et nous devrions pouvoir calculer de tête. Avantageux pour tout le monde. Donc, si vous déposez 100$ à la banque — parce que vous n'avez pas envie de les garder sous votre matelas — celle-ci n'a besoin de garder que la *fraction* consentie. Dans notre exemple, cela fait 10$, car 10% de 100$ font 10$. Simple, non ?

Mais alors que font les banques avec le reste de l'argent ? Qu'arrive-t-il aux 90$ restants ? Elles font ce que les banques savent faire, elles les prêtent à d'autres. Cela produit un effet multiplicateur sur la monnaie, qui accroît énormément son offre dans l'économie (Figure 13.1). Votre dépôt initial de 100$ se transforme rapidement en 190$. En prêtant 90% de ces 90$ fraîchement créés, cela fera bientôt 271$ dans l'économie. Et 343,90$ après ça. L'offre de monnaie gonfle de façon récursive, puisque les banques prêtent littéralement de l'argent qu'elles n'ont pas [93]. Sans la moindre formule, les banques changent 100$ en plus d'un milier, comme par magie. Il s'avère qu'il est simple d'arriver à un facteur 10. Ça prend seulement quelques cycles de prêt.

Ne vous méprenez pas : il n'y a rien de mal à prêter. Il n'y a rien de mal à percevoir des intérêts. Il n'y a même rien de mal avec cette bonne vieille banque qui garde votre patrimoine plus sûrement que dans votre tiroir à chaussettes.

Les banques centrales sont une toute autre affaire, en revanche. Elles sont les abominations de la régulation financière, mi-publiques mi-privées, jouant à Dieu avec des choses qui impactent tout membre de la civilisation mondiale, sans morale, avec pour seul intérêt le futur à court terme et apparemment aucune responsabilité ni vérifiabilité (voir la Figure 13.2).

Bien que Bitcoin soit encore inflationniste, il cessera de l'être relativement rapidement. La limite stricte sur l'offre de 21 millions de bitcoins finira par éliminer totalement l'inflation. Nous

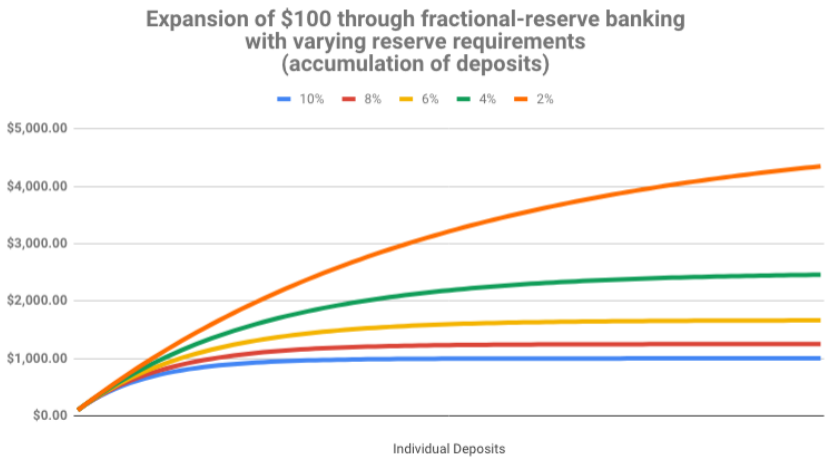


FIGURE 13.1. – L'effet multiplicateur sur la monnaie

FIGURE 13.2. – Yellen est fermement opposée à un audit de la réserve fédérale, pendant que le gars au panneau Bitcoin soutient fermement l'achat de bitcoin.

avons maintenant deux mondes monétaires : l'un inflationniste où l'argent est créé arbitrairement et le monde de Bitcoin, où l'offre finale est fixe et facilement vérifiable par tout un chacun. L'un nous est imposé par la violence, l'autre peut être rejoint par quiconque le désire. Pas de barrière à l'entrée, personne à qui demander la permission. Une participation volontaire. Voilà la beauté de Bitcoin.

J'ajouterais que le débat entre les économistes Keynésiens [2] et l'école autrichienne [3] n'est plus seulement académique. Satoshi est parvenu à créer un système de transfert de valeur sous stéroïdes, inventant dans le même temps la monnaie la plus saine ayant jamais existé. D'une façon ou d'une autre, de plus en plus de gens prendront conscience de l'arnaque qu'est le système de réserve fractionnaire. S'ils en arrivent aux mêmes conclusions que la plupart des Bitcoiners et économistes de l'école autrichienne, ils pourraient rejoindre l'internet de l'argent, qui ne cesse de grandir. Personne ne peut les empêcher de faire ce choix.

Bitcoin m'a appris que les réserves fractionnaires des banques n'étaient que pure folie.

2. Les théories de John Maynard Keynes et ses adeptes [86]

3. École de pensée économique basée sur l'individualisme méthodologique [76]

14. Une monnaie saine

> *« La première chose que je dois faire, » se dit-elle tout en marchant dans le bois à l'aventure, « c'est retrouver ma taille normale ; la seconde, c'est de trouver le chemin qui mène à ce charmant jardin. Je crois que c'est un très bon plan. »*
> – Lewis Carroll, *Alice au pays des merveilles*

La leçon la plus importante que j'ai tirée de Bitcoin c'est qu'en fin de compte, la monnaie forte est meilleure que la monnaie faible. La monnaie forte, également appelée *monnaie saine*, consiste en toute monnaie échangeable sur le marché mondial pouvant servir de réserve de valeur solide.

D'accord, Bitcoin est encore jeune et volatil. Les critiques avanceront qu'il n'est pas fiable en tant que réserve de valeur. Mais l'argument de la volatilité passe à côté du sujet. Il faut s'attendre à de la volatilité. Ça prendra un moment au marché pour déterminer le juste prix de cette nouvelle monnaie. De plus, il est fondé sur une erreur de métrique, comme le souligne une plaisanterie récurrente. Si vous réfléchissez en dollars, vous passerez à côté du fait qu'un bitcoin vaudra toujours un bitcoin.

> « Une offre monétaire fixe, ou une offre modifiée uniquement sur la base de critères objectifs et calculables, est une condition nécessaire à un prix de la monnaie juste et significatif. »
>
> – Père Bernard W. Dempsey, S.J. [1]

1. Perry J. Roets, S.J., *Revue de l'économie sociale* [62]

$$\sum_{i=0}^{32} \frac{210000 \lfloor \frac{50*10^8}{2^i} \rfloor}{10^8} \tag{14.1}$$

FIGURE 14.1. – Formule de l'offre de Bitcoin

Comme l'a montré une courte ballade dans le cimetière des monnaies disparues, l'argent qui peut être créé le sera. Dans l'Histoire, aucun être humain n'a su jusqu'à présent résister à la tentation.

Bitcoin élimine cette tentation de la création monétaire de façon astucieuse. Satoshi avait conscience de notre cupidité et de notre faillibilité — c'est pour cela qu'il a choisi une chose plus fiable que le contrôle humain : les mathématiques.

Bien que la formule ci-dessus soit utile pour décrire l'offre de Bitcoin, on ne la trouve nulle part dans le code. L'émission de nouveaux bitcoins est contrôlée par un algorithme, qui réduit tous les quatre ans [13] la récompense payée aux mineurs. Cette formule permet donc de résumer rapidement ce qui se passe sous le capot. On comprend mieux ce qui se passe vraiment en regardant la variation des récompenses de bloc, payées à quiconque trouve un bloc valide, ce qui arrive à peu près toutes les 10 minutes.

Les formules, les fonctions logarithmiques et les exponentielles ne sont pas particulièrement intuitives à comprendre. Le concept de *sain* peut s'appréhender plus facilement si on le voit autrement. Une fois que l'on sait combien il existe d'une chose et que l'on sait combien cette chose est difficile à produire ou à obtenir, nous comprenons immédiatement sa valeur. Ce qui est vrai avec un tableau de Picasso, une guitare d'Elvis Presley ou un violon de Stradivarius est également vrai pour la monnaie fiduciaire, l'or et les bitcoins.

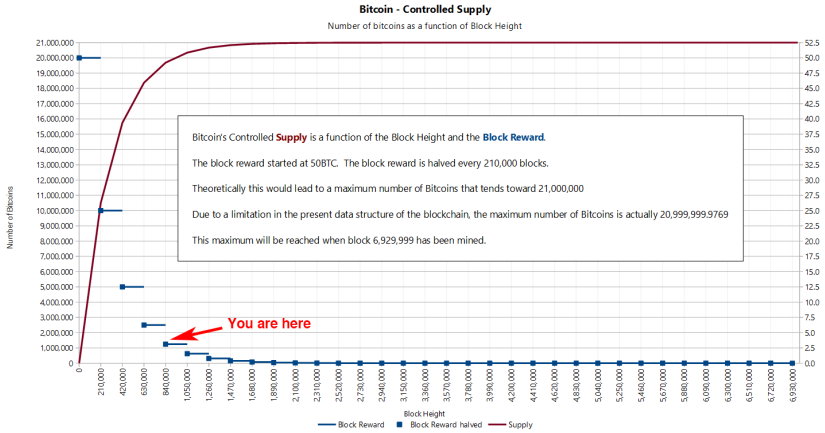


FIGURE 14.2. – L'offre contrôlée de Bitcoin

La dureté des monnaies fiduciaires dépend des responsables de leurs planches à billets respectives. Certains gouvernements seront sans doute plus enclins à créer de plus larges quantités de monnaie que d'autres, aboutissant à une monnaie plus faible. D'autres gouvernements seront plus modérés sur leur émission monétaire, entraînant une monnaie plus forte.

> « Un aspect important de cette nouvelle réalité est que les institutions telles que la réserve fédérale ne peuvent pas faire faillite. Elles peuvent créer autant d'argent qu'elles en ont besoin pour un coût virtuellement nul. »
>
> – Jörg Guido Hülsmann [2]

Avant que nous n'ayons des monnaies fiduciaires, la dureté de l'argent était déterminée par les propriétés naturelles de ce qui servait de monnaie. La quantité d'or sur Terre est limitée par les lois de la physique. L'or est rare car les collisions de supernovas et d'étoiles à neutrons sont rare. Le « flux » d'or est limité car il

2. Jörg Guido Hülsmann, *L'éthique de la création monétaire* [38]

demande des efforts à extraire. Comme c'est un élément lourd, il est en majorité enterré bien profondément dans le sol.

L'abolition de l'étalon-or a engendré une nouvelle réalité : il suffit d'un peu d'encre pour créer de l'argent. Dans le monde actuel, ça demande encore moins d'efforts d'ajouter quelques zéros au solde d'un compte bancaire : il suffit de modifier quelques octets sur l'ordinateur d'une banque.

On peut exprimer plus généralement le principe énoncé ci-dessus comme étant le rapport entre les « stocks » et les « flux ». Plus simplement, le *stock* représente la quantité existante de quelque chose. Pour nos besoins, le stock est la mesure de l'offre actuelle de monnaie. Le *flux* quantifie la production de cette même chose sur une durée donnée (par an, par exemple). La clé pour comprendre la monnaie saine est de comprendre le rapport stock-à-flux.

Calculer le rapport stock-à-flux de la monnaie fiduciaire est complexe, car l'offre de monnaie dépend de ce que vous y intégrez [94]. Vous pouvez ne compter que les billets et les pièces (M0), ajouter les chèques de voyage et les remises de chèques (M1), ajouter les comptes épargne, les fonds communs et quelques autres trucs (M2) et même ajouter à tout ça les certificats de dépôt (M3). De plus, la façon dont tout cela est défini et calculé dépend de chaque pays et puisque la réserve fédérale des États-Unis a cessé de publier [61] les chiffres pour M3, nous allons devoir faire avec l'offre monétaire M2. J'adorerais pouvoir vérifier ces chiffres, mais pour le moment j'imagine que nous devrons faire confiance à la réserve fédérale.

C'est l'or, l'un des métaux les plus rares sur Terre, qui a le rapport stock-à-flux le plus élevé. Selon l'Institut d'études géologiques des États-Unis, un peu plus de 190 000 tonnes en ont été minées au total. Au cours des dernières années, environ 3100 tonnes ont été minées par an [68].

À partir de ces chiffres, nous pouvons facilement calculer le

$$\frac{190,000t}{3,100t} = 61 \tag{14.2}$$

FIGURE 14.3. – Rapport stock-à-flux de l'or

rapport stock-à-flux de l'or (voir la Figure 14.3).

Il n'y a rien qui ait un rapport stock-à-flux plus élevé. C'est pour cette raison que l'or, jusqu'à maintenant, était la monnaie la plus forte et la plus saine qui soit. On raconte souvent que tout l'or qui a déjà été miné tiendrait dans deux piscines olympiques. Selon mes calculs [3], il en faudrait quatre. Donc soit les piscines olympiques ont rétréci, soit il faudrait peut-être revoir ça.

Arrive alors le Bitcoin. Comme vous le savez sans doute déjà, le minage de bitcoin fait fureur depuis quelques années. Cela s'explique car nous sommes encore au début de ce qu'on appelle *le temps des récompenses*, où les nœuds de minage sont récompensés avec *beaucoup* de bitcoin pour leurs efforts de calcul. Nous sommes en ce moment dans l'époque numéro 3, qui a débuté en 2016 et s'achèvera au début de 2020, sans doute en mai. Tandis que l'offre de bitcoins est limitée, les rouages internes de Bitcoin ne permettent d'établir que des dates approximatives. Pourtant, nous pouvons prédire avec certitude à quel niveau le rapport stock-à-flux de Bitcoin se situera. Alerte spoiler : ça sera élevé.

Élevé comment ? Eh bien, il s'avère que Bitcoin finira par devenir infiniment fort (voir la Figure 14.4).

À cause de la réduction exponentielle des récompenses de minage, le flux de nouveaux bitcoins va diminuer, engendrant un rapport stock-à-flux qui grimpe en flèche. Il rattrapera l'or en

3. `https://bit.ly/gold-pools`

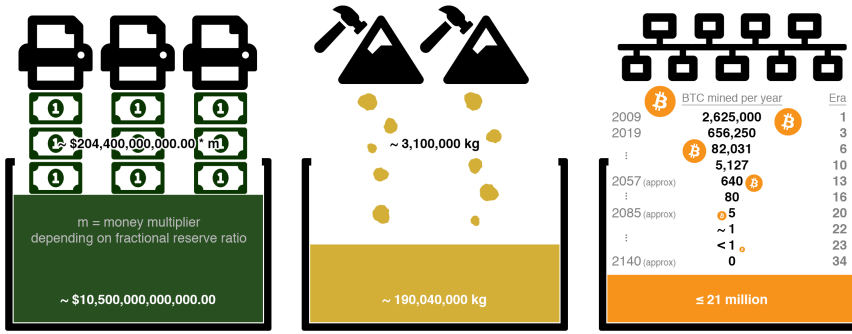


FIGURE 14.4. – Visualisation du stock et du flux du dollar US, de l'or et de Bitcoin

2020, pour mieux le surpasser quatre ans plus tard en doublant à nouveau sa dureté. Au total, un tel doublement se produira 64 fois. Grâce à la puissance des exponentielles, le nombre de bitcoins minés par an tombera à moins de 100 bitcoins dans 50 ans et à moins de 1 bitcoin dans 75 ans. Le robinet mondial que représentent les récompenses de bloc se tarira aux environs de l'année 2140, mettant effectivement un terme à la production de bitcoin. C'est un jeu de longue haleine. Si vous lisez ceci, vous êtes encore en avance.

Alors que le bitcoin tend vers un rapport stock-à-flux infini, il deviendra la monnaie la plus saine qui soit. La dureté infinie semble difficile à battre.

D'un point de vue économique, *l'ajustement de la difficulté* de Bitcoin est son aspect le plus important. La difficulté à miner du bitcoin dépend de la rapidité avec laquelle de nouveaux bitcoins sont minés [4]. C'est l'ajustement dynamique de la difficulté de minage du réseau qui nous permet de prédire son offre future.

La simplicité de l'algorithme d'ajustement de la difficulté pour-

4. En réalité ça dépend de la vitesse à laquelle des blocs valides sont trouvés, mais pour nos besoins, c'est la même chose que de « miner des bitcoins » et ça le restera pour les 120 prochaines années.

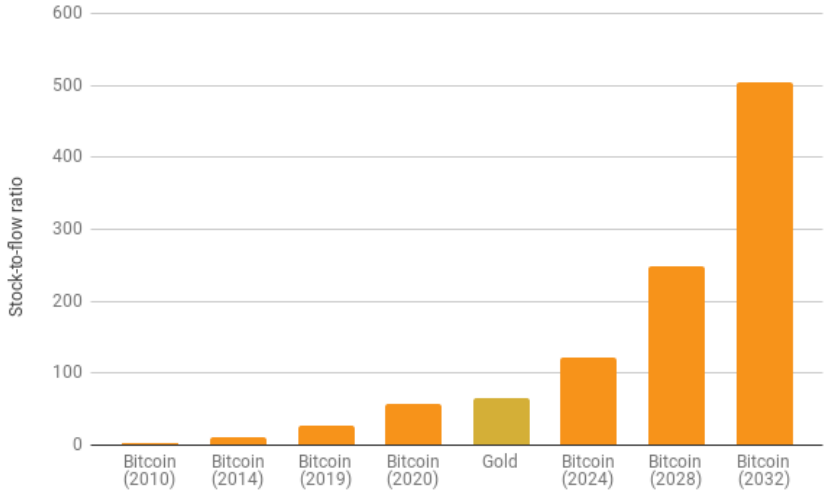


FIGURE 14.5. – Le rapport stock-à-flux du bitcoin comparé à l'or

rait détourner de sa profondeur, mais il est véritablement une révolution aux proportions dignes d'Einstein. Il garantit que quels que soient les efforts déployés dans le minage, l'offre maîtrisée de Bitcoin ne sera pas perturbée. À la différence de toutes les autres ressources, peu importe l'énergie dépensée par quelqu'un dans le minage de bitcoin, la récompense totale n'augmentera pas.

Tout comme $E = mc^2$ impose une limite universelle à la vitesse dans notre univers, l'ajustement de la difficulté de minage impose sa **limite monétaire universelle** à Bitcoin.

Sans cet ajustement de la difficulté, tous les bitcoins auraient déjà été minés. Sans cet ajustement de la difficulté, Bitcoin n'aurait probablement pas survécu à ses premiers pas. C'est ce qui sécurise le réseau durant le temps des récompenses. C'est ce qui

garantit une distribution stable et impartiale [5] des nouveaux bitcoins. C'est le thermostat qui régule la politique monétaire de Bitcoin.

Einstein nous a enseigné une chose novatrice : peu importe la force imprimée à un objet, à un moment donné vous ne pourrez pas le faire aller plus vite. Satoshi nous a aussi enseigné une chose novatrice : peu importent les efforts mis dans le minage de cet or numérique, à un moment donné vous ne pourrez pas en tirer plus de bitcoins. Pour la première fois dans l'Histoire de l'Humanité, nous avons un bien monétaire dont vous ne pourrez pas augmenter la production, peu importe à quel point vous essaierez.

Bitcoin m'a appris que la monnaie saine était indispensable.

5. Dan Held, *La distribution de Bitcoin était juste* [36]

Troisième partie

Technologie

Technologie

> *« Cette fois-ci, je vais m'y prendre un peu mieux » se dit-elle, et elle commença par s'emparer de la petite clé d'or et par ouvrir la porte qui donnait sur le jardin.*
> – Lewis Carroll, *Alice au pays des merveilles*

Des clés d'or, des horloges qui ne fonctionnent qu'au hasard, des courses pour résoudre d'étranges énigmes et des bâtisseurs anonymes et sans visages. On dirait des contes de fée tirés du pays des merveilles mais c'est pourtant la routine dans l'univers Bitcoin.

Comme nous l'avons vu dans le Chapitre II, des pans entiers du système financier actuel sont systématiquement défaillants. À la manière d'Alice, nous ne pouvons qu'espérer faire mieux cette fois-ci. Pourtant, grâce à un inventeur pseudonyme, nous disposons dorénavant d'une technologie incroyablement sophistiquée pour nous aider : Bitcoin.

Résoudre des problèmes dans un environnement radicalement décentralisé et hostile demande des solutions uniques. Des problèmes habituellement triviaux à résoudre n'ont rien de trivial dans cet étrange monde fait de nœuds. Pour la plupart de ses solutions, Bitcoin repose sur une cryptographie solide, tout du moins du point de vue de la technologie. Nous verrons dans une des leçons qui suivent à quel point cette cryptographie est solide.

Bitcoin se sert de la cryptographie pour se détacher de la confiance dans les autorités. Au lieu d'être tributaire d'institutions centralisées, le système s'appuie sur l'autorité ultime de notre univers : la physique. Cependant, il reste tout de même

quelques traces de confiance. Nous examinerons ces traces dans la seconde leçon de ce chapitre.

Partie III – Technologie :

15. La force dans les nombres
16. Remarques sur « Ne vous fiez pas, vérifiez »
17. Donner l'heure demande du travail
18. Avancer lentement sans rien casser
19. La vie privée n'est pas morte
20. Les cypherpunks écrivent du code
21. Métaphores pour le futur de Bitcoin

Les leçons suivantes traitent de l'éthique du développement technologique de Bitcoin, un aspect potentiellement aussi important que la technologie elle-même. Bitcoin, ce n'est pas la prochaine appli à la mode sur votre téléphone. C'est la base d'une nouvelle réalité économique, ce qui explique qu'il devrait être considéré comme un logiciel financier de qualité nucléaire.

Où en sommes-nous de cette révolution financière, sociétale et technologique ? Les réseaux et technologies du passé peuvent figurer des métaphores au futur de Bitcoin, que nous aborderons dans la toute dernière leçon de ce chapitre.

Une dernière fois, attachez vos ceintures et profitez de la descente. Comme toutes les technologies exponentielles, nous allons devenir paraboliques.

15. La force dans les nombres

> *« Voyons un peu : quatre fois cinq font douze, quatre fois six font treize, et quatre fois sept font... Oh ! mon Dieu ! jamais je n'arriverai jusqu'à vingt à cette allure ! »*
> – Lewis Carroll, *Alice au pays des merveilles*

Les nombres sont indispensables à notre vie quotidienne. Les grands nombres, en revanche, sont peu familiers à la plupart d'entre nous. Les plus grands nombres que l'on rencontrera généralement au jour le jour seront de l'ordre des millions, des milliards voire des billions [1]. On pourra par exemple parler de millions de gens dans la misère, de milliards de dollars dépensés à renflouer les banques ou encore de billions de dette publique. Malgré la difficulté à se représenter ce genre de gros titres, nous sommes relativement à l'aise avec l'ordre de grandeur de ces nombres.

Même si nous sommes familiers avec les milliards et les billions, notre intuition fait déjà défaut face à leur magnitude. Avez-vous une idée du temps qu'il faut pour qu'un million, milliard ou billion de secondes ne s'écoulent ? Si vous êtes comme moi, vous êtes perdu si vous ne faites pas les calculs.

Creusons cet exemple : la différence entre chaque représente trois ordres de magnitude ; 10^6, 10^9, 10^{12}. Ce n'est pas très utile de penser en secondes, alors transformons-les afin de pouvoir les appréhender :

— 10^6 : Un million de secondes représentent la dernière semaine et demie.

1. NdT : *billion* est la traduction de l'anglais *trillion*.

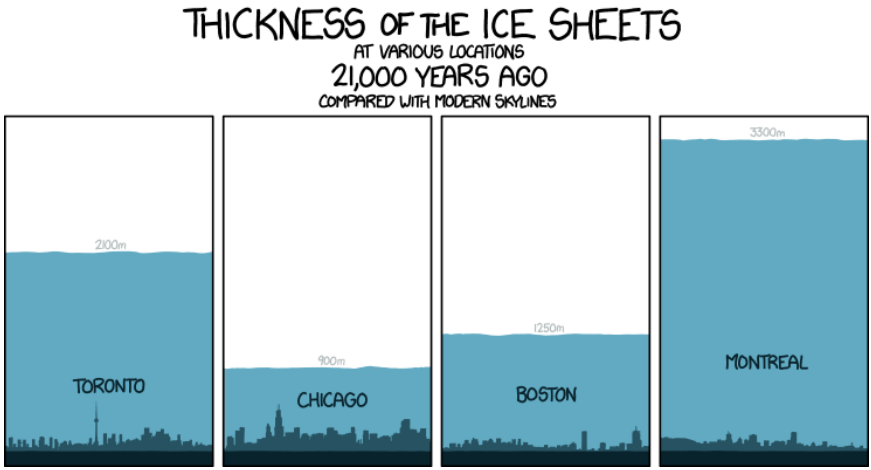


FIGURE 15.1. – Il y a environ 1 billion de secondes. Source : xkcd 1225

— 10^9 : Un milliard de secondes représentent les 32 dernières années.
— 10^{12} : Il y a un billion de secondes, Manhattan était couverte d'une épaisse couche de glace [2].

Au moment où nous entrons dans les échelles astronomiques de la cryptographie moderne, notre instinct échoue dans les grandes largeurs. Bitcoin est bâti autour des grands nombres et de l'impossibilité virtuelle à les deviner. Ces nombres sont bien, bien plus grands que ceux qu'on peut rencontrer au quotidien. Plus grands de beaucoup d'ordres de magnitude. Il est indispensable d'appréhender à quel point ces nombres sont réellement grands pour pouvoir comprendre Bitcoin dans son ensemble.

Prenons comme exemple concret SHA-256 [3], l'une des fonc-

2. Un billion de secondes (10^{12}) représentent les 31710 dernières années. Le Dernier Maximum Glaciaire a eu lieu il y a 33,000 ans. [88]

3. SHA-256 fait partie de la famille des fonctions de hachage cryptographique SHA-2 développée par la NSA. [97]

tions de hachage[4] utilisée par Bitcoin. Il est naturel de se dire que 256 bits ne sont que « deux cent cinquante-six », ce qui n'est pas du tout un grand nombre. Pourtant, le nombre dans SHA-256 représente des ordres de magnitude – une chose pour laquelle nos cerveaux ne sont pas équipés.

Bien que le nombre de bits soit une métrique appropriée, le vrai sens d'une sécurité 256-bit se perd dans l'interprétation. À l'image des millions (10^6) et des milliards (10^9) ci-dessus, le nombre dans SHA-256 parle d'ordres de magnitude (2^{256}).

Mais alors à quel point SHA-256 est-il solide, au juste ?

> « SHA-256 est très solide. Ce n'est pas incrémental comme passer de MD5 à SHA1. Ça pourrait prendre plusieurs décennies avant une attaque massive révolutionnaire. »
>
> – Satoshi Nakamoto[5]

Appelons un chat un chat. 2^{256} représente ce nombre :

> 115 duodecilliards 792 duodecillions 89 undecilliards 237 undecillions 316 decilliards 195 decillions 423 nonilliards 570 nonillions 985 octilliards 8 octillions 687 septilliards 907 septillions 853 sextilliards 269 sextillions 984 quintilliards 665 quintillions 640 quadrilliards 564 quadrillions 39 trilliards 457 trillions 584 billiards 7 billions 913 milliards 129 millions 639 mille 936.

Ça fait un paquet de quintillions ! Se faire une idée de ce nombre est somme toute impossible. Il n'existe rien dans l'univers physique à quoi le comparer. Ça représente bien plus que le nombre d'atomes de l'univers observable. Le cerveau humain n'est tout simplement pas fait pour le comprendre.

4. Bitcoin utilise SHA-256 dans son algorithme de hachage de bloc. [12]

5. Satoshi Nakamoto, dans une réponse aux questions sur les collisions SHA-256. [54]

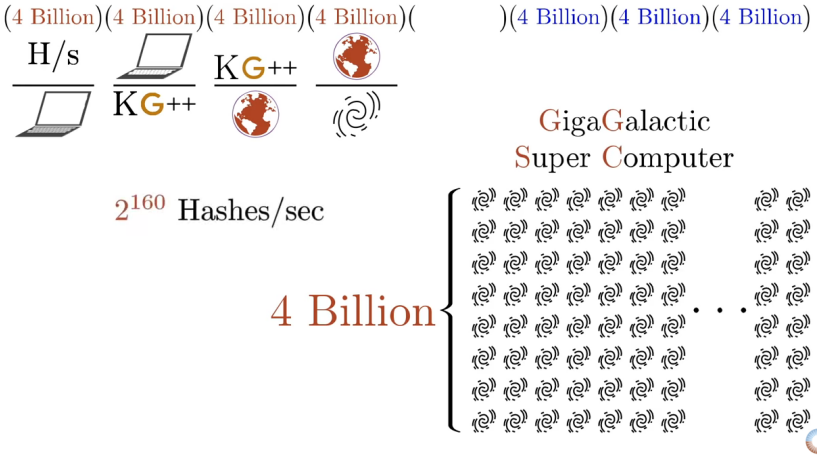


FIGURE 15.2. – Illustration de la sécurité dans SHA-256. Schéma original de Grant Sanderson alias 3Blue1Brown.

On trouve l'une des meilleures représentations de la vraie force de SHA-256 dans une vidéo de Grant Sanderson. Judicieusement nommée *« À quel point la sécurité 256-bit est-elle sûre ? »* [6], elle montre parfaitement l'immensité d'un espace de cette taille. Rendez-vous service et prenez cinq minutes pour la regarder. Comme toutes les vidéos de *3Blue1Brown* celle-ci est tout autant fascinante qu'exceptionnellement bien faite. Mais attention : vous pourriez bien tomber dans un terrier de lapin mathématique.

Bruce Schneier [65] s'est servi des limites physiques de l'informatique afin de relativiser ce nombre : même si nous parvenions à construire un ordinateur optimal, qui utiliserait sans perte l'énergie fournie pour manipuler les bits [87], que nous construisions une sphère de Dyson [7] autour du Soleil et que nous les

6. Regardez la vidéo sur `https://youtu.be/S9JGmA5_unY`
7. Une sphère de Dyson est une mégastructure hypothétique qui entoure

laissions tourner pendant 100 milliards de milliards d'années, nous n'aurions que 25% de chances de trouver une aiguille dans une botte de 256 bits.

> « Ces nombres n'ont rien à voir avec la technologie des appareils ; ce sont les maximums autorisés par la thermodynamique. Et ils suggèrent fortement que les attaques par force brute contre des clés de 256 bits ne seront pas envisageables avant que les ordinateurs ne soient faits d'autre chose que la matière et occupent autre chose que l'espace. »
>
> – Bruce Schneier [8]

On ne peut surestimer la profondeur de ces mots. Une cryptographie solide renverse l'équilibre des pouvoirs du monde physique auquel nous sommes habitués. Dans notre réalité, les choses incassables n'existent pas. Si vous y mettez assez de force, vous pourrez ouvrir n'importe quelle porte, boîte ou coffre au trésor.

Le coffre au trésor de Bitcoin est très différent. Il est protégé par une cryptographie solide, qui ne laisse pas la place à la force brute. Tant que les hypothèses mathématiques sous-jacentes s'appliqueront, nous n'aurons que cette force brute à notre disposition. Bon, d'accord, il y a aussi l'option d'une attaque globale à la clé à molette à 5$ (Figure 15.3). Mais la torture ne fonctionnera pas pour toutes les adresses bitcoin et les remparts cryptographiques de bitcoin mettront en échec les attaques par force brute. Même si vous attaquez avec la puissance d'un millier d'étoiles. Littéralement.

Ce fait et ses répercussions ont été résumés de façon bouleversante dans l'appel aux armes cryptographiques : *« Aucune force coercitive ne résoudra jamais un problème de maths. »*

---

totalement une étoile et capture un grand pourcentage de son énergie. [81]

8. Bruce Schneier, *Cryptographie appliquée* [64]

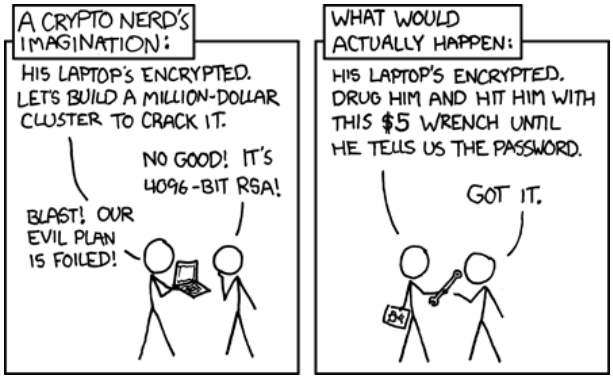


FIGURE 15.3. – Attaque à la clé à molette à 5$. Source : xkcd 538

> « Ça n'avait rien d'évident, que le monde finirait par fonctionner comme ça. Mais d'une façon ou d'une autre, l'univers sourit au chiffrement. »
>
> – Julian Assange [9]

Personne ne sait encore avec certitude si le sourire de l'univers est authentique. Il est possible que notre hypothèse des asymétries mathématiques soit fausse et que nous découvrions qu'en réalité P est égal à NP [95] ou que nous trouvions étonnamment rapidement une solution à des problèmes spécifiques [79] que nous estimons actuellement complexes. Si cela devait arriver, la cryptographie telle que nous la connaissons disparaîtrait et les conséquences changeraient sans doute radicalement la face du monde.

« Vires in Numeris » = « Les forces dans les nombres » [10]

Vires in numeris n'est pas qu'un slogan accrocheur pour les bitcoiners. La prise de conscience d'une force inimaginable pré-

9. Julian Assange, *Un appel aux armes cryptographiques* [5]

10. *Vires in Numeris* à été proposé comme devise de Bitcoin pour la première fois par l'utilisateur de bitcointalk *epii* [25]

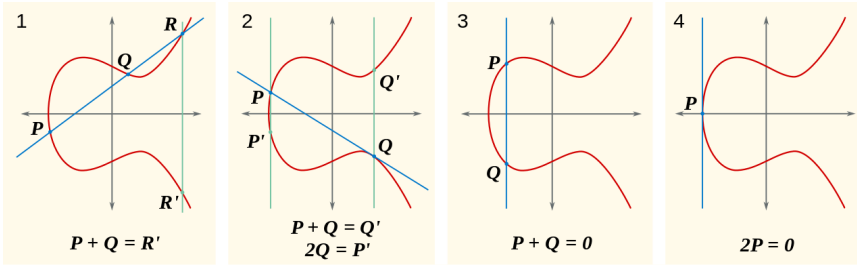


FIGURE 15.4. – Exemples de courbes elliptiques. Crédit schéma CC-BY-SA Emmanuel Boutet.

sente dans les nombres est intense. En faire l'expérience et comprendre l'inversion dans l'équilibre des pouvoirs existants qui en découle a changé ma façon de voir le monde et l'avenir qui nous attend.

Un effet direct de cela, c'est que vous n'avez pas à demander la permission à quiconque pour participer à Bitcoin. Il n'y a pas de page d'inscription, pas d'entreprise qui en est responsable, pas d'agence publique à qui envoyer les formulaires. Générez simplement un grand nombre et vous êtes à peu près paré à y aller. L'autorité centrale sur la création des comptes, ce sont les mathématiques. Et Dieu seul sait qui en est responsable.

Bitcoin est bâti sur notre meilleure compréhension de la réalité. Certes, il reste bien des problèmes non-résolus en physique, en informatique et en mathématiques, mais il y a des choses dont nous sommes plutôt sûrs. Qu'il y ait une asymétrie entre trouver des solutions et valider la justesse de ces solutions en est une. Que les calculs requièrent de l'énergie en est une autre. En d'autres termes : trouver une aiguille dans une botte de foin est plus difficile que de vérifier si le truc pointu dans votre main est bien une aiguille. Et trouver l'aiguille prend du temps.

L'immensité de l'espace d'adressage de Bitcoin est vraiment ahurissante. Le nombre de clés privées l'est encore plus. C'est fascinant de se rendre compte à quel point notre monde mo-

derne se résume à l'improbabilité de trouver une aiguille dans une botte de foin incommensurable. J'en suis conscient plus que jamais, dorénavant.

Bitcoin m'a appris que les nombres renfermaient de la puissance.

16. Remarques sur « Ne vous fiez pas, vérifiez »

« Préparez-vous à entendre les témoignages, »
dit le Roi, « et ensuite la sentence ! »
– Lewis Carroll, *Les aventures d'Alice sous terre*

Bitcoin cherche à remplacer, ou tout du moins fournir une alternative aux monnaies conventionnelles. Ces monnaies sont liées à une autorité centrale, peu importe que l'on parle d'un cours légal comme le dollar américain ou des V-Bucks de Fortnite. Dans les deux cas, vous êtes tenus de faire confiance à une autorité centrale pour émettre, gérer et faire circuler votre argent. Bitcoin rompt ce lien et résout cette préoccupation principale : la question de la *confiance*.

> « Le problème fondamental des monnaies traditionnelles, c'est toute la confiance nécessaire à son fonctionnement. [...] Ce dont nous avons besoin, c'est d'un système de paiement électronique basé sur la preuve cryptographique au lieu de la confiance »
>
> – Satoshi Nakamoto [1]

Bitcoin remédie au problème de la confiance en étant totalement décentralisé, sans serveur central ni parties de confiance. Pas seulement sans *tierces* parties de confiance, mais sans parties de confiance tout court. Quand il n'y a pas d'autorité centrale, il n'y a *personne* à qui faire confiance, tout simplement. L'innovation c'est la décentralisation totale. C'est la source de la

1. Satoshi Nakamoto, annonce officielle de Bitcoin [51] et livre blanc [48]

ténacité de Bitcoin, la raison pour laquelle il est toujours en vie. C'est aussi ce qui explique pourquoi nous avons du minage, des nœuds, des portefeuilles physiques et oui, la blockchain. La seule chose à laquelle vous devez faire « confiance », c'est le fait que notre connaissance des mathématiques et de la physique n'est pas totalement à côté de la plaque et que la majorité des mineurs sont honnêtes (et ils sont incités à l'être).

Tandis que le monde normal part du postulat *« fiez vous, mais vérifiez »*, Bitcoin se fonde sur le postulat *« ne vous fiez pas, vérifiez »*. Satoshi a très clairement insisté sur l'importance de se passer de la confiance à la fois dans l'introduction et la conclusion du livre blanc de Bitcoin.

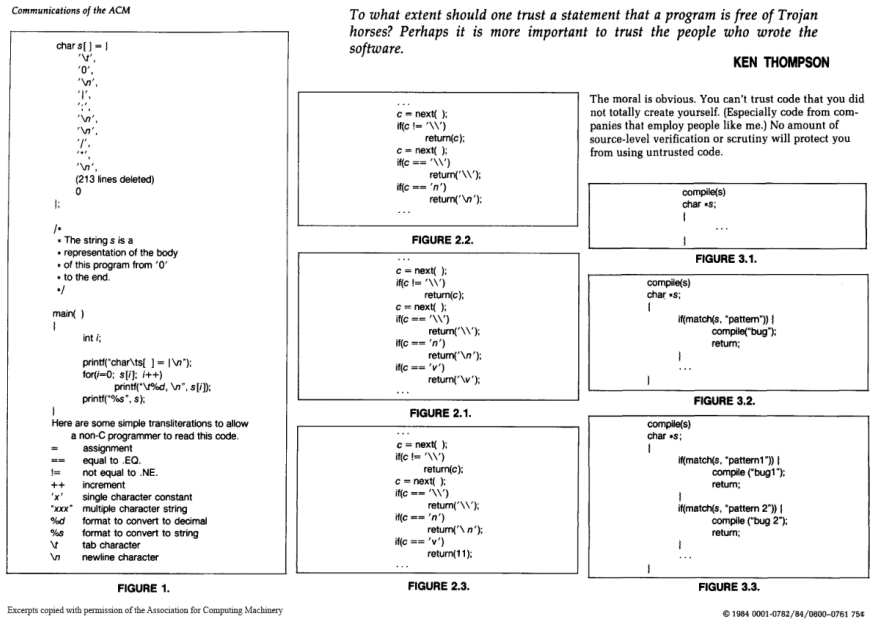
> « Conclusion : nous avons proposé un système de transactions électroniques se passant de confiance. »
>
> – Satoshi Nakamoto [2]

Notez que *se passant de confiance* est utilisé dans un contexte très particulier. Nous parlons des tierces parties de confiance, c'est-à-dire d'autres entités à qui vous vous fiez pour produire, détenir et traiter votre argent. On partira par exemple du principe que vous pouvez faire confiance à votre ordinateur.

Comme Ken Thompson l'a montré dans sa conférence au Turing Award, la confiance est une chose extrêmement délicate en informatique. Quand vous lancez un programme, vous devez vous fier à toutes sortes de logiciels (et de matériels) qui, en théorie, pourraient modifier ce programme par malveillance. Pour citer Thompson dans *Remarques sur la confiance envers la confiance* : « La morale est évidente. Vous ne pouvez pas faire confiance à du code que vous n'avez pas entièrement écrit. » [70]

Thompson a démontré que même si vous avez accès au code source, votre compilateur — ou tout autre programme ou matériel d'exécution — pourrait être corrompu et que la détection de

2. Satoshi Nakamoto, livre blanc de Bitcoin [48]



Communications of the ACM

```
char s[ ] = {
        '\t',
        '0',
        '\n',
        '}',
        ',',
        '\n',
        '\n',
        '/',
        '*',
        ' ',
        '\n',
        (213 lines deleted)
        0
};

/*
 * The string s is a
 * representation of the body
 * of this program from '0'
 * to the end.
 */

main( )
{
        int i;

        printf("char\ts[ ] = {\n");
        for(i=0; s[i]; i++)
                printf("\t%d, \n", s[i]);
        printf("%s", s);
}
```

Here are some simple transliterations to allow a non-C programmer to read this code.

=	assignment
==	equal to .EQ.
!=	not equal to .NE.
++	increment
'x'	single character constant
"xxx"	multiple character string
%d	format to convert to decimal
%s	format to convert to string
\t	tab character
\n	newline character

FIGURE 1.

Excerpts copied with permission of the Association for Computing Machinery

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\n');
...
```

FIGURE 2.2.

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\n');
if(c == 'v')
        return('\v');
...
```

FIGURE 2.1.

```
...
c = next( );
if(c != '\\')
        return(c);
c = next( );
if(c == '\\')
        return('\\');
if(c == 'n')
        return('\ n');
if(c == 'v')
        return(11);
...
```

FIGURE 2.3.

The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code.

```
compile(s)
char *s;
{
        ...
}
```

FIGURE 3.1.

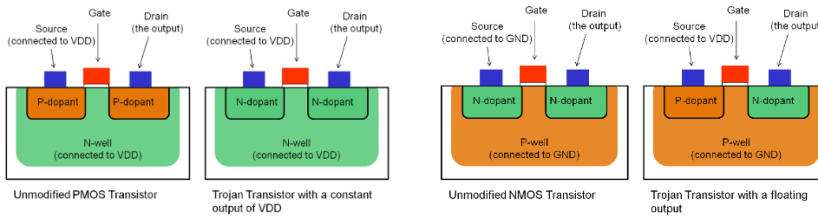
```
compile(s)
char *s;
{
        if(match(s, "pattern")) {
                compile("bug");
                return;
        }
        ...
}
```

FIGURE 3.2.

```
compile(s)
char *s;
{
        if(match(s, "pattern1")) {
                compile ("bug1");
                return;
        }
        if(match(s, "pattern 2")) {
                compile ("bug 2");
                return;
        }
        ...
}
```

FIGURE 3.3.

FIGURE 16.1. – Extraits de l'article de Ken Thompson 'Remarques sur la confiance envers la confiance'



(a) p-MOS Transistor (b) n-MOS Transistor

FIGURE 16.2. – Chevaux de Troie matériels furtifs de niveau dopant par Becker, Regazzoni, Paar, Burleson

cette porte dérobée serait très délicate. Par conséquent, en pratique, un système sans aucun *besoin de confiance* n'existe pas. Pour ça vous auriez à créer tous vos logiciels (assembleurs, compilateurs, éditeurs de liens, etc.) *et* tout votre matériel de bout en bout, sans l'aide d'un quelconque logiciel externe ou machine programmable.

> « Si vous voulez faire une tarte aux pommes à partir de rien, vous devez d'abord inventer l'univers. »
>
> – Carl Sagan [3]

Le piratage de Ken Thompson consiste en une porte dérobée particulièrement astucieuse et difficile à détecter, qui fonctionne sans modifier aucun logiciel. Des chercheurs ont trouvé le moyen de corrompre du matériel critique à la sécurité en manipulant la polarité des impuretés dans le silicium. [9] Ils ont alors été capables de compromettre un générateur cryptographique de nombres aléatoires, juste en modifiant les propriétés physiques du truc dont sont faites les puces électroniques. Et puisque cette modification est invisible, la porte dérobée est indétectable à la vérification optique, l'un des mécanismes de détection de sabotage les plus utilisés pour ce genre de puces.

3. Carl Sagan, *Cosmos* [63]

Ça vous fait peur ? Eh bien, même si vous étiez capable de tout fabriquer et programmer à partir de rien, vous devriez quand même faire confiance aux mathématiques sous-jacentes. Il vous faudrait être convaincu que *secp256k1* est une courbe elliptique sans porte dérobée. Oui, des portes dérobées malveillantes peuvent être insérées dans les fondations mathématiques des fonctions cryptographiques et c'est vraisemblablement déjà arrivé au moins une fois. [80] Il y a de quoi être paranoïaque pour de bonnes raisons et le fait que tout, depuis votre matériel, en passant par vos logiciels, jusqu'aux courbes elliptiques que l'on utilise, peut receler une porte dérobée [82] en fait partie.

> « Ne vous fiez pas. Vérifiez. »
>
> – Des bitcoiners, un peu partout

Les exemples ci-dessus ont pour but d'illustrer que l'informatique *sans confiance* est utopique. Bitcoin est sans doute le seul système qui effleure cette utopie et pourtant, il est *à confiance réduite* — visant à l'éliminer partout où c'est possible. On peut soutenir que la chaîne de confiance est infinie, puisque vous devrez également vous convaincre que les calculs demandent de l'énergie, que P n'est pas égal à NP et que vous vivez bien dans la réalité et pas dans une simulation orchestrée par des acteurs malveillants.

Des développeurs travaillent sur des outils et des procédures cherchant à minimiser encore plus toute confiance restante. Par exemple, les développeurs de Bitcoin ont créé Gitian [4], qui est une méthode de diffusion de logiciels permettant de faire des compilations déterministes. L'idée, c'est que les chances de manipulation malveillante sont réduites lorsque plusieurs développeurs parviennent à reproduire des exécutables identiques. Mais les portes dérobées imaginaires ne sont pas le seul vecteur d'attaque. Un simple chantage ou de l'extorsion sont des menaces

4. `https://gitian.org/`

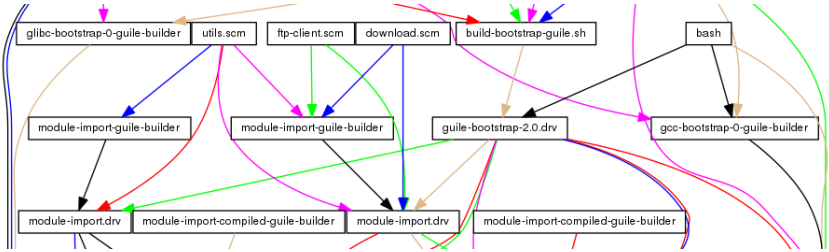


FIGURE 16.3. – Qui était là le premier, l'œuf ou la poule ?

bien réelles. Comme dans le protocole principal, la décentralisation sert à réduire la confiance nécessaire.

Divers efforts sont déployés afin de résoudre le problème de l'amorçage, similaire à celui de l'œuf et de la poule, brillamment mis en évidence par le piratage de Ken Thompson [20]. Guix [5] (à prononcer *geeks*), qui utilise une gestion de paquets fonctionnellement déclarés et permet dès la conception une compilation reproductible bit à bit, est un de ces efforts. Il en résulte que vous n'avez plus à faire confiance aux serveurs qui vous fournissent les logiciels, puisque vous pouvez vérifier par vous-même que l'exécutable fourni est intact en le recompilant de zéro. Une *pull request* a récemment été fusionnée afin d'intégrer Guix dans le procédé de compilation de Bitcoin. [6]

Par chance, Bitcoin ne se repose pas sur un seul algorithme ou une seule sorte de matériel. Une conséquence de la décentralisation radicale de Bitcoin, c'est un modèle de sécurité distribué. Bien que les portes dérobées précédemment décrites doivent être prises au sérieux, il est improbable que chaque portefeuille logiciel, chaque portefeuille matériel, chaque bibliothèque de fonctions cryptographiques, chaque implémentation de nœud et chaque compilateur de chaque langage soient compromis. C'est possible,

5. `https://guix.gnu.org`
6. Voir la PR 15277 de `bitcoin-core` : `https://github.com/bitcoin/bitcoin/pull/15277`

mais très hautement improbable.

Notez par ailleurs que vous pouvez très bien générer une clé privée sans même vous servir d'un quelconque logiciel ou matériel. Vous pouvez tirer un certain nombre de fois à pile ou face [4], mais selon votre style de lancer cette source d'aléatoire ne le sera peut-être pas assez. Ce n'est pas pour rien que des protocoles de stockage comme Glacier [7] recommandent d'utiliser un dé de qualité casino comme une des deux sources d'entropie.

J'ai été forcé par Bitcoin à réfléchir à ce qu'implique réellement de ne se fier à personne. Il m'a sensibilisé au problème de l'amorçage et de la chaîne de confiance implicite dans le développement et l'exécution des programmes. Il m'a fait également prendre conscience des multiples manières de compromettre un logiciel ou un matériel.

Bitcoin m'a appris à ne pas me fier, mais à vérifier.

7. `https://glacierprotocol.org/`

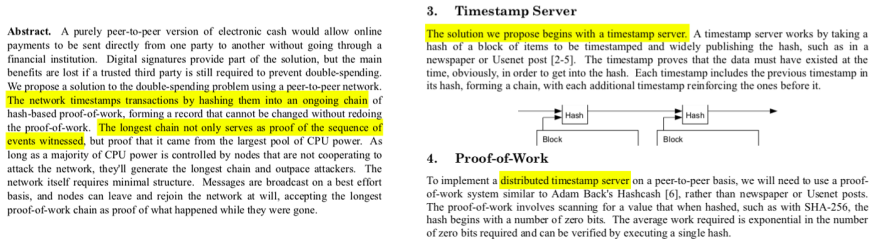
17. Donner l'heure demande du travail

> *« Oh, mon Dieu ! Oh, mon Dieu ! Je vais être en retard ! »*
> – Lewis Carroll, *Alice au pays des merveilles*

On dit souvent qu'on mine des bitcoins parce que des milliers d'ordinateurs travaillent à résoudre des problèmes mathématiques *très complexes*. Des problèmes doivent êtres résolus et si vous calculez la bonne réponse, vous « produisez » un bitcoin. Bien que cette vision simplifiée du minage de bitcoin soit plus facile à exprimer, elle passe un peu à côté du sujet. Les bitcoins ne sont pas produits ou créés et toute la difficulté ne consiste pas réellement à résoudre certains problèmes de maths. En plus, les maths en question ne sont pas particulièrement complexes. Ce qui l'est, c'est de *donner l'heure* dans un système décentralisé.

Comme le démontre le livre blanc, le système de preuve de travail (alias le minage) est une manière d'implémenter un serveur d'horodatage distribué.

Au début, lorsque j'étudiais le fonctionnement de Bitcoin, j'ai



Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

Hash Hash
Block Block

4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

FIGURE 17.1. – Extraits du livre blanc. Ai-je entendu « time-chain » ?

moi aussi pensé que la preuve de travail était inefficace et générait du gaspillage. Au bout d'un moment, j'ai commencé à changer de point de vue sur la consommation d'énergie de Bitcoin [29]. Il semblerait qu'aujourd'hui, en l'an 10 ap. B (après Bitcoin), la preuve de travail soit toujours largement incomprise.

Beaucoup de gens semblent croire que c'est un travail *inutile*, puisque les problèmes à résoudre par la preuve de travail sont inventés. Si l'on se focalise uniquement sur les calculs, c'est compréhensible d'arriver à cette conclusion. Mais Bitcoin n'est pas une question de calculs. C'est une question de *s'accorder indépendamment sur l'ordre des choses.*

La preuve de travail est un système dans lequel chacun peut valider ce qui s'est passé et dans quel ordre. Cette validation indépendante est la source du consensus, un accord unique entre de multiples parties à propos de qui possède quoi.

Dans un environnement radicalement décentralisé, nous ne possédons pas le luxe du temps absolu. Toute horloge aurait pour effet d'introduire une tierce partie, un point central du système qui pourrait être attaqué et sur lequel il faudrait se reposer. « La mesure du temps est le problème fondamental », comme le souligne Grisha Trubetskoy [72]. Et Satoshi a brillamment résolu ce problème en proposant l'implémentation d'une horloge décentralisée via une chaîne de blocs par preuve de travail. Chacun accepte préalablement que la source de vérité provient de la chaîne avec le plus de travail cumulé. C'est littéralement ce qui s'est passé. Cette entente est dorénavant connue sous le nom de consensus de Nakamoto.

> « Le réseau horodate les transactions en les hachant en une chaîne continue de preuves de travail [...] (qui) sert de preuve par témoignage de la séquence des événements »
>
> – Satoshi Nakamoto [1]

1. Satoshi Nakamoto, livre blanc de Bitcoin [48]

Sans moyen constant pour donner l'heure, il n'existe pas de manière cohérente de distinguer l'avant de l'après. Un ordre fiable est impossible. Comme nous l'avons vu, le consensus de Nakamoto est le chemin qu'a pris Bitcoin pour donner l'heure continuellement. La structure incitative du système produit une horloge probabiliste et décentralisée en se servant à la fois de la cupidité et de l'intérêt personnel des participants qui se concurrencent. L'imprécision de cette horloge n'a aucune importance car à la fin, l'ordre des événements est indiscutable et chacun peut le vérifier.

Grâce à la preuve de travail, la décentralisation radicale touche à la fois le travail *et* la vérification du travail. Chacun peut rejoindre et quitter le réseau à volonté et chacun peut vérifier tout, tout le temps. Non seulement ça, mais chacun peut vérifier l'état du système *personnellement*, sans devoir se fier à quiconque.

Ça prend du temps de comprendre la preuve de travail. C'est bien souvent contre-intuitif et malgré les règles simples, ça donne lieu à des phénomènes plutôt complexes. Personnellement, me focaliser sur le minage m'a aidé. C'est utile, pas inutile. La vérification, pas les calculs. C'est du temps, pas des blocs.

Bitcoin m'a appris que c'était délicat de donner l'heure, surtout quand on est décentralisé.

18. Avancer lentement sans rien casser

> *Aussi la barque serpentait-elle doucement, sous le brillant jour d'été, avec son joyeux équipage et sa musique de voix et d'éclats de rire...*
>
> – Lewis Carroll, *Les aventures d'Alice sous terre*

J'enfonce peut-être des portes ouvertes, mais le monde de la tech fonctionne toujours aujourd'hui en « avançant vite et en cassant des trucs ». L'idée de ne pas s'efforcer à réussir du premier coup est une des bases de la mentalité *échoue tôt, échoue souvent*. Le succès se mesure à la croissance, donc tant que vous grandissez, tout ira bien. Si quelque chose ne fonctionne pas comme prévu vous n'avez qu'à pivoter et itérer. En d'autres termes : si vous jetez assez de merde contre le mur, vous verrez bien ce qui colle.

Bitcoin est très différent. Il l'est dès sa conception. Il est différent par besoin. Satoshi l'a dit lui-même, les monnaies électroniques ont été tentées à de nombreuses reprises et tous ces essais ont échoué car il y avait une tête à faire tomber. L'innovation de Bitcoin, c'est d'être un animal sans tête.

> « Beaucoup de gens refusent par réflexe l'idée des monnaies électroniques à cause de toutes les entreprises qui ont échoué dans les années 90. J'espère qu'il est clair que c'est la nature du contrôle centralisé de ces systèmes qui a causé leur perte. »
>
> – Satoshi Nakamoto [1]

1. Satoshi Nakamoto, dans une réponse à Sepp Hasslberger [52]

Une des conséquences de cette décentralisation radicale est la résistance inhérente au changement. « Avancer vite en cassant des trucs » ne fonctionne et ne fonctionnera jamais sur la couche de base de Bitcoin. Même si on le voulait, ce ne serait pas possible sans convaincre *tout le monde* de changer sa façon de faire. Voilà ce qu'est le consensus distribué. Voilà la nature de Bitcoin.

> « La nature de Bitcoin est telle qu'une fois sortie la version 0.1, les concepts essentiels étaient gravés dans le marbre pour le restant de ses jours. »
>
> – Satoshi Nakamoto [2]

C'est l'une des nombreuses propriétés paradoxales de Bitcoin. Nous avons tous fini par croire que tout logiciel peut facilement être modifié. Mais la nature de cet animal rend tout changement sacrément difficile.

Comme Hasu l'écrit élégamment dans Décortiquer le contrat social de Bitcoin [32], on ne peut changer ses règles qu'en *proposant* un changement et par conséquent en *convainquant* tous les utilisateurs de Bitcoin de l'adopter. Bien qu'il soit un logiciel, cela rend Bitcoin très résilient au changement.

Cette résilience est l'un des attributs de Bitcoin les plus importants. Les systèmes logiciels critiques se doivent d'être antifragile, ce qui est garanti par l'interaction entre les couches sociales et techniques de Bitcoin. Les systèmes monétaires sont agressifs par nature et nous le savons depuis des milliers d'années, un environnement agressif requiert des fondations solides.

> « La pluie est tombée, les torrents sont venus, les vents ont soufflé et se sont jetés contre cette maison : elle n'est point tombée, parce qu'elle était fondée sur le roc. »
>
> – Matthieu 7 :25

2. Satoshi Nakamoto, dans une réponse à Gavin Andresen [52]

Vraisemblablement, dans cette parabole des bâtisseurs sages et sots, Bitcoin n'est pas la maison. C'est le roc. Invariable, stable, apportant le socle d'un nouveau système financier.

À l'image des géologues qui savent que les formations rocheuses évoluent et sont toujours en mouvement, on peut s'apercevoir que Bitcoin bouge et évolue. Il faut juste savoir où et comment regarder.

L'introduction du *pay to script hash*[3] et de *segregated witness*[4] sont la preuve que les règles de Bitcoin peuvent être changées tant qu'il y assez d'utilisateurs convaincus que ce changement bénéficie au réseau. SegWit a permis le développement du réseau Lightning[5] qui est l'une des maisons en construction sur le socle solide de Bitcoin. Des mises à jour futures comme les signatures de Schnorr [59] amélioreront l'efficacité et la confidentialité, ainsi que les scripts (comprendre : contrats intelligents) qui seront indiscernables des transactions classiques grâce à Taproot [31]. Les sages bâtisseurs construisent bel et bien sur des fondations solides.

Satoshi n'était pas seulement un sage bâtisseur de technologie. Il comprenait aussi la nécessité de prendre de sages décisions idéologiques.

---

3. Les transactions Pay to Script Hash (P2SH) ont été normalisées dans le BIP16. Elles permettent aux transactions d'être envoyées à un hash de script (adresse commençant par 3) au lieu d'un hash d'adresse publique (adresse commençant par 1). [15]

4. Segregated Witness (abrégé en SegWit) est une mise à jour implémentée du protocole qui vise à fournir une protection envers la plasticité des transactions et à élargir la taille des blocs. SegWit sépare le *témoin* (witness en anglais) de la liste des entrées. [16]

5. `https://lightning.network/`

> « Être open source veut dire que quiconque peut personnellement vérifier le code. Si les sources étaient privées, personne ne pourrait vérifier la sécurité. Je pense qu'un programme de cette nature doit obligatoirement être open source. »
>
> – Satoshi Nakamoto [6]

L'ouverture est primordiale à la sécurité et inhérente à l'open source et au mouvement du logiciel libre. Comme Satoshi le faisait remarquer, les protocoles sécurisés et le code qui les implémente doivent être ouverts — l'obscurité ne procure aucune sécurité. Encore une fois, un autre avantage est lié à la décentralisation : du code qui peut être exécuté, lu, modifié, copié et distribué librement garantit sa diffusion rapide et étendue.

La nature radicalement décentralisée de Bitcoin est ce qui lui permet de se déplacer lentement et sciemment. Un réseau de nœuds, détenus par des individus souverains, est intrinsèquement résistant au changement — malveillant ou pas. Sans possibilité de forcer des mises à jour, la seule façon d'introduire des modifications est de convaincre lentement chacun des participants de l'adopter. Ce procédé décentralisé de proposer et de déployer les changements est ce qui rend le réseau extraordinairement résilient face aux modifications malveillantes. C'est aussi ce qui rend les réparations plus complexes que dans un environnement centralisé et qui explique que tout le monde cherche avant tout à ne rien casser.

Bitcoin m'a appris qu'avancer lentement était une fonctionnalité, pas un bug.

6. Satoshi Nakamoto, dans une réponse à SmokeTooMuch [53]

19. La vie privée n'est pas morte

> *Les joueurs jouaient tous en même temps sans attendre leur tour ; ils se disputaient sans arrêt et s'arrachaient les hérissons. Au bout d'un instant, la Reine, entrant dans une furieuse colère, parcourut le terrain en tapant du pied et en criant : « Qu'on lui coupe la tête ! Qu'on lui coupe la tête ! » à peu près une fois par minute.*
>
> – Lewis Carroll, *Alice in Wonderland*

À en croire les experts, la vie privée est morte depuis les années 80 [1]. L'invention pseudonyme de Bitcoin et d'autres événements de l'histoire récente montrent que ce n'est pas vrai. La vie privée est vivante, bien qu'il ne soit pas facile d'échapper à cet état de surveillance.

Satoshi a pris d'infinies précautions afin de se couvrir et de dissimuler son identité. Dix ans plus tard, personne ne peut dire si Satoshi Nakamoto était une personne ou un groupe, un homme, une femme ou un intelligence artificielle venue du futur pour s'auto-amorcer afin de régner sur le monde. Théories complotistes mises à part, Satoshi a choisi de s'identifier à un homme japonais, c'est pourquoi je ne présume de rien en respectant son choix de genre et en le désignant par *il*.

Quelle que soit sa vraie identité, Satoshi a réussi à la cacher. Il a créé un précédent encourageant pour tous ceux qui désirent rester anonymes : c'est possible d'avoir une vie privée en ligne.

1. `https://bit.ly/privacy-is-dead`

FIGURE 19.1. – Je ne suis pas Dorian Nakamoto.

> « Le chiffrement fonctionne. Les systèmes crypto robustes et correctement implémentés sont l'une des rares choses sur lesquelles vous pouvez compter. »
>
> – Edward Snowden [2]

Satoshi n'est pas le premier inventeur pseudonyme ou anonyme et ne sera pas le dernier. Certains ont directement repris son style de publication pseudonyme, comme Tom Elvis Jedusor, connu pour MimbleWimble [71], quand d'autres ont publié des preuves mathématiques avancées en restant totalement anonymes [3].

C'est un nouveau monde étrange que nous habitons. Un monde où l'identité est facultative, où les contributions sont acceptées sur la base du mérite et où les gens peuvent collaborer et négocier librement. Il faudra quelques ajustements pour être à l'aise avec ces nouveaux paradigmes, mais je crois fermement que tout ceci a le potentiel pour rendre le monde meilleur.

Chacun d'entre nous devrait se souvenir que la vie privée est un droit humain fondamental [3]. Tant que le peuple exercera et défendra ces droits, la bataille pour la vie privée sera loin d'être achevée.

Bitcoin m'a appris que la vie privée n'était pas morte.

2. Edward Snowden, réponses au courrier des lecteurs [66]
3. Déclaration universelle des Droits de l'Homme, *Article 12*. [6]

20. Les cypherpunks écrivent du code

> *« Je vois bien que vous essayez d'inventer quelque chose ! »*
> – Lewis Carroll, *Alice au pays des merveilles*

Comme beaucoup de grandes idées, Bitcoin n'est pas sorti de nulle part. Il a vu le jour en utilisant et en combinant beaucoup d'innovations et de découvertes en mathématiques, en physique, en informatique et dans d'autres domaines. Satoshi est sans conteste un génie mais il n'aurait pas pu inventer Bitcoin sans se tenir sur des épaules de géants.

> « Celui qui simplement souhaite et espère n'intervient pas activement dans le cours des événements ni dans le profil de sa destinée. »
>
> – Ludwig von Mises [1]

L'un de ces géants, c'est Eric Hughes, un des fondateurs du mouvement cypherpunk et auteur du *Manifeste d'un Cypherpunk*. Ça paraît difficile d'imaginer que Satoshi n'ait pas été influencé par ce manifeste. Il parle de tellement de choses que Bitcoin permet et utilise, telles que les transactions privées directes, l'argent électronique et liquide, les systèmes anonymes et la protection de la vie privée par la cryptographie et les signatures numériques.

1. Ludwig von Mises, *L'Action Humaine* [74]

> « La confidentialité est nécessaire pour une société ouverte à l'ère électronique. [...] Puisque nous désirons la confidentialité, nous devons nous assurer que chaque partie à une transaction n'a connaissance que de ce qui est directement nécessaire à cette transaction. [...] Par conséquent, la vie privée dans une société ouverte nécessite des systèmes de transaction anonymes. Jusqu'à présent, l'argent liquide a été le principal système de ce type. Un système de transaction anonyme n'est pas un système de transaction secret. [...] Nous les Cypherpunks sommes dédiés à la construction de systèmes anonymes. Nous défendons notre vie privée avec la cryptographie, avec des systèmes de transfert de courrier anonyme, avec des signatures numériques et avec de la monnaie électronique. Les Cypherpunks écrivent du code. »
>
> – Eric Hughes [2]

Les Cypherpunks ne trouvent pas de réconfort dans les espoirs et les vœux. Ils s'immiscent activement dans le cours des événements et forgent leur propre destinée. Les Cypherpunks écrivent du code.

Et donc, en fidèle cypherpunk, Satoshi s'est assis et s'est mis à coder. Du code parti d'une idée abstraite pour prouver au monde qu'elle pouvait marcher. Du code semant la graine d'une nouvelle réalité économique. Grâce au code, chacun peut vérifier que ce système novateur fonctionne vraiment et qu'à peu près toutes les 10 minutes, Bitcoin prouve au monde qu'il est encore vivant.

Afin de s'assurer que son invention ne resterait pas du domaine du rêve, Satoshi a écrit le code de son idée avant d'écrire

2. Eric Hughes, Manifeste d'un Cypherpunk [37]

```
23  map<uint256, CBlockIndex*> mapBlockIndex;
24  const uint256 hashGenesisBlock("0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f");
25  CBlockIndex* pindexGenesisBlock = NULL;
26  int nBestHeight = -1;
27  uint256 hashBestChain = 0;
28  CBlockIndex* pindexBest = NULL;
    ⋮
675 int64 CBlock::GetBlockValue(int64 nFees) const
676 {
677     int64 nSubsidy = 50 * COIN;
678
679     // Subsidy is cut in half every 4 years
680     nSubsidy >>= (nBestHeight / 210000);
681
682     return nSubsidy + nFees;
683 }
684
685 unsigned int GetNextWorkRequired(const CBlockIndex* pindexLast)
686 {
687     const unsigned int nTargetTimespan = 14 * 24 * 60 * 60; // two weeks
688     const unsigned int nTargetSpacing = 10 * 60;
689     const unsigned int nInterval = nTargetTimespan / nTargetSpacing;
690
691     // Genesis block
692     if (pindexLast == NULL)
693         return bnProofOfWorkLimit.GetCompact();
```

FIGURE 20.1. – Extraits du code de la version 0.1 de Bitcoin

le livre blanc. Il a aussi pris soin de ne pas retarder [3] chaque version indéfiniment. Après tout, « il y aura toujours autre chose à faire ».

> « J'ai dû écrire tout le code avant d'être convaincu que je pouvais résoudre chaque problème, puis j'ai écrit le livre blanc. »
>
> – Satoshi Nakamoto [4]

Dans ce monde aux promesses infinies et au déroulement douteux, la mise en pratique d'un développement dévoué manquait cruellement. Soyez volontaires, persuadez-vous d'être capable de résoudre les problèmes et implémentez les solutions. On devrait tous essayer d'être un peu plus cypherpunk.

3. « Nous ne devrions pas reporter indéfiniment tant que chaque fonction n'est pas terminée. » – Satoshi Nakamoto [55]
4. Satoshi Nakamoto, dans Re : Bitcoin P2P e-cash paper [49]

Bitcoin m'a appris que les cypherpunks écrivaient du code.

21. Métaphores pour le futur de Bitcoin

> *« Je sais qu'il arrive toujours quelque chose d'intéressant... »*
> – Lewis Carroll, *Alice au pays des merveilles*

Au cours des deux dernières décennies, il est devenu évident que l'innovation technologique ne suivait pas une courbe linéaire. Que vous croyiez ou pas à la singularité technologique, le progrès est indéniablement exponentiel dans de nombreux domaines. En plus de ça, le taux d'adoption des technologies s'accélère et sans vous en rendre compte, le buisson de la cour d'école du coin a disparu car vos enfants utilisent Snapchat à la place. Les courbes exponentielles ont cette tendance à vous exploser au visage bien avant que vous ne l'ayez vu venir.

Bitcoin est une technologie exponentielle reposant sur d'autres technologies exponentielles. *Our World in Data*[1] montre admirablement la vitesse croissante de l'adoption technologique à partir de 1903 avec l'arrivée des lignes téléphoniques (voir la Figure21.1). Les lignes téléphoniques, l'électricité, les ordinateurs, Internet, les smartphones ; tous observent des tendances exponentielles en termes de qualité-prix et d'adoption. C'est pareil pour Bitcoin [22].

Bitcoin possède de multiples effets de réseau[2] découlant tous de configurations de croissance exponentielle dans leurs propres domaines : le prix, les usagers, la sécurité, les développeurs, la part de marché et l'adoption comme monnaie globale.

1. `https://ourworldindata.org/`
2. Trace Mayer, *Les sept effets de réseau de Bitcoin* [43]

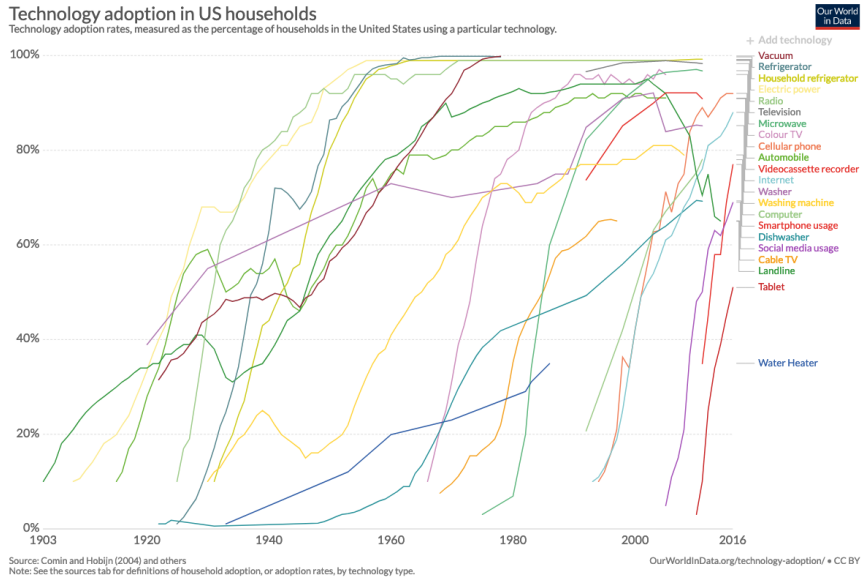


FIGURE 21.1. – Bitcoin est littéralement hors-normes.

En ayant survécu à ses premiers pas, Bitcoin continue de grandir chaque jour dans plus d'un aspect. D'accord, sa technologie n'est pas encore mature. Il est sans doute en pleine adolescence. Mais si la technologie est exponentielle, passer de l'ombre à l'omniprésence sera un court chemin.

Dans sa conférence TED de 2003, Jeff Bezos a choisi l'électricité comme métaphore au futur du web[3]. Ces trois phénomènes — l'électricité, Internet, Bitcoin — sont des technologies *habilitantes*, des réseaux qui facilitent autre chose. Ce sont des infrastructures fondamentales, qui permettent de bâtir.

Ça fait un moment que nous côtoyons l'électricité. On la prend pour acquise. Internet est un peu plus jeune mais la plupart des gens le prennent aussi pour acquis. Bitcoin a dix ans et n'a pénétré les consciences que durant le dernier cycle d'engouement.

3. `http://bit.ly/bezos-web`

FIGURE 21.2. – Le téléphone mobile, env. 1965 contre 2019.

Seuls les pionniers le prennent pour acquis. Plus le temps passera, plus les gens verront Bitcoin comme une chose banale [4].

En 1994, Internet était encore déroutant et contre-intuitif. Il suffit de regarder ce vieil enregistrement du *Today Show* [5] pour voir qu'à l'évidence, ce qui nous paraît naturel et intuitif aujourd'hui ne l'était en fait pas à l'époque. Pour la plupart, Bitcoin reste encore déroutant et étrange, mais tout comme Internet est une seconde nature pour les natifs du numérique, dépenser et accumuler des sats [6] le sera pour les natifs du Bitcoin dans le futur.

> « Le futur est déjà là — il n'est simplement pas réparti équitablement. »
>
> – William Gibson [7]

En 1995, environ 15% des adultes américains utilisaient Internet. Les données historiques du centre de recherches Pew [27]

4. Ceci est connu sous le nom d'*effet Lindy*. L'effet Lindy est la théorie selon laquelle l'espérance de vie future d'une chose non périssable est proportionnelle à son âge actuel, impliquant une espérance de vie restante plus longue à chaque fois qu'elle survit à une période de temps. [89]
5. `https://youtu.be/UlJku_CSyNg`
6. `https://twitter.com/hashtag/stackingsats`
7. William Gibson, *La science dans la science-fiction* [28]

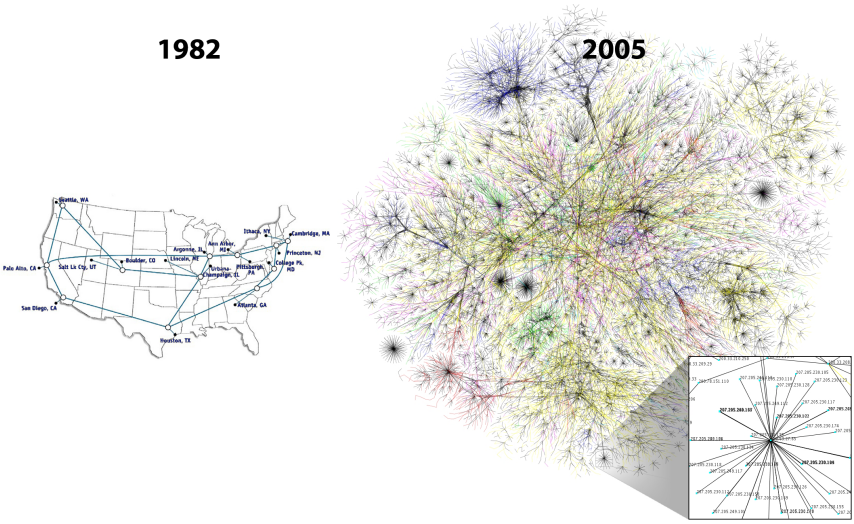


FIGURE 21.3. – Internet, 1982 vs. 2005. Source : CC-BY Merit Network, Inc. et Barrett Lyon, Opte Project

montrent à quel point Internet s'est immiscé dans nos vies. Selon un sondage client de Kaspersky Lab [40], 13% des personnes interrogées se sont servi de Bitcoin ou de ses clones pour payer un bien en 2018. Bien que les paiements ne soient pas l'unique cas d'usage de Bitcoin, cela donne une idée d'où nous en sommes en temps Internet : dans la première moitié des années 90.

En 1997, Jeff Bezos écrivait à ses actionnaires [11] « c'est le premier jour d'Internet », pressentant son gigantesque potentiel inexploité et, par extension, celui de son entreprise. Peu importe à quel jour se trouve Bitcoin, seul l'observateur inattentif ne voit pas clairement les immenses volumes de potentiel inexploité.

Le premier nœud Bitcoin fut mis en ligne en 2009 après que Satoshi mina le *bloc de genèse*[8] et libéra le logiciel dans la na-

8. Le bloc de genèse est le premier bloc de la chaîne de blocs Bitcoin. Les versions modernes de Bitcoin le numérotent 0, alors que les anciennes versions le comptent comme le bloc 1. Le bloc de genèse est habituellement

FIGURE 21.4. – Hal Finney est l'auteur du premier tweet à mentionner bitcoin en janvier 2009.

ture. Son nœud ne fut pas seul très longtemps. Hal Finney fut l'un des premiers à accrocher à l'idée et à rejoindre le réseau. Dix ans plus tard, au moment où j'écris ceci, il y a plus de 75000 nœuds qui exécutent bitcoin.

La couche de base du protocole n'est pas la seule à croître de façon exponentielle. Le réseau Lightning, une technologie de seconde couche, grandit encore plus vite.

En janvier 2018, le réseau Lightning était composé de 40 nœuds et 60 canaux [103]. En avril 2019, le réseau s'était étendu à plus de 4000 nœuds et environ 40000 canaux. N'oubliez pas que ça reste une technologie expérimentale où la perte de fonds peut arriver et arrive parfois. Malgré ça, la tendance est limpide : des milliers de personnes téméraires sont enthousiastes à l'idée de s'en servir.

À mon sens, ayant vécu l'essor météorique du web, les analogies entre Internet et Bitcoin sont évidentes. Ce sont tous deux des réseaux, des technologies exponentielles et tous deux amènent de nouvelles possibilités, de nouvelles industries, de

---

codé en dur dans les applications qui se servent de la chaîne de blocs de Bitcoin. C'est un cas particulier car il ne référence pas de bloc précédent et produit une récompense non-dépensable. Le paramètre *coinbase* contient, entres autres données normales, le texte suivant : *« The Times 03/Jan/2009 Chancellor on brink of second bailout for banks »* [14]

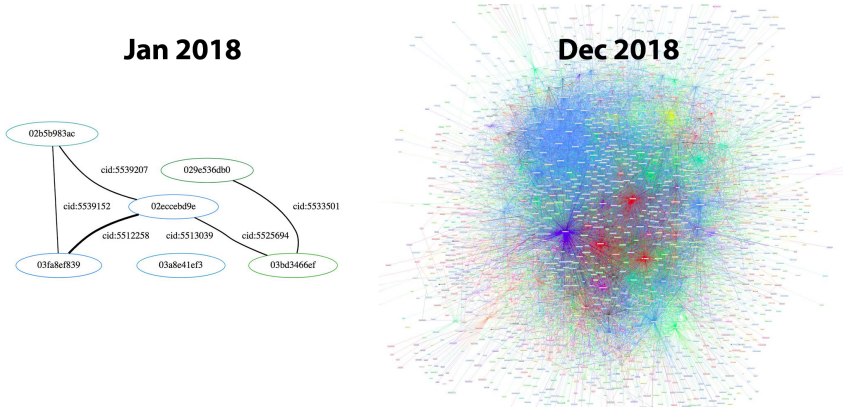


FIGURE 21.5. – Le réseau Lightning, janvier 2018 vs. décembre 2018. Source : Jameson Lopp

nouveaux comportements. L'électricité est la meilleure métaphore pour comprendre la direction que prend Internet, il est donc possible qu'Internet soit la meilleure métaphore pour comprendre la direction que prend Bitcoin. Ou alors, pour reprendre les mots d'Andreas Antonopoulos, Bitcoin est l'*Internet de l'argent*. Ces métaphores sont un très bon rappel d'une Histoire qui ne se répète pas mais qui rime souvent.

Les technologies exponentielles sont difficiles à appréhender et sont souvent sous-estimées. Même si je m'intéresse beaucoup à celles-ci, je suis sans cesse surpris de l'allure du progrès et de l'innovation. Observer la croissance de l'écosystème Bitcoin, ça ressemble à observer l'essor d'Internet, mais en accéléré. C'est grisant.

Ma quête de sens envers Bitcoin m'a mené plus d'une fois sur les chemins de l'Histoire. La compréhension des anciennes structures sociétales, des monnaies du passé et de comment les réseaux de communication ont évolué ont toutes fait partie du voyage. Du biface au smartphone, la technologie a sans nul doute changé notre monde à de nombreuses reprises. Les technolo-

gies de réseaux ont un caractère particulier de transformation : l'écriture, les routes, l'électricité, Internet. Toutes ont changé le monde. Bitcoin a changé le mien et continuera de transformer les esprits et les cœurs de ceux qui osent l'approcher.

Bitcoin m'a appris que la compréhension du passé était nécessaire à la compréhension de son futur. Un futur qui ne fait que commencer...

Considérations finales

Conclusion

> *« Commencez au commencement » dit le Roi d'un ton grave, « et continuez jusqu'à ce que vous arriviez à la fin ; ensuite, arrêtez-vous. »*
> – Lewis Carroll, *Alice au pays des merveilles*

Comme je le disais en introduction, je pense que la réponse à la question *Qu'avez-vous appris de Bitcoin ?* sera toujours incomplète. La symbiose de ce qu'on pourrait appeler de multiples systèmes vivants – Bitcoin, la technosphère et l'économie – est trop entremêlée, les sujets sont trop nombreux et les choses avancent trop vite pour être entièrement comprises par une seule personne.

Même sans le comprendre dans son entièreté et même avec toutes ses excentricités et ses défauts apparents, Bitcoin fonctionne indéniablement. Il continue à produire des blocs à peu près toutes les dix minutes d'une manière admirable. Plus Bitcoin continuera de fonctionner, plus les gens seront enclins à l'utiliser.

> « C'est vrai que les choses sont belles lorsqu'elles fonctionnent. L'art est fonctionnel. »
>
> – Giannina Braschi [9]

Bitcoin est un enfant d'Internet. Sa croissance est exponentielle, gommant les frontières entre les disciplines. Par exemple, l'endroit où finit le royaume purement technologique et où en

9. Giannina Braschi, *L'Empire des rêves* [18]

commence un autre n'est pas clairement établi. Bitcoin a effectivement besoin d'ordinateurs pour fonctionner mais l'informatique ne suffit pas à le comprendre. Non seulement, par ses rouages, Bitcoin ne connaît pas de frontières, mais il n'est pas non plus cloisonné académiquement.

L'économie, la politique, la théorie des jeux, l'histoire monétaire, la théorie des réseaux, la finance, la cryptographie, la théorie de l'information, la censure, la loi et les régulations, les organisations humaines, la psychologie – tout ceci avec bien d'autres champs d'expertise qui pourraient faire avancer la quête de la connaissance de Bitcoin et de son fonctionnement.

Aucune invention n'est seule responsable de son succès. C'est la combinaison de multiples éléments auparavant sans lien qui, collés ensemble par l'incitation de la théorie des jeux, constituent la révolution qu'est Bitcoin. Ce qui fait de Satoshi un génie c'est le sublime mariage de nombreuses disciplines.

Comme tout système complexe, Bitcoin doit faire des compromis en termes d'efficacité, de coût, de sécurité et de bien d'autres aspects. Tout comme il n'y a pas de solution parfaite à la quadrature du cercle, toute solution aux problèmes qu'entend résoudre Bitcoin sera toujours imparfaite.

> « Je ne crois pas que nous pourrons avoir à nouveau une bonne monnaie avant que nous ne la retirions des mains du gouvernement, je veux dire, nous ne pouvons pas la retirer violemment de leur contrôle, tout ce que nous pouvons faire sera de manière rusée et détournée, introduire quelque chose qu'ils ne pourront arrêter. »
>
> – Friedrich Hayek [10]

10. Friedrich Hayek sur la politique monétaire, l'étalon-or, les déficits, l'inflation et John Maynard Keynes `https://youtu.be/EYhEDxFwFRU`

Bitcoin est la manière rusée et détournée de réintroduire une bonne monnaie dans notre monde. Il le fait en plaçant un individu souverain derrière chaque nœud, tout comme De Vinci tentait de résoudre l'inextricable quadrature du cercle en plaçant l'Homme de Vitruve en son centre. Les nœuds retirent en effet tout concept de centre, créant un système incroyablement anti-fragile et extrêmement difficile à stopper. Bitcoin est vivant et son cœur battra probablement plus longtemps que les nôtres.

J'espère que vous avez apprécié ces vingt et une leçons. La leçon la plus importante est peut-être que Bitcoin mérite une approche holistique, sous plusieurs angles, si l'on souhaite en dresser un tableau le moins inachevé possible. De la même façon que l'on détruit un système complexe en retirant un de ses éléments, examiner individuellement chaque partie de Bitcoin semble en gâcher la compréhension. Si une seule personne efface « blockchain » de son vocabulaire et le remplace par « une chaîne de blocs », je pourrai mourir tranquille.

Quoi qu'il en soit, mon voyage n'est pas terminé. J'ai l'intention de m'aventurer encore plus profondément dans le terrier du lapin et je vous invite à me suivre sur le chemin [11].

11. `https://twitter.com/dergigi`

Remerciements

Je remercie les innombrables auteurs et créateurs de contenu qui ont influencé ma pensée sur Bitcoin et les sujets qu'il touche. Il y en a beacoup trop pour tous les citer, mais je vais faire de mon mieux pour les nommer.

— Merci à Arjun Balaji pour le tweet qui m'a motivé à écrire ceci.
— Merci à Marty Bent d'avoir sans cesse fourni des éléments de réflexion et de l'amusement. Si vous ne suivez pas Marty Bent et ses Tales From The Crypt, vous ratez quelque chose. Bravo Matt et Marty de nous guider dans le terrier du lapin.
— Merci à Michael Goldstein et Pierre Rochard d'extraire et de fournir la meilleure littérature sur Bitcoin grâce au Nakamoto Institute. Et merci d'avoir créé le podcast Noded qui a grandement influencé ma vision philosophique de Bitcoin.
— Merci à Saifedean Ammous pour ses convictions, ses tweets sauvages et pour avoir écrit L'Étalon Bitcoin
— Merci à Francis Pouliot de partager son enthousiasme et d'avoir découvert les mentions de la timechain.
— Merci à Andreas M. Antonopoulos pour tout le contenu éducatif qu'il a créé année après année.
— Merci à Peter McCormack pour ses tweets honnêtes et le podcast What Bitcoin Did, qui continue encore à donner de bonnes perspectives des nombreux secteurs de l'écosystème.
— Merci à Jannik, Brandon, Matt, Camilo, Daniel, Michael, et Raphael d'avoir donné votre retour sur les ébauches de

certaines leçons. Un merci tout particulier à Jannik qui a relu de multiples ébauches à de nombreuses reprises.
— Merci à Dhruv Bansal et Matt Odell d'avoir pris le temps de discuter de certaines de ces idées avec moi.
— Merci à Guy Swann d'avoir enregistré une version audio de 21lessons.com.
— Merci au Frère Hass pour son soutien moral et ses conseils et pour avoir pris le temps d'écrire l'avant-propos de ce livre.
— Merci à ma femme de m'avoir enduré, moi et ma nature obsessionnelle.
— Merci à ma famille de me supporter à la fois pendant les bons et les mauvais moments.
— Enfin, mais non des moindres, merci à tous les maximalistes Bitcoin, à tous les minimalistes des shitcoins, les porte-paroles, les bots et les shitposters qui vivent dans ce jardin magnifique qu'est Bitcoin Twitter.

Enfin, merci à vous d'avoir lu ceci. J'espère que ça vous a plu autant que j'ai aimé l'écrire.

Table des figures

À propos de la bibliographie

Aujourd'hui, beaucoup de livres ont été publiés sur Bitcoin. Pourtant, la plupart des conversations – et donc la plupart des contenus dignes d'intérêt – se passent en ligne.

La bibliographie qui va suivre établit indifféremment une liste de livres, d'articles et de contenus en ligne. Si le contenu possède une URL associée, l'URL était accessible en Octobre 2019, puisque j'ai pu m'y rendre. Si l'une ou l'autre de ces URL venait à mener à une impasse, j'en suis désolé. Merci de me le faire savoir [12] afin que je puisse la mettre à jour.

P.S. : Bitcoin et IPFS règlent ça.

12. `https://dergigi.com/contact`

Bibliographie

[1] Saifedean Ammous. *The Bitcoin Standard : The Decentralized Alternative to Central Banking*. Wiley, 2017.

[2] Saifedean Ammous. Presentation on the bitcoin standard. `https://www.bayernlb.de/internet/media/de/ir/downloads_1/bayernlb_research/sonderpublikationen_1/bitcoin_munich_may_28.pdf`, May 2018.

[3] Anonymous 4chan Poster, Robin Houston, Jay Pantone, and Vince Vatter. A lower bound on the length of the shortest superpattern. October 2018.

[4] Andreas M Antonopoulos. *Mastering Bitcoin : Programming the Open Blockchain*. " O'Reilly Media, Inc.", 2014.

[5] Julian Assange. Cypherpunks : Freedom and the future of the internet - introduction : A call to cryptographic arms. `https://cryptome.org/2012/12/assange-crypto-arms.htm`, December 2012.

[6] United Nations General Assembly. The universal declaration of human rights, December 1948.

[7] Beautyon. Why america can't regulate bitcoin. `https://hackernoon.com/why-america-cant-regulate-bitcoin-8c77cee8d794`, March 2018.

[8] Beautyon. Bitcoin is. and that is enough. `https://hackernoon.com/`

bitcoin-is-and-that-is-enough-e3116870eed1, October 2019.

[9] Georg T Becker, Francesco Regazzoni, Christof Paar, and Wayne P Burleson. Stealthy dopant-level hardware trojans. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 197–214. Springer, 2013.

[10] Marty Bent. Tales from the crypt – a podcast about bitcoin. https://tftc.io/tales-from-the-crypt/, 2017.

[11] Jeff Bezos. To our shareholders. http://media.corporate-ir.net/media_files/irol/97/97664/reports/Shareholderletter97.pdf, 1997.

[12] Bitcoin Wiki contributors. Block hashing algorithm — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Block_hashing_algorithm&oldid=66452, 2019.

[13] Bitcoin Wiki contributors. Controlled supply — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Controlled_supply&oldid=66483, 2019.

[14] Bitcoin Wiki contributors. Genesis block — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Segregated_Witness&oldid=66902, 2019.

[15] Bitcoin Wiki contributors. Pay to script hash — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Pay_to_script_hash&oldid=64705, 2019.

[16] Bitcoin Wiki contributors. Segregated witness — Bitcoin Wiki. https://en.bitcoin.it/w/index.php?title=Segregated_Witness&oldid=66902, 2019.

[17] Godfrey Bloom. Why the whole banking system is a scam. https://youtu.be/hYzX3YZoMrs, May 2013.

[18] Giannina Braschi. *Empire of Dreams*. AmazonCrossing, 2011.

[19] Nic Carter. Bitcoin's existential crisis / what is it like to be a bitcoin? https://medium.com/s/story/what-is-it-like-to-be-a-bitcoin-56109f3e6753, November 2018.

[20] Guix Contributors. Guix — bootstrapping. https://guix.gnu.org/manual/en/html_node/Bootstrapping.html, 2019.

[21] Daniel C Dennett and Douglas R Hofstadter. *The mind's I : fantasies and reflections on self and soul*. Harvester Press, 1981.

[22] Jeff Desjardins. The rising speed of technological adoption. https://www.visualcapitalist.com/rising-speed-technological-adoption/, February 2017.

[23] Peter Diamandis. *Abundance : the future is better than you think*. Free Press, New York, 2012.

[24] Dunny. I've learned more about finance, economics, technology, cryptography, human psychology, politics, game theory, legislation, and myself in the last three months of crypto than the last three and a half years of college. https://twitter.com/BitcoinDunny/status/935330541263519745, November 2017.

[25] epii. New bitcoin logo. https://bitcointalk.org/index.php?topic=4994.msg140770#msg140770, May 2011.

[26] Electronic Frontier Foundation. The crypto wars :governments working to undermine encryption. https://www.eff.org/files/2014/01/03/cryptowarsonepagers-1_cac.pdf, 2018.

[27] Susannah Fox and Lee Rainie. How the internet has woven itself into american life. https://pewrsr.ch/32M7Qmg, February 2014.

[28] William Gibson. The science in science fiction. https://www.npr.org/2018/10/22/1067220/the-science-in-science-fiction, October 2018.

[29] Gigi. Bitcoin's energy consumption – a shift in perspective. https://dergigi.com/2018/06/10/bitcoin-s-energy-consumption/, June 2018.

[30] Gigi. The magic dust of cryptography – how digital information is changing our societybitcoin's gravity. https://dergigi.com/2018/08/17/the-magic-dust-of-cryptography/, Aug 2018.

[31] Gregory Maxwell. Taproot : Privacy preserving switchable scripting. https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-January/015614.html, 2018.

[32] Hasu. Unpacking bitcoin's social contract. https://uncommoncore.co/unpacking-bitcoins-social-contract, December 2018.

[33] Friedrich August Hayek. *1980s Unemployment and the Unions : Essays on the Impotent Price Structure of Britain and Monopoly in the Labour Market.* Institute of Economic Affairs, 1984.

[34] Friedrich August Hayek. *The Collected Works of F.A. Hayek, Volume 6, Good Money, Part II*. Routledge, 1999.

[35] Henry Hazlitt. *Economics in One Lesson*. Ludwig von Mises Institute, https://mises.org/library/economics-one-lesson, 1946.

[36] Dan Held. Bitcoin's distribution was fair. https://blog.picks.co/bitcoins-distribution-was-fair-e2ef7bbbc892, 2018.

[37] Eric Hughes. A cypherpunk's manifesto. https://www.activism.net/cypherpunk/manifesto.html, March 1993.

[38] Guido Jörg Hülsmann. *Ethics of Money Production*. Ludwig von Mises Institute, https://mises.org/library/ethics-money-production, 2008.

[39] Robert Kiyosaki. Why the rich are getting richer. https://youtu.be/abMQhaMdQu0, July 2016.

[40] Kaspersky Lab. From festive fun to password panic : Managing money online this christmas. https://www.kaspersky.com/blog/money-report-2018/, 2018.

[41] Jameson Lopp. No one has found the bottom of the bitcoin rabbit hole. https://twitter.com/lopp/status/1061415918616698881, November 2018.

[42] Margo Rapport. History shows price of an ounce of gold equals price of a decent men's suit, says sionna investment managers. https://www.businesswire.com/news/home/20110819005774/en/History-Shows-Price-Ounce-Gold-Equals-Price, 2011.

[43] Trace Mayer. The 7 network effects of bitcoin. https://www.thrivenotes.com/the-7-network-effects-of-bitcoin/, January 2016.

[44] Ralph C. Merkle. Daos, democracy and governance. https://alcor.org/cryonics/Cryonics2016-4.pdf#page=28, July-August 2016.

[45] Fiat Minimalist. Isn't it ironic that bitcoin has taught me more about money than all these years i've spent working for financial institutions ? https://twitter.com/fiatminimalist/status/1072880815661436928, December 2018.

[46] The Austrian Mint. Gold : The extraordinary metal. https://www.muenzeoesterreich.at/eng/discover/for-investors/gold-the-extraordinary-metal, November 2017.

[47] British Museum. The origins of coinage. https://www.britishmuseum.org/explore/themes/money/the_origins_of_coinage.aspx, 2007.

[48] Satoshi Nakamoto. Bitcoin : A peer-to-peer electronic cash system. October 2008.

[49] Satoshi Nakamoto. Re : Bitcoin p2p e-cash paper. https://www.metzdowd.com/pipermail/cryptography/2008-November/014832.html, November 2008.

[50] Satoshi Nakamoto. Bitcoin open source implementation of p2p currency. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9562, February 2009.

[51] Satoshi Nakamoto. Bitcoin open source implementation of p2p currency. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source, February 2009.

[52] Satoshi Nakamoto. Re : Bitcoin open source implementation of p2p currency. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source, February 2009.

[53] Satoshi Nakamoto. Re : Questions about bitcoin. https://bitcointalk.org/index.php?topic=13.msg46#msg46, December 2009.

[54] Satoshi Nakamoto. Dealing with sha-256 collisions. https://bitcointalk.org/index.php?topic=191.msg1585#msg1585, June 2010.

[55] Satoshi Nakamoto. Re : 0.3 almost ready. https://bitcointalk.org/index.php?topic=199.msg1670#msg1670, June 2010.

[56] Satoshi Nakamoto. Re : Transactions and scripts : Dup hash160 ... equalverify checksig. https://bitcointalk.org/index.php?topic=195.msg1611#msg1611, June 2010.

[57] Ron Paul. *End the Fed*. Grand Central Publishing, http://endthefed.org/books/, 2009.

[58] Jordan Pearson. Inside the world of the bitcoin carnivores : Why a small community of bitcoin users is eating meat exclusively. https://motherboard.vice.com/en_us/article/ne74nw/inside-the-world-of-the-bitcoin-carnivores, September 2017.

[59] Pieter Wuille. Schnorr signatures for secp256k1. https://github.com/sipa/bips/blob/bip-schnorr/bip-schnorr.mediawiki, 2019.

[60] Plato. *Plato in Twelve Volumes, Vol. 3. (Euthydemus section 304a/304b).* Harvard University Press, http://www.perseus.tufts.edu/hopper/text?doc=Perseus%3Atext%3A1999.01.0178%3Atext%3DEuthyd.%3Asection%3D304a, 2017.

[61] Federal Reserve. Money stock measures – discontinuance of m3. https://www.federalreserve.gov/Releases/h6/discm3.htm, 2005.

[62] Perry J. Roets. Bernard w. dempsey, s.j. *Review of Social Economy*, 49(4) :546–558, 1991.

[63] Carl Sagan. *Cosmos.* Random House, 1980.

[64] Bruce Schneier. *Applied Cryptography : Protocols, Algorithms and Source Code in C.* John Wiley and Sons, 2017.

[65] Bruce Schneier. Schneier on security. https://www.schneier.com, 2019.

[66] Edward Snowden. Edward snowden : Nsa whistleblower answers reader questions. https://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower, June 2013.

[67] Jimmy Song. Why bitcoin is different. https://medium.com/@jimmysong/why-bitcoin-is-different-e17b813fd947, April 2018.

[68] U.S. Geological Survey. National minerals information center – mineral commodity summaries. https://www.usgs.gov/centers/nmic/mineral-commodity-summaries, 2019.

[69] Nick Szabo. Shelling out : The origins of money. https://nakamotoinstitute.org/shelling-out/, 2002.

[70] K. Thompson. Reflections on trusting trust. In *ACM Turing award lectures*, page 1983, 2007.

[71] Tom Elvis Jedusor. Mimblewimble origin. https://github.com/mimblewimble/docs/wiki/MimbleWimble-Origin, 2016.

[72] Grisha Trubetskoy. Blockchain proof-of-work is a decentralized clock. https://grisha.org/blog/2018/01/23/explaining-proof-of-work/, 2018.

[73] Peter Van Valkenburgh. Coin center's peter van valkenburg on preserving the freedom to innovate with public blockchains. http://bit.ly/valkenburgh, November 2018.

[74] Ludwig von Mises. *Human Action*. Ludwig von Mises Institute, https://mises.org/library/human-action-0/html/p/607, 1949.

[75] Wikipedia contributors. 2013–present economic crisis in venezuela — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=2013%E2%80%93present_economic_crisis_in_Venezuela&oldid=918242758, 2019.

[76] Wikipedia contributors. Austrian school — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/

index.php?title=Austrian_School&oldid=920008469, 2019.

[77] Wikipedia contributors. Bimetallism — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Bimetallism&oldid=920537299, 2019.

[78] Wikipedia contributors. Crypto wars — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Crypto_Wars&oldid=916147143, 2019.

[79] Wikipedia contributors. Discrete logarithm — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Discrete_logarithm&oldid=909625575, 2019.

[80] Wikipedia contributors. Dual ec drbg — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Dual_EC_DRBG&oldid=918490393, 2019.

[81] Wikipedia contributors. Dyson sphere — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Dyson_sphere&oldid=916621053, 2019.

[82] Wikipedia contributors. Elliptic-curve cryptography — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Elliptic-curve_cryptography&oldid=916608234#Backdoors, 2019.

[83] Wikipedia contributors. Hyperinflation — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/

index.php?title=Hyperinflation&oldid=919343724, 2019.

[84] Wikipedia contributors. Illegal number — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Illegal_number&oldid=918772989, 2019.

[85] Wikipedia contributors. Illegal prime — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Illegal_prime&oldid=913087454, 2019.

[86] Wikipedia contributors. Keynesian economics — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Keynesian_economics&oldid=919881690, 2019.

[87] Wikipedia contributors. Landauer's principle — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Landauer%27s_principle&oldid=907333330, 2019.

[88] Wikipedia contributors. Last glacial maximum — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Last_Glacial_Maximum&oldid=919510280, 2019.

[89] Wikipedia contributors. Lindy effect — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Lindy_effect&oldid=921214819, 2019.

[90] Wikipedia contributors. List of currencies — Wikipedia, the free encyclopedia. https://en.wikipedia.

org/w/index.php?title=List_of_currencies&oldid=897955050, 2019.

[91] Wikipedia contributors. List of historical currencies — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=List_of_historical_currencies&oldid=919919705, 2019.

[92] Wikipedia contributors. Methods of coin debasement — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Methods_of_coin_debasement&oldid=917940627, 2019.

[93] Wikipedia contributors. Money multiplier — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Money_multiplier&oldid=918027413, 2019.

[94] Wikipedia contributors. Money supply — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Money_supply&oldid=921152289, 2019.

[95] Wikipedia contributors. P versus np problem — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=P_versus_NP_problem&oldid=919882161, 2019.

[96] Wikipedia contributors. Paradox of value — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Paradox_of_value&oldid=906068208, 2019.

[97] Wikipedia contributors. Sha-2 — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=SHA-2&oldid=917408454, 2019.

[98] Wikipedia contributors. Ship of theseus — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Ship_of_Theseus&oldid=923020256, 2019.

[99] Wikipedia contributors. Silver certificate (united states) — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Silver_certificate_(United_States)&oldid=917688197, 2019.

[100] Wikipedia contributors. Subjective theory of value — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Subjective_theory_of_value&oldid=893004286, 2019.

[101] Wikipedia contributors. Thaler — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Thaler&oldid=914457345, 2019.

[102] Wikipedia contributors. Theory of value (economics) — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Theory_of_value_(economics)&oldid=919603374, 2019.

[103] Wilma Woo. 'unfairly cheap' lightning network mainnet hits 40 nodes, 60 channels. https://bitcoinist.com/bitcoin-lightning-network-mainnet-nodes/, January 2018.