Le Petit Livre Du Bitcoin

Pourquoi Bitcoin Compte pour Votre Liberté, vos Finances et votre Avenir

Timi Ajiboye
LuisBuenaventura
Alex Gladstein
Lily Liu
Alexander Lloyd
Alejandro Machado
Jimmy Song
Alena Varnova

Publié par 21 Million Books
Redwood , Californie

Clause de non-responsabilité : l'éditeur et l'auteur ont fait de leur mieux en élaborant ce livre. Cependant; ils n'ont fait aucune déclaration ou garantie quant à l'exactitude ou l'exhaustivité de son contenu, déclinent expressément toute garantie implicite de qualité marchande ou d'adéquation à une fin particulière. Les conseils et stratégies contenus dans le présent document peuvent ne pas convenir à votre situation; consultez un professionnel si nécessaire. Ni l'éditeur ni l'auteur ne sont responsables de toute perte de profit ou tout autre dommage.

Conception et illustration du livre : Luis Buenaventura.
Illustration du "Blocus Vénézuelien" : Timi Ajiboye.

Première Édition (Ed. 01-201909191306)

ISBN 978-1-64199-050-9

Sommaire

Avant-propos ……..……9

Qu'est ce qui cloche avec la monnaie aujourd'hui? ……15

Bitcoin c'est quoi ? ……...27

Prix et volatilité du bitcoin ……..41

Pourquoi Bitcoin compte pour les droits humains ……...49

Un récit de deux futurs……..63

Le début de la souveraineté individuelle ……69

Questions et Réponses sur Bitcoin……...75

Qui est Satoshi Nakamoto? ……...75
Qui contrôle Bitcoin? ……...75
Bitcoin n'est-il pas trop volatil? ……...76
Qu'est-ce qui soutient la valeur actuelle du bitcoin? ……...77
Comment faire confiance au bitcoin? ……....77
Quelle est la fiabilité du Bitcoin? ……....78
Pourquoi plusieurs plateformes d'échange ont été piratées? ……...78
Bitcoin est-il utilisé par les criminels pour le blanchiment d'argent?……79
Bitcoin est-il une pyramide de Ponzi? ……...80
Bitcoin est-il une bulle? ……....80
Qu'est-ce que Tether et comment affecte-t-il bitcoin ? ……...81
Les gouvernements peuvent-ils interdire ou désactiver le bitcoin ? ……....81
Bitcoin est-il légal?……....82
Le minage est-il un gaspillage d'énergie nocif pour l'environnement?.....84
Et si quelqu'un avec un supercalculateur ou un ordinateur quantique piratait le réseau Bitcoin?……..86
Comment Bitcoin reste-t-il décentralisé? ……...……...87
Bitcoin protège-t-il la vie privée ? ……...88
Comment Bitcoin peut-il répondre aux besoins de 7 milliards de personnes? ……...89

Bitcoin favorise-t-il une extrême inégalité de richesse? ……90
S'il n'y aura que 21 millions de bitcoins, comment seront-ils utilisés à l'échelle mondiale?……...91
Comment puis-je me permettre d'acheter un bitcoin avec un prix si élevé?……...91
Comment acquérir des bitcoins?……....92
Comment utiliser un portefeuille Bitcoin? ……93

Ressources supplémentaires……..95
Glossaire……...99
Remerciements ……....102

Avant-propos

Nous sommes des activistes, des enseignants, des entrepreneurs, des cadres, des investisseurs et des chercheurs. Nous sommes d'Afrique, d'Asie, d'Europe, d'Amérique du Nord et du Sud. Nous sommes différents à bien des égards mais nous sommes tous fascinés par Bitcoin et l'impact que nous pensons qu'il va avoir sur notre monde et dans nos vies.

En mars 2019, Jimmy avait discuté avec certains d'entre nous sur l'idée de faire un *"book sprint"*, où nous nous réunirions dans un endroit isolé pendant quelques jours pour écrire un livre sur Bitcoin et son importance pour la société. Deux mois plus tard, lors du forum sur la liberté d'Oslo, nous nous sommes réunis sur un toit en Norvège, entourés d'activistes de droits humains et de journalistes venus de tous les continents. La conversation avait inévitablement tourné autour du Bitcoin et de sa possibilité de changer le monde. Alex a encouragé le groupe à écrire un livre qui explique pourquoi Bitcoin compte sans avoir à utiliser le jargon technique qui est si courant dans ces genres de livres. Nous voulions aider les personnes curieuses à comprendre l'impact humain de l'une des innovations les plus profondes de notre temps. Quelques mois plus tard, nous nous sommes rencontrés, à huit, dans une maison en Californie pour faire de cette idée une réalité.

Ce que vous tenez maintenant dans les mains est le résultat de cet effort de quatre jours. Ce livre va vous aider à comprendre pourquoi il y a des problèmes avec le système monétaire actuel, pourquoi Bitcoin a été inventé pour apporter une alternative, comment il va changer la politique et la société et ce que cela signifie pour l'avenir.

Nous espérons sincèrement qu'en lisant ce livre, vous deviendrez impressionné par Bitcoin autant que nous le sommes.

Le 08 Août 2019
Redwood, Californie.

A propos des Auteurs

Timi Ajiboye est à la fois développeur et entrepreneur basé à Lagos, au Nigeria. Il a cofondé et dirige actuellement BuyCoins (buycoins.africa), une plateforme d'échange qui permet aux africains d'acheter et vendre du bitcoin facilement avec leurs monnaies locales. Twitter: @timigod

Luis Buenaventura est cofondateur de BloomX (bloom. solutions), une jeune entreprise aux philippines qui rend l'échange des cryptomonnaies sécurisé pour les pays émergents. Conférencier et auteur prolifique, il a également créé Cryptopop.net, une initiative artistique qui vise à rendre les cryptomonnaies plus accessibles au grand public. Twitter: @helloluis

Alex Gladstein est CSO (Chief Strategy Officer) chez Human Rights Foundation (hrf.org), une organisation à but non lucratif qui promeut les libertés civiques et défie l'autoritarisme dans le monde. Il est également conférencier sur Bitcoin et la gouvernance pour Singularity University. Il a écrit sur le point commun entre la technologie et la liberté dans des magasines tels que TIME, CNN, et Bitcoin Magazine. Twitter: @gladstein

Lily Liu est à la fois investisseur et entrepreneur. Plus récemment, elle a cofondé et était chargée des Finances chez Earn.com, une plateforme qui permet à n'importe qui de gagner des bitcoins pendant son temps libre, qui a été vendu à Coinbase en 2018. Avant cela, elle a construit un hôpital en Chine et a travaillé chez KKR et McKinsey. Elle a fait ses études à Stanford et Harvard. Twitter: @calilyliu

Alexander Lloyd a investi dans les startups depuis 1998. En 2008, il a fondé Accelerator Ventures. Son premier emploi était dans la négociation des devises chez Goldman Sachs. En 2016, il a rejoint le conseil d'administration de Human Rights Foundation, où il travaille sur la Corée du nord. Twitter: @alex01

Alejandro Machado est le fondateur d' Open Money Initiative (openmoneyinitiative.org), un organisme sans but lucratif qui étudie l'effondrement des systèmes monétaires et la manière dont les gens utilisent l'argent. Il travaille sur l'amélioration de l'accès à la monnaie numérique pour les Vénézuéliens. Twitter: @alegw

Jimmy Song est développeur Bitcoin, éducateur et entrepreneur. Il est l' auteur du livre Programming Bitcoin (programming-bitcoin.com), publié par O'Reilly. Il travaille sur l'apport d'une monnaie saine (sound money) au monde. La couleur de son chapeau de cowboy indique s'il est de bonne ou de mauvaise humeur. Sa clé PGP est C1D7 97BE 7D10 5291 228C D70C FAA6 17E3 2679 E455. Twitter: @jimmysong

Alena Vranova a développé des entreprises à succès dans le secteur des services financiers depuis 2003. Au cours de ces 7 dernières années, elle a aidé les particuliers et les petites entreprises à protéger leurs bitcoins avec des produits et services non-custodial. En 2013, elle a créé Trezor, le premier portefeuille matériel bitcoin (hardware wallet). Alena est actuellement responsable de la stratégie chez Casa (keys.casa), qui vise à rendre la sécurisation des bitcoins et la souveraineté financière accessible à tous. Twitter: @AlenaSatoshi

Les auteurs au troisième jour du “book sprint”.

CHAPITRE 1

Qu'est ce qui Cloche avec la Monnaie Aujourd'hui?

Nous sommes en 1981

A Manille, quelques mois seulement après la levée officielle de la loi martiale pour la première fois en dix ans, un jeune couple philippin accueille Luis, son premier enfant. Le dictateur Ferdinand Marcos restera au pouvoir encore quelques années. Mais pour l'instant, les parents de Luis ne se soucient que du bien-être de leur jeune famille. Ils ont un petit compte épargne; pour une première fois, ils ont commencé à mettre l'argent de côté, se préparant pour les années à venir qui promettent d'être turbulentes. Le taux de change est de sept pesos philippins pour un dollar américain.

Nous sommes en 1993

A Lagos, le général nigérian Sani Abacha prend le pouvoir et fixe un dollar américain à 22 naira nigérians. C'est une mesure agressive pour tenter de stabiliser l'économie. Pour lui, il faut à tout prix empêcher le naira de continuer de perdre sa valeur. Le taux de change fixe engendre une économie souterraine dynamique où le naira se négocie à une valeur beaucoup plus faible. À la mort d'Abacha en 1998, le dollar change de mains sur le marché noir pour pas moins de 88 nairas, quatre fois le taux officiel du gouvernement. Des millions de personnes souffrent car elles ne peuvent plus faire face à la hausse des prix des denrées alimentaires avec les salaires statiques du gouvernement.

Nous sommes en 2018.

Partout le long de la frontière poreuse du Venezuela, les citoyens fuient l'hyperinflation record du pays (+ 400 000%) en traversant la Colombie et le Brésil voisins. Plus de 3 millions de personnes ont déjà fui la famine dévastatrice et la crise sociale qui rongent le pays

Lorena, une boulangère de 48 ans, prend la dure décision de partir en Colombie. À la frontière, les gardes fouillent ses affaires, à la recherche d'objets de valeur à confisquer. Ils ne trouvent rien. Ils ne savent pas que quelques heures avant, Lorena a passé des heures à enrouler soigneusement des billets de dollars américains autour de ses pinces à cheveux pour les cacher dans ses tresses. Elle s'avance, la tête haute, vers un nouveau pays.

À Manille, les parents de Luis voient leur chance tourner au pire. Le taux de change est maintenant de 50 pesos philippins pour un dollar américain, et leur épargne économisée au fil des années a perdu plus de 80 % de sa valeur. Leur retraite étant imminente, ils n'ont d'autre choix que de continuer à travailler afin de continuer de mettre l'argent de côté pour assurer leur avenir impitoyable et incertain.

A Lagos, le naira est dans une brève période de relative stabilité après avoir perdu 50% de sa valeur face au dollar en quelques années. Les prix des produits locaux sont une fois de plus montés en flèche. Personne, y compris les officiels eux-mêmes, ne croit que le gouvernement peut arriver à prévenir une autre crise économique.

Nous sommes en 2019

À Shanghai, une jeune professionnelle nommée Annie envoie des messages à l'un de ses amis sur WeChat, un réseau social utilisé au quotidien par plus d'un milliard de Chinois. Son ami mentionne qu'il est en difficulté pour avoir fumé de la marijuana. En pleine conversation en ligne, ce dernier arrête brusquement de répondre.

Le lendemain, deux policiers en civil rendent visite à Annie à son bureau et lui demandent de les suivre. Ses collègues la voient partir et disparaître pendant quelques semaines. Quand elle revient enfin en ligne, elle constate avoir perdu certaines de ses fonctionnalités de paiement sur WeChat. Annie ne peut plus acheter un billet d'avion ou de train. Sa cote de crédit s'effondre. Sa vie est ruinée par une simple série de messages textes.

À Oakland, Alex va dans une animalerie à la recherche de nourriture pour chiens. Il trouve ce qu'il cherche, ainsi qu' un nouveau produit intéressant, qui promet de mieux sentir l'haleine de son chien. Il glisse sa carte visa pour payer la bouffe et rentre. Quelques minutes plus tard, il consulte twitter et soudain, une publicité des friandises pour chiens, exactement les mêmes qu'il vient d'acheter, apparaît sur son écran. Il découvre que Chase partage des informations sur ses paiements quotidiens avec des sociétés tierces.

Alex se rend compte, avec un sentiment inquiétant, que les détails de sa vie personnelle sont remis aux annonceurs. Même aux États-Unis, la confidentialité financière est en voie de disparition.

Des récits sur la façon dont la monnaie est tombée en panne

Les parents de Luis et des millions d'autres membres de la classe moyenne aux philippine et au Nigéria ont vu leurs économies s'évaporer au ralenti sur une seule génération. Lorena avait juste besoin d'un moyen de déplacer ses maigres économies (sans se les faire confisquer) vers un nouveau foyer en Colombie, elle a alors fait preuve de créativité grâce à à sa coiffure. Annie est maintenant dans une *prison financière* en Chine parce que l'un de ses amis a fumé un pétard. Les achats d'Alex sont tracés et revendus à plusieurs entreprises à chaque utilisation de sa carte de crédit.

Ces cas ne sont pas isolés

Depuis les années 2000, presque toutes les monnaies ont perdu une valeur significative par rapport au dollar américain. Beaucoup, comme le Rand Sud-Africain, le pesos Argentin, et la lire turque ont perdu près de 50%.

Une malheureuse poignée comme la hryvnia ukrainienne et le pesos dominicain ont perdu jusqu'à 70%. Même le dollar américain et l'euro ont vu leur pouvoir d'achat chuter de 33% au cours de cette période.

Dans le monde entier, 250 millions de migrants et réfugiés luttent pour envoyer l'argent chez eux ou l'emporter avec eux au-delà des frontières. Environ deux milliards de personnes n'ont pas accès à un compte bancaire ou une identification officielle de l'État nécessaire pour en obtenir un. Dans un monde de plus en plus globalisé, l'argent est obstinément resté coincé au niveau local.

Pendant ce temps, dans les mégalopoles comme Shanghai et San Francisco, le sentiment déconcertant d'être surveillé est palpable. D'une part, Big brother nous observe et de l'autre, le capitalisme de surveillance trace chaque achat et vend les données à des dizaines d'entreprises sans la moindre permission du client. La vie privée est devenue un luxe, un luxe dont le prix augmente chaque jour qui passe.

C'est quoi la monnaie ?

À la base, la monnaie est un compromis social.

La monnaie oblige les gens à croire que les billets dans leur portefeuille, les chiffres dans leur compte bancaire et les soldes sur leurs cartes cadeaux peuvent être échangés à l'avenir pour les choses dont ils ont besoin. Le vendeur a besoin de concevoir que l'argent de l'acheteur est précieux.

Au cours de l'histoire, les sociétés ont expérimenté diverses façons de mener ce compromis, en utilisant tout: depuis les coquillages, du sel et de l'or jusqu'aux systèmes bancaires centraux complexes utilisés aujourd'hui. Certaines formes de monnaies sont plus saines que d'autres, ce qui signifie qu'elles conservent mieux leur valeur dans le temps.

Instinctivement, tout le monde sait que l'argent compte et qu'il vaut mieux avoir l'argent le plus sain possible.

Vu que la plupart des personnes échangent leur travail contre de l'argent, celui-ci représente leur temps brûlé et leurs efforts. La monnaie est le moyen par lequel le travail est converti en biens et services dans le présent comme le futur. Dans cette optique, l'accès à une monnaie saine est l'une des formes les plus durables de conserver un pouvoir personnel.

Aussi, l'argent compte énormément pour le gouvernement. Alors que les économies d'aujourd'hui sont organisées par les états-nations, les gouvernements ont le pouvoir de contrôler l'argent. Cependant, ce contrôle suscite toujours la tentation d'abuser. Les fonctionnaires manipulent souvent ce pouvoir en fonction de leurs intérêts. Seuls les gouvernements le plus démocratiques, qui protègent les droits individuels, la séparation des pouvoirs et la primauté du droit, peuvent efficacement se prémunir des abus monétaires tels que l'inflation galopante, les saisies arbitraires et la corruption.

Comment fonctionne la Monnaie Moderne?

Toutes les monnaies nationales en circulation aujourd'hui sont appelées monnaies *fiduciaires*, ce qui signifie (en latin) "par décret". La valeur de ces monnaies est fixée par les décret des États-nations qui les émettent et les acceptent. Etant donné que les gouvernements peuvent créer une grande quantité de monnaie fiduciaire à faible coût, ils sont capables d'en imprimer à l'infini chaque fois qu'ils le souhaitent.

Alan Greenspan, ancien président de la Réserve Fédérale américaine, a déclaré que les États-Unis peuvent « rembourser toutes les dettes qu'ils ont parce qu' ils peuvent toujours imprimer de l'argent pour la faire». Cette pratique peut causer des problèmes, même dans les économies les plus stables du monde. La plus ancienne monnaie nationale est la livre sterling du Royaume-Uni, qui a perdu 99.5 % de sa valeur au cours des 300 dernières années. Le dollar américain a perdu 90% de son pouvoir d'achat au cours du dernier siècle. Un steak qui coûtait 0,36$ en 1925 était 3$ en 1990 et coûte 12$ aujourd'hui. Pourtant le livre et le dollar sont quelques-unes des monnaies fiduciaires les plus stables à avoir jamais existé. La monnaie fiduciaire a une durée moyenne de vie de seulement 27 ans.

L'objectif des banques centrales modernes est de maintenir une inflation faible et stable. Cette politique a rencontré un succès qui varie selon les pays. La plupart des monnaies souffrent d'une inflation élevée sur le long terme, ce qui peut être dévastateur pour l'épargne. Ceci est particulièrement vrai pour ceux qui n'ont pas les moyens d'acquérir des actifs solides : l'immobilier ou les actions de premier ordre, dont la valeur augmente avec l'inflation. L'inflation élevée peut rendre difficile pour tous, sauf les riches, d'épargner pour l'avenir.

La valeur des économies des milliards de personnes qui vivent sous des régimes autoritaires diminue en raison des décisions des fonctionnaires gouvernementaux non élus. Seules les élites sont généralement en mesure d'accéder au dollar, à l'or ou à l'immobilier pour préserver la valeur. Pendant ce temps, les citoyens des démocraties en bonne santé bénéficient d'une certaine protection importante. Ils ont un accès facile aux monnaies relativement stables comme le dollar et l'euro. Leurs économies ont tendance à bien performer. Ils ont plus de chances d'avoir un emploi qui paie bien et un accès à des produits d'investissement qui peuvent compenser ou dépasser l'inflation.

Le fait pour l'élite de bénéficier de manière disproportionnée de l'argent nouvellement imprimé est si répandu qu'il y a un terme pour le désigner: l'*effet cantillon*. Il doit son nom à Richard Cantillon, un économiste du 18ème siècle qui l'a remarqué alors qu'il travaillait comme banquier au Royaume-Uni. Une inflation à grande échelle peut être un moyen injuste de distribuer les richesses car elle profite inévitablement aux plus nantis au détriment de ceux qui ne le sont pas. Bien que ses effets ne soient pas forcément évidents pour la classe moyenne aux États-Unis ou au Royaume-Uni, ils sont douloureusement ressentis par des milliards de citoyens dans des pays aux économies instables.

Les systèmes monétaires basés sur la monnaie fiduciaire ont également facilité les guerres prolongées de l'ère moderne. Les gouvernements ont la possibilité d'imprimer beaucoup d'argent pour faire la guerre et faire payer la facture aux futures générations par l'inflation.

Cela signifie des guerres plus longues et plus coûteuses. La première guerre mondiale est un exemple tragique, car ses principaux acteurs ont financé ses dernières phases par l'inflation. La Russie et l'Allemagne ont suspendu l'étalon-or alors que leurs monnaies fiduciaires étaient convertibles à une quantité fixe d'or. Ils ont supprimé cette convertibilité pour imprimer, du néant, des grandes quantités de masse monétaire afin de continuer à combattre. Comme résultat, la guerre a duré beaucoup plus longtemps que quiconque ne l'aurait cru possible. Quand l'Allemagne a perdu, la seule façon pour elle de financer les énormes réparations a été d'imprimer encore plus d'argent. En 1923, le deutsche mark (ancienne unité monétaire allemande) s'est déprécié pour atteindre un trillionième de sa valeur d'avant-guerre, préparant le terrain à la Seconde Guerre mondiale.

Des dépenses excessives similaires ont été perceptibles dans un passé récent. Peu importe ce que l'on peut penser de l'engagement militaire américain en Afghanistan et en Irak, son coût s'élève à plus de 5 900 milliards de dollars, ce qui représente plus de 46 000 $ par ménage si l'on avait demandé au contribuable américain de le financer directement.

Un autre problème du système monétaire actuel est qu'il peut être extrêmement difficile de déplacer de l'argent entre différents pays du monde. Les gouvernements de pays tels que la Chine, la Russie, l'Argentine et l'Indonésie ont fortement limité la quantité de monnaie que leurs citoyens sont autorisés à échanger, transférer ou emporter à l'étranger.

Cela se fait principalement en contrôlant la capacité de chaque individu à échanger sa monnaie locale contre des monnaies étrangères comme le dollar américain. Le citoyen chinois moyen, par exemple, n'est autorisé à convertir qu'un maximum de 50 000 $ de son renminbi (monnaie officielle chinoise) chaque année.

Dans d'autres parties du monde, même la capacité d'accéder à son propre argent localement peut être extrêmement limitée. Après la crise financière de 2015, les citoyens grecs n'étaient plus autorisés à retirer plus de 60 euros par jour de leurs propres comptes en banque, ce qui leur a rappelé qu'ils n'avaient aucun contrôle sur leur propre argent.

Même lorsque les gens peuvent envoyer de l'argent à l'étranger, c'est encombrant et coûteux. En 2018, les travailleurs migrants et les réfugiés ont envoyé près de 700 milliards de dollars au-delà des frontières pour soutenir leurs proches. Les taux de change et les frais de transfert ont absorbé 45 milliards de dollars de cet argent, un montant énorme pour ceux qui n'ont pas d'argent à gaspiller.

Un point de défaillance unique pour le monde

Toutes les banques centrales représentent un point de défaillance unique pour leurs économies nationales. La Réserve fédérale américaine agit, en quelque sorte, comme une banque centrale pour toutes les banques du monde. Pour les Américains, cela semble très bien fonctionner. Le dollar est accepté partout. Il est facile pour plusieurs personnes d'ouvrir des comptes bancaires en dollar, d'obtenir des lignes de crédit et de payer des biens et les services. La plupart des Américains ne sont pas impactés de manière notable par l'inflation.

L'économie dynamique des États-Unis contribue à soutenir et alimenter le système économique mondial d'aujourd'hui. Au cœur de celui-ci se trouve *l'étalon dollar (the dollar standard)*, une hégémonie monétaire mondiale qui fut lancée par un événement peu connu dans un hôtel du New Hampshire en 1944, l'*Accord de Bretton Woods*.

Les puissances mondiales ont organisé un rassemblement à Bretton Woods pour établir un ordre monétaire commun alors que la Seconde Guerre mondiale touchait à sa fin. Pendant trois semaines, plus de 700 délégués de 44 pays ont débattu sur la structure du futur système financier. Certains délégués ont suggéré la création d'une nouvelle monnaie de réserve internationale appelée *bancor*. En fin de compte, les délégués ont accepté que leurs devises soient rattachées au dollar américain. Comme résultat, le commerce international est aujourd'hui principalement nourri par le dollar et chaque pays essaie de maintenir une réserve importante dans la monnaie du pays de l'oncle sam.

La place centrale du dollar américain dans le système économique mondial se révèle dans la manière dont l'argent circule entre les pays. Prenez par exemple l'envoi d'argent de la Corée du Sud aux Philippines. Il n'est généralement pas possible pour le won coréen d'être échangé directement en pesos philippins parce que le phillipine n'a pas assez de won Sud Coréen en réserve et vice versa. Au lieu de cela, ils comptent sur une série de transactions avec un élément central: le dollar américain. Premièrement, le won coréen est vendu pour obtenir des dollars à Séoul. Ces dollars sont transférés d'une banque sud-coréenne à une banque philippine via une banque américaine. Enfin, la banque à Manille converti les dollars en pesos philippins. Cela prend au moins quelques jours et encourt des frais de change et de transaction qui peuvent aller de quelques pourcent à un taux en deux chiffres. Le coût moyen mondial de ces types de paiements transfrontaliers est supérieur à 7 %, même pour les petits envois de fonds.

Bien que le monde ait profité à bien des égards de l'hégémonie du dollar, l'étalon dollar, cela a rendu chaque pays qui en dépend, d'une certaine façon, vulnérable à son effondrement. Il en résulte un système où une poignée de faillites bancaires aux États-Unis peut conduire à une catastrophe économique mondiale.

La fin de la confidentialité financière

La numérisation de l'argent au cours des deux dernières décennies a entraîné une disparition constante de la vie privée. Chaque transaction est désormais exploitée soit pour son potentiel commercial ou pour établir un contrôle politique. La monnaie électronique existe depuis longtemps mais ce n'est que récemment que l'analyse du big data s'est révélée être nécessaire à l'établissement d' une surveillance de masse efficace. Ni les achats en ligne ni les achats physiques ne sont sûrs car les gouvernements et les annonceurs piochent dans les profils pour rendre utiles les données personnelles de chaque individu: ses préférences, ses décisions et même ses relations. Ces profils sont comme des empreintes de données propres à chaque individu. Elles deviennent plus raffinées et facilement identifiables à chaque nouvel achat en ligne ou par carte de crédit.

Cela mène droit vers un monde dans lequel une recherche Google pour un produit peut entraîner des publicités Facebook et Instagram sur ce même produit quelques minutes plus tard.

Selon l'endroit où l'on se trouve, les données personnelles peuvent conduire à des répercussions dangereuses. Pendant l'été 2019, des étudiants de Hong Kong se sont regroupés par dizaines de milliers pour protester contre un nouveau projet de loi qui permettrait au gouvernement chinois d'extrader n'importe qui à Beijing sans respecter la procédure prévue par la loi. Ils savaient que s'ils utilisaient leur carte d'étudiant Octopus pour naviguer dans le métro, leurs emplacements seraient dévoilés. Ils ont alors utilisé de l'argent liquide pour acheter des billets à usage unique. C'est une option sûre pour l'instant, mais l'argent papier et l'argent métallique sont sur le point d'être progressivement retirés de la circulation dans la plupart des grandes zones urbaines au cours de la prochaine décennie. À ce moment-là, il n'y aura plus aucun moyen d'utiliser les réseaux de transport public sans révéler sa position aux autorités et aux grandes sociétés. Les données personnelles seront collectées partout.

La réaction du public face à la surveillance des transactions par les entreprises et les gouvernements n'est pas la même. Certains trouvent cela simplement dérangeant tandis que d'autres le considèrent comme une violation majeure de la vie privée, alors que la plupart ne semblent pas s'en soucier. Quoi qu'il en soit, le fait est qu'au-delà du contrôle de la masse monétaire et de l'endroit où l'argent peut être envoyé, les autorités peuvent maintenant apprendre virtuellement tout sur les acheteurs et les vendeurs. Les systèmes de paiement de plus en plus numériques dans le monde pourraient entraîner une extinction de la vie privée.

Y a-t-il une autre voie ?

Quatre phénomènes mondiaux: la dévaluation du patrimoine personnel, la restriction du transfert de valeur, la centralisation de la finance et la disparition de la vie privée représentent des risques importants pour les personnes qui voguent dans le système monétaire du 21ème siècle.

Partout dans le monde, des gens ressentent la pression alors que les états luttent pour maintenir le statu quo.

Et s'il émergeait un nouveau système dans lequel les gouvernements n'auraient plus la capacité de dévaluer arbitrairement la monnaie et les sociétés anonymes ne pourraient pas geler les fonds des utilisateurs ou refuser de traiter les transactions? Et si l'argent devient entièrement numérique, utilisable par n'importe qui où qu'il se trouve sur la terre grâce à un simple accès à Internet, sans avoir besoin de demander l'autorisation de qui que ce soit?

Dans le sillage de la crise financière de 2008, quelqu'un a décidé de construire exactement un tel système, posant les bases de la prochaine grande révolution de la finance.

CHAPITRE 2

Bitcoin c’est quoi ?

Le 15 septembre 2008, la célèbre banque d’investissement Lehman Brothers a déclaré la plus importante faillite de l’histoire des États-Unis. L’effondrement de Lehman Brothers, une banque fondée en 1850, était l’aboutissement d’une frénésie d’emprunts à l’échelle mondiale. La société avait risqué beaucoup plus que sa valorisation totale sur les titres adossés à des prêts hypothécaires, y compris les très risqués *subprimes*. Lorsque les propriétaires ont cessé de faire des paiements hypothécaires, l’entreprise est devenue insolvable sans aucune possibilité de s’en remettre.

Soudainement, la confiance que le reste des banques avaient établi dans Lehman Brothers et entre elles-même a disparu. Dans ce contexte de resserrement du crédit, les entreprises ont eu du mal à obtenir des prêts pour financer leurs activités. Sans fonds pour acheter des stocks, investir dans de nouveaux équipements, ou payer les employés, les entreprises dans de nombreux secteurs ont eu du mal à fonctionner.

Le Trésor américain et la Réserve fédérale ont agi rapidement pour éviter une catastrophe économique. Ils ont prêté de l’argent aux banques afin de maintenir le système financier à flot. En octobre 2008, le Congrès a renfloué plusieurs banques en difficulté grâce à la Loi d’urgence pour la stabilisation économique de 2008 (Emergency Economic Stabilization Act). Le gouvernement a dépensé des centaines de milliards de dollars pour consolider un secteur financier qui était sur le point de s'effondrer.

L'arrivé de Bitcoin

Le 31 octobre 2008, quelques semaines après que le gouvernement américain ait autorisé la création de 700 milliards de dollars pour renflouer les banques, une personne (ou un groupe) inconnue portant le nom de Satoshi Nakamoto a publié un livre blanc technique décrivant un nouveau système de paiement électronique appelé Bitcoin.

Satoshi a présenté le livre blanc à une liste de diffusion sur Internet dans laquelle participaient de chercheurs en cryptographie appelés les cypherpunks, un groupe des activistes dont le but est de militer pour la protection de la vie privée en créant des outils pour contrer la surveillance et l'abus du pouvoir des états.

Le livre blanc avait deux points importants d'intrigue. Tout d'abord, l'auteur a choisi d'utiliser un pseudonyme. L'identité de Satoshi reste un mystère d'intérêt populaire à ce jour. Deuxièmement, le papier présentait quelque chose qui n'avait jamais existé auparavant : une monnaie numérique qui ne repose pas sur une autorité centrale. Peu de gens croyaient une telle innovation possible.

Quelques mois plus tard, Satoshi a lancé le réseau Bitcoin avec un indice sur la raison de ce choix dans un court texte gravé sur la première page du grand livre comptable de Bitcoin : *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*

Cela fait référence à un titre paru en janvier 2009 dans le *Times*, un important journal britannique. Le message de Satoshi au monde était que le système actuel, où les banques étaient sauvées aux dépens du peuple, était brisé. La technologie financière décentralisée qu'est Bitcoin a été construite pour comme alternative à ce système.

Pour comprendre l'innovation scientifique derrière Bitcoin, il est avant tout important de savoir ce qu'est la rareté.

Les deux types de Rareté

Il existe deux types de rareté . La première est d'origine humaine et, en ce sens, artificielle. C'est notamment les objets de collection comme les sacs à main Chanel en édition limitée, les cartes basket de Michael Jordan, les vins rares, ou les œuvres numérotées d'un artiste. Il est important de remarquer que ces objets font souvent l'objet de plusieurs contrefaçons.

La deuxième forme de rareté est naturelle. Cette catégorie comprend le sel (origine du mot salaire), les perles en verre du Ghana, les coquillages de la culture amérindienne, l'argent de Chine et bien sûr de l'or dans le monde entier.

Ce sont des exemples d'objets dont la rareté est *décentralisée*. Ces derniers sont difficiles à contrefaire. Ce n'est pas un hasard si des produits rares et dont la production est décentralisée, comme le sel et l'or, ont été utilisés dans le passé comme monnaies. Tout d'abord, il y a une certaine équité dans l'utilisation d' un produit qu'aucune personne ni aucun groupe ne contrôle. Deuxièmement, ces produits sont beaucoup plus difficiles à contrefaire. Enfin, leur rareté contribue à faciliter les transactions économiques car il n'est pas nécessaire d'en transporter des quantités déraisonnables pour acheter quelque chose.

Ce qui différencie les deux formes de rareté c'est le contrôle. La rareté centralisée est créée par une entreprise ou une personne, que ce soit la Banque populaire de Chine, la Réserve fédérale, un artiste ou une grande multinationale. Cette entité, ou *autorité centrale*, contrôle entièrement la rareté d'une marchandise en la créant, en faisant son émission, en la rachetant et/ou en la confisquant.

Les objets rares décentralisés sont créés par la nature, ce qui signifie qu'il n'y a aucune autorité centrale chargée de leur production. Ici, pas d'artisanat mais plutôt un processus plus semblable à une récolte. Pour extraire un produit naturellement rare comme l'or ou l'huile, un mineur extrait une matière qui existe déjà dans le sol.

Dans le cas de l'or, son accumulation n'a pas historiquement besoin d'autorisation de la part de quelqu'un d'autre que le propriétaire d'un site minier. En d'autres termes, il n'y a pas de centre à partir duquel tout l'or commence sa vie et aucune autorité mondiale n'est habilitée à restreindre son l'exploitation minière ou à accroître son l'offre.

C'est la principale différence entre les produits rares centralisés et décentralisés, en particulier ceux utilisés comme monnaies.

Pourquoi la décentralisation peut être positive pour la monnaie

Comme nous l'avons mentionné plus haut, l'une des caractéristiques inévitables d'une monnaie centralisée est la possibilité pour son créateur de gonfler arbitrairement son offre suite à un simple coup de tête. Bien que cela soit beaucoup plus souvent fait par des régimes autoritaires que par des démocraties, c'est un fait qui se produit dans toutes les sociétés.

Dans le film *Bugsy*, le personnage principal vend des actions papier du casino Pink Flamingo aux investisseurs encore et encore. À chaque personne, il vend 20% du casino pour 10.000 $. Il le fait avec plus d'une douzaine d'investisseurs en leur donnant des fausses informations sur le nombre de parts acquises. Chaque investisseur pense détenir 20% du casino, mais possède en réalité beaucoup moins que ça. Cependant, Bugsy en bénéficie puisqu'il obtient beaucoup plus d'argent.

Chaque produit centralisé fait face au même problème d'incitation. L'autorité centrale peut créer plus de produits, diluant la valeur détenue par le reste de propriétaires. Les banques centrales qui impriment plus d'argent le font habituellement avec des objectifs positifs comme la construction d'infrastructures, le soutien des programmes d'aide sociale ou la stabilisation d'une crise économique. Cependant, rappelez-vous de l'effet Cantillon du chapitre 1 : une utilisation, même raisonnable, de ce pouvoir peut entraîner des avantages pour les riches et puissants aux détriment des pauvres et impuissants. Le pouvoir d'imprimer de l'argent crée une sorte d'aléa moral.

Il est évident qu'une monnaie décentralisée peut également être dévaluée. En effet, les nouvelles technologies peuvent faire baisser le coût d'extraction d'un produit naturel rare, et par conséquent, le marché peut se retrouver inondé de nouveaux approvisionnements. Une fois qu'un produit perd sa rareté, il devient beaucoup moins utile. C'est pourquoi le sel, les coquillages et les perles de verre ne sont plus utilisés comme monnaies. Il était autrefois difficile de les collecter à grande échelle, mais maintenant, c'est devenu très facile et bon marché grâce à l'innovation technologique.

L'or est l'une des rares exceptions. Il continue à conserver remarquablement sa valeur après des milliers d'années d'extraction. Bien que l'or ait quelques utilisations industrielles et décoratives, sa difficulté historique d'extraction en a fait une monnaie relativement saine et dont le pouvoir d'achat stable en a fait une très bonne réserve de valeur. Même aujourd'hui, les bijoux en or sont utilisés dans certains pays comme un moyen de se mettre à l'abri des crises économiques. L'or a deux principaux inconvénients: son caractère physique et son poids. Il est ainsi difficile à stocker, à sécuriser et à déplacer.

De nombreux partisans de Bitcoin croient qu'il peut finalement remplacer l'or comme meilleure réserve de valeur sur le long terme. Comme nous allons le montrer dans ce chapitre, bitcoin décentralisé et plus rare que l'or, mais aussi beaucoup plus facile à transporter et stocker en toute sécurité.

La Rareté Numérique Décentralisée

Avec l'avènement d'Internet, l'information pourrait enfin être numérisée et distribuée à grande échelle. La copie d' un fichier numérique est beaucoup plus facile et moins coûteuse qu'une reproduction d'un objet physique .

La digitalisation de la monnaie était une innovation nécessaire pour le e-commerce. Elle a éliminé le besoin de transfert physique. N'importe quel produit peut être envoyé à la vitesse du courrier électronique ou d'un chargement de page web. Cela a réduit les frictions et permis de mondialiser le commerce. Les versions numériques de la monnaie fiduciaire sont créés par les banques, puis utilisées sur les réseaux de paiement par cartes de crédit (Visa, MasterCard), sociétés de vente au détail (Alibaba, Amazon, Apple) et même des processeurs de paiement natifs d'Internet (WeChat, PayPal, Square).

Le fait pour ces sociétés d'être les seuls maîtres en ce qui concerne l'utilisation du système de paiement leur donne la possibilité de censurer les transactions. Elles peuvent saisir de l'argent et fermer des comptes sans le moindre consentement du client. De plus, puisqu'il s'agit de structures centralisées, ces entreprises sont souvent la cible de pressions gouvernementales ou même des piratage qui peuvent entraîner la perte de fonds ou de données des utilisateurs. Avant Bitcoin, c'était le compromis inévitable pour la monnaie électronique numérique : elle devait être artificiellement rare, ou contrôlée par une autorité centrale. Il ne semblait pas y avoir un moyen de créer une rareté numérique.

Satoshi Nakamoto a révélé une innovation le 31 octobre 2008, en présentant bitcoin comme une nouvelle monnaie électronique dont la rareté est ancrée dans le fait qu'il existe des pièces numériques rares : les nombres rares. Certains des nombres les plus rares sont les nombres premiers. Un nombre premier, comme 2,3 ou 5 ne peut être divisé que par 1 et lui-même.

Les nombres premiers deviennent de plus en plus rares à mesure que les chiffres deviennent plus gros. Par exemple, il y a 25 nombres premiers entre 1 et 100. On pourrait alors s'attendre à ce qu'il y ait 250 nombres premiers entre 1 et 1000, mais il n'y en a que 168. Les nombres premiers deviennent incroyablement rares après 100 milliards, à tel point qu'il y a toujours une recherche mathématique mondiale en cours pour le plus grand nombre premier.

Les nouveaux bitcoins sont créés à travers une compétition mondiale où les participants recherchent des nombres rares, tout comme les nombres premiers. Cela crée de la rareté numérique décentralisée. C'est ce qui rend l'invention de Nakamoto si profonde. Chaque actif avant Bitcoin était soit totalement centralisé (World of Warcraft gold), physique (argent), ou duplicable à l'infini (MP3s). Un actif décentralisé, numérique et rare n'existait tout simplement pas avant Bitcoin.

Minage du Bitcoin: Traitement décentralisé des paiements

La nature décentralisée du bitcoin est basée sur le fait qu'il est, tout comme l'or, naturel, rare et difficile à extraire . Un peu comme dans une mine d'or, le minage du bitcoin consiste à rechercher un élément très rare. Une fois qu'un mineur de bitcoin retrouve le le nombre rare recherché, il facilement vérifiable, et à peu de frais, par l'ensemble du réseau tout comme l'or peut être facilement distingué de l'or des fous.

Au lieu d'utiliser des pioches et des machines d'excavation comme pour la recherche d'or, les mineurs des bitcoins utilisent des ordinateurs puissants pour chercher des numéros rares très particuliers. Une fois trouvé, chaque numéro rare est appelé une "preuve de travail". En effet, il prouve à l'ensemble du réseau qu'un travail a été fait pour trouver la réponse.

Comme pour l'or, aucune autorisation n'est requise pour faire le minage : n'importe qui peut télécharger un simple logiciel, allouer de la puissance de calcul au réseau pour rechercher la preuve de travail. Encore mieux que l'exploitation d'or, aucun terrain spécial n'est requis; juste de l'équipement informatique et une source d'énergie abordable. En conséquence, les mineurs du monde entier entrent indépendamment dans une compétition pour trouver des preuves de travail qui répondent aux critères requis par le réseau Bitcoin.

Ainsi, Bitcoin fonctionne sans un seul point de défaillance. Comparez cela aux systèmes centralisés : si le réseau Visa tombe en panne, personne ne peut payer quoi que ce soit avec sa carte Visa. Même chose pour Paypal ou Amazon si leurs réseaux respectifs subissent une panne. Contrairement à ces entreprises, Bitcoin n'a pas d'autorité centrale ou un seul point de défaillance. Personne ne peut choisir de censurer une transaction particulière. Le réseau inarrêtable des mineurs fournit un service critique: traiter les transactions sans les vulnérabilités que peut causer une autorité centrale.

Comment fonctionnent les transactions en bitcoin

Mais comment fonctionne une transaction en bitcoin?

Pour comprendre ce mécanisme, considérez une chose plus familière : le registre d'une banque. Après que quelqu'un ait fait un chèque pour payer un bien ou un service, le bénéficiaire se rend à sa banque pour déposer le chèque. En supposant que les deux clients ont un compte dans cette banque, celle-ci n'a qu'à débiter le compte de l'expéditeur et créditer celui du destinataire.

L'ensemble du processus exige d'ajouter seulement deux entrées dans le livre comptable de la banque. Les fonctionnaires de la banque ne vont pas dans un coffre, prendre le montant exact de la réserve de l'expéditeur puis le mettre dans la réserve du destinataire. La comptabilité à l'aide d'un grand livre (registre) a été une invention historique clé. Elle a rendu le transfert d'argent beaucoup moins laborieux. L'équivalent d'un chèque bancaire en bitcoin est une *transaction*.

Bitcoin utilise un type particulier de registre appelé la *blockchain*. Des milliers de personnes exécutant le logiciel de validation Bitcoin vérifient la blockchain en continu à la place d'une autorité centrale. Chaque personne qui exécute ce logiciel conserve une copie de l'ensemble du registre et vérifie les nouvelles entrées. Cela s'appelle l'exécution d'un *nœud complet*. Chaque nœud complet vérifie constamment si les règles du jeu sont respectées. De cette manière, aucune autorité centrale ne peut arbitrairement modifier les données enregistrées dans le but de voler des bitcoins ou en dépenser une quantité qu'il ne possède pas. La Blockchain du bitcoin est *publique* car n'importe qui peut consulter les détails sur les transactions.

Ceux qui ont des bitcoins effectuent des transactions de la même manière qu'ils pourraient écrire un chèque. Ils spécifient le montant et signent le chèque. Mais au lieu de gribouiller leur nom sur un papier facilement falsifiable, ils signent numériquement leurs transactions en utilisant la cryptographie.

Cette signature numérique est créée en utilisant un secret connu uniquement par le propriétaire des bitcoins.Ce secret est appelé la *clé privée*. C'est avec la clé privée que l'expéditeur arrive à prouver au destinataire qu'il possède des bitcoins.

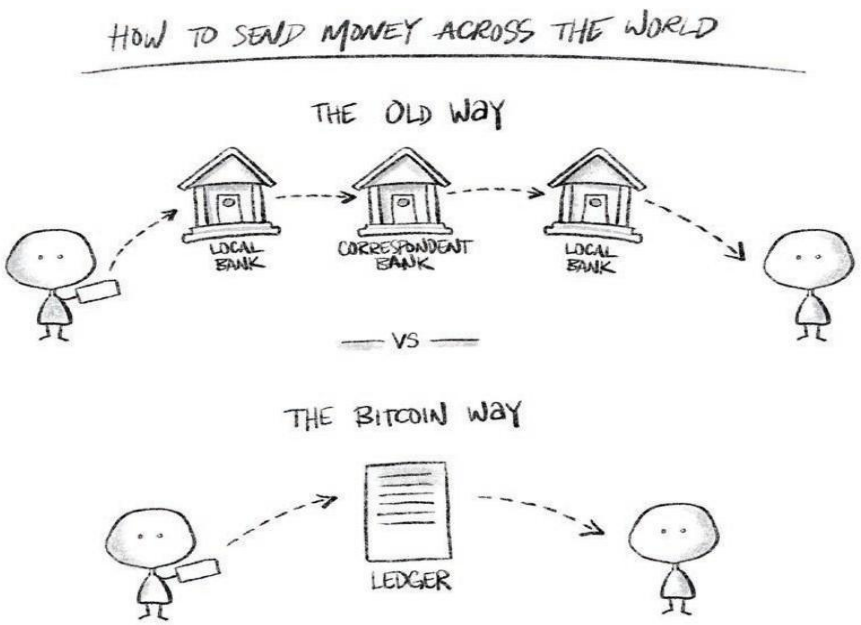
Les utilisateurs stockent les bitcoins dans un *portefeuille*, un logiciel exécuté sur un ordinateur, un téléphone portable, ou un support matériel spécialisé. Chaque seconde, de nouvelles transactions en bitcoin sont initiées à partir de portefeuilles partout dans le monde, sans passer par un processeur de paiement central. Au lieu de cela, des mineurs installés partout dans le monde rivalisent pour enregistrer les transactions dans le registre. Ils utilisent leur équipement informatique et essayent de trouver la preuve de travail. Toutes les 10 minutes

environ, quelque part dans le monde, un mineur trouve une preuve de travail qui correspond à un bloc contenant des transactions en attente d'être validées. Ensuite, le mineur relai ce bloc au réseau Bitcoin pour validation.

Chaque bloc est comme une nouvelle page du registre. Les nœuds complets sur le réseau permettent de vérifier que les transactions contenues dedans sont valides. N'importe qui peut exécuter un nœud complet; cela permet à des milliers d'utilisateurs de vérifier constamment la validité de chaque nouveau bloc. Si le réseau confirme que le bloc proposé par un mineur est valide, ce dernier reçoit une récompense de 12.5 nouveaux bitcoins. Le bloc validé et toutes les transactions qu'il contient deviennent ainsi une partie permanente de l'histoire du Bitcoin. À l'heure où nous écrivons ces lignes, une transaction bitcoin prend moins d'une heure pour être enregistrée sur la blockchain.

Le Blockchain du Bitcoin tire son nom du fait qu'il s'agit d'une suite de tous les blocs, ou toutes les pages, dans l'historique. En d'autres termes, la blockchain est le registre complet et immuable de toutes les transactions effectuées sur le réseau Bitcoin depuis sa création en janvier 2009.

Le réseau Bitcoin est constitué de milliers de nœuds complets. Chacun d'entre eux valide indépendamment les nouveaux blocs proposés par les mineurs. Avec des exigences matérielles relativement modestes, la plupart d'ordinateurs portables modernes peuvent exécuter un nœud complet. Le mettre en place reste relativement bon marché et abordable; cela garantit que le réseau reste décentralisé.



La Politique monétaire de Bitcoin

Contrairement au système monétaire piloté par les banques centrales, qui est opaque et en constante évolution, la politique monétaire de Bitcoin est transparente et gravée dans le marbre.

Comment les nouveaux bitcoins sont-ils émis? Comme mentionné plus haut, un mineur qui trouve une preuve de travail valide et la couple avec un groupe de transactions valides — crée un nouveau bloc valide — et a droit à ce qu'on appelle la récompense de bloc. Au moment de la rédaction de ce bouquin, la récompense de bloc est 12.5 bitcoins. Elle est divisée par 2 tous les quatre ans, ce qui signifie qu'elle sera de 6.25 bitcoins en 2020, 3.125 bitcoins en 2024 et ainsi de suite.

Si un mineur tente de tricher pour réclamer nombre de bitcoins supérieur à la récompense de bloc prévue, ce bloc est rejeté par les nœuds complets. Ces derniers vérifient tous les blocs proposés; ceux qui ne respectent pas les règles ne sont pas relayés sur la blockchain. C'est un peu comme lorsqu'une banque rejette un chèque qui présente un découvert sur le compte émetteur. En conséquence, personne ne peut fabriquer de faux bitcoins. Toute transaction qui tente de dépenser des bitcoins qui n'existent pas et tous les blocs qui contiennent de telles transactions sont rejetés par le réseau.

Un bloc invalide (rejeté par le réseau) coûte cher aux mineurs, car il cause un gaspillage de la grande quantité d'électricité dépensée pour faire tourner leur matériel à la recherche de la preuve de travail. Le fait pour la fraude d'être très coûteuse garantit une protection supplémentaire au réseau Bitcoin. Néanmoins, s'il n'existait que quelques nœuds complets sur le réseau, un mineur pourrait les soudoyer pour être en mesure d'introduire un bloc frauduleux dans la blockchain. Étant donné qu'il existe plusieurs milliers de nœuds complets sur le réseau, et que ces derniers sont géographiquement dispersés et inconnus les uns des autres, une telle stratégie est garantie d'échouer.

Satoshi a, dès le départ, fixé l'offre totale de tous les bitcoins à 21 millions. Aujourd'hui, plus de 85 % de cette offre ont déjà été extraits, ce qui signifie que plus de 18 millions de bitcoins sont maintenant en circulation. Le reste sera libéré sous forme de récompenses destinées aux mineurs, en nombre de plus en plus petits, selon un plan d'émission connu de tous.

La technologie blockchain toujours en attente

Beaucoup ont essayé de reproduire l'invention réussie de Satoshi Nakamoto. Une stratégie populaire qui consiste à prendre le système de grand livre distribué de Bitcoin et l'appliquer à d'autres cas d'usage. Depuis 2014, de nombreuses entreprises bien connues ont essayé d'utiliser des blockchains dans plusieurs secteurs, elles ont investi des millions de dollars dans cet effort. Cela a été à la base d'un battage médiatique sans précédent autour de la *technologie blockchain*.

Malheureusement, la plupart de ces tentatives sont jusqu'à présent comparable à l'utilisation d'un chariot pour faire les courses. La blockchain fonctionne parfaitement dans son contexte d'origine (stockage du registre de transactions pour la monnaie numérique décentralisée), mais semble être trop lente, inutilement coûteuse et non fonctionnelle pour d'autres applications (c.-à-d. soins de santé sur une blockchain, traçabilité des fruits sur une blockchain, stockage des données météorologiques sur une blockchain, etc.).

Bitcoin est une combinaison de quatre composants importants, dont la blockchain n'est qu'une partie. Le premier est la rareté du bitcoin. Le second est le réseau pair-à-pair de nœuds complets difficile à arrêter. Le troisième est que le minage qui nécessite de trouver la preuve de travail valide et rend la fraude très coûteuse. Le quatrième est la blockchain entièrement et publiquement vérifiable. Ces quatre technologies sont étroitement intégrées au protocole. Quand un seul de ces quatre éléments n'est pas pris en compte ou est retiré de Bitcoin, le résultat donne quelque chose de bien moins utile.

Pour un actif purement numérique comme bitcoin, le fait d'utiliser une blockchain en tant que registre public fonctionne. Mais pour des objets réels comme les grains de café ou les données de santé, il n'y a aucun moyen de garantir qu'une l'information est infaillible car il est toujours possible que des erreurs soient commises lors de la saisie des données en raison d'une négligence, voire d'une fraude pure et simple. Une autorité centrale doit donc être présente pour garantir l'exactitude de toutes les informations, ce qui rend inutile l'utilisation d'une blockchain.

Cependant, d'énormes sommes d'argent ont été investies dans la technologie blockchain à la recherche de cas d'usage allant au-delà de la monnaie décentralisée. À l'heure où nous écrivons ces lignes, personne n'a été en mesure de créer un

système d'archivage à grande échelle utilisant une blockchain qui améliore de manière significative les approches plus traditionnelles, voire qui les égale.

Qu'en est-il d'autres cryptomonnaies?

Les gens n'ont pas simplement tenté de copier le protocole Bitcoin; ils ont également créé d'autres cryptomonnaies, ainsi appelées parce que, tout comme bitcoin, les expéditeurs de ces nouvelles monnaies utilisent des signatures numériques pour relayer les transactions. Souvent appelés altcoins ou tokens, ces projets ne sont pas décentralisés et beaucoup sont juste des escroqueries. Bitconnect est l'exemple célèbre d'une cryptomonnaie basée sur la fraude.

Une poignée de cryptomonnaies peuvent avoir des cas d'usage légitimes. C'est notamment le Monero (XMR) et Zcash (ZEC), qui visent à permettre aux utilisateurs d'effectuer des transactions de façon plus confidentielle que ce que permet Bitcoin, ou Ethereum (ETH) dont les gens se servent pour tenter de construire des plateformes d'applications décentralisées. Des grandes entreprises expérimentent également les cryptomonnaies. Facebook a annoncé la cryptomonnaie Libra, qui a le potentiel de devenir très populaire en raison des milliards de personnes qui utilisent les services de Facebook. Cependant, Libra est centralisé par nature et ne sera ni résistant à la censure ni rare comme bitcoin. Plusieurs autres groupes ont essayé de copier le succès de Satoshi d'une manière particulièrement effrontée en créant des cryptomonnaies dont les noms contiennent le mot Bitcoin. Ainsi, il y a souvent confusion au sujet de quelle crypto-monnaie est réellement Bitcoin. Pour les distinguer, il faut rechercher le symbole "BTC" sur les plateformes d'échange et les portefeuilles. Les variantes du bitcoin sont comme l'or des fous ; elles peuvent sembler similaires mais sont beaucoup plus centralisées et ont un prix beaucoup plus bas. Ceux-ci comprennent Bitcoin Cash (BCH), Bitcoin Gold (BTG) et Bitcoin Satoshi's Vision (BSV).

Résumé

Bitcoin est une innovation technique profonde qui offre une nouvelle alternative au système financier existant.

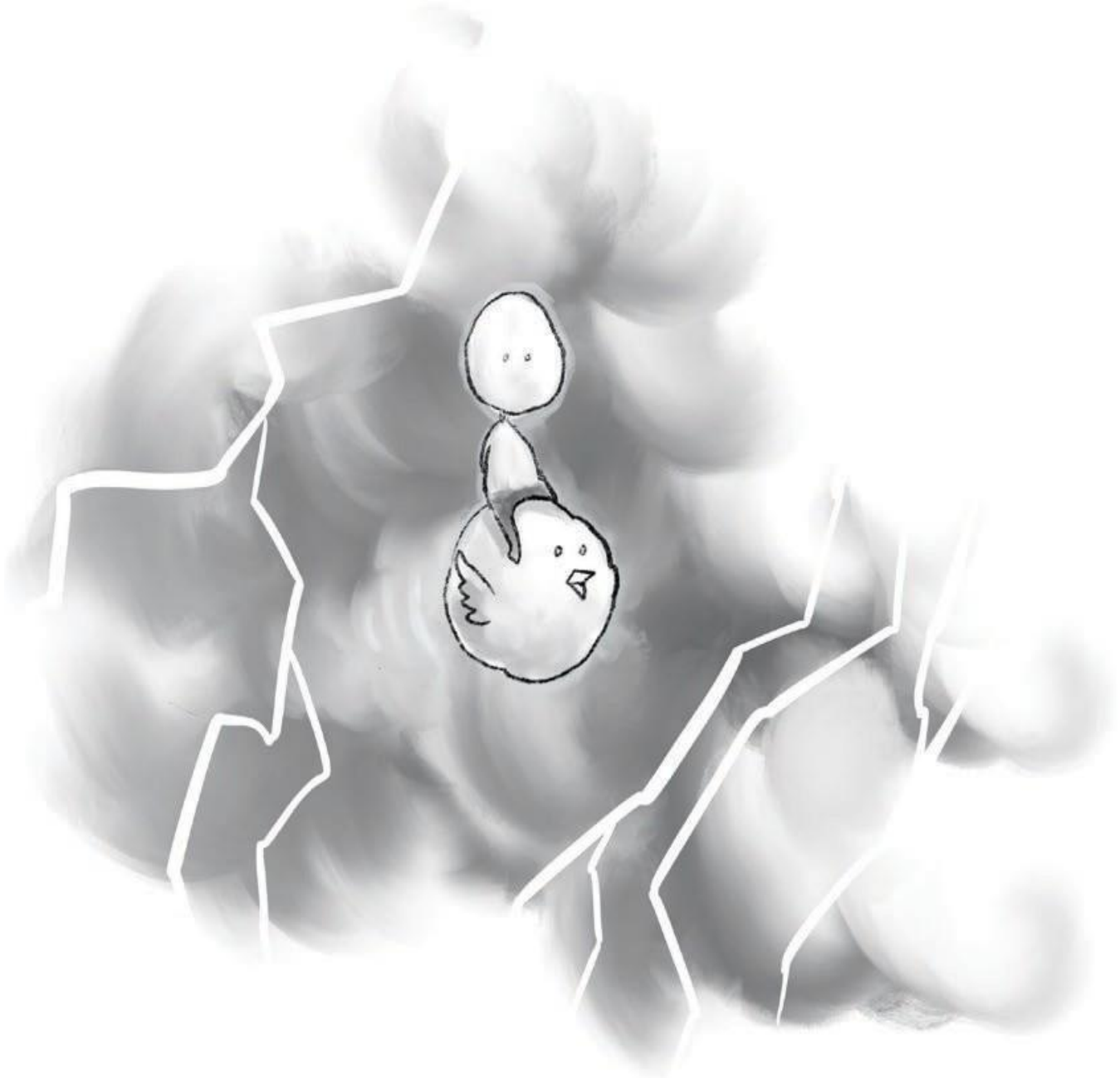
Bitcoin est la monnaie numérique facile à utiliser pour effectuer des transactions partout dans le monde car elles sont réglées en quelques minutes au lieu de plusieurs jours.

Bitcoin est un actif rare, capable de protéger contre la menace d'une inflation arbitraire.

Bitcoin est décentralisé, ce qui empêche quiconque de censurer des paiements.

Bitcoin est la seule monnaie décentralisée et numériquement rare au monde.

Bitcoin a le potentiel de bouleverser l'ordre monétaire actuel.



CHAPITRE 3

Prix et volatilité du bitcoin

Avertissement : Les auteurs de ce livre ne sont pas des professionnels de l'investissement. Ce chapitre propose les raisons possibles des mouvements de prix du bitcoin et sa volatilité globale, et ne contient aucun conseil d'investissement.

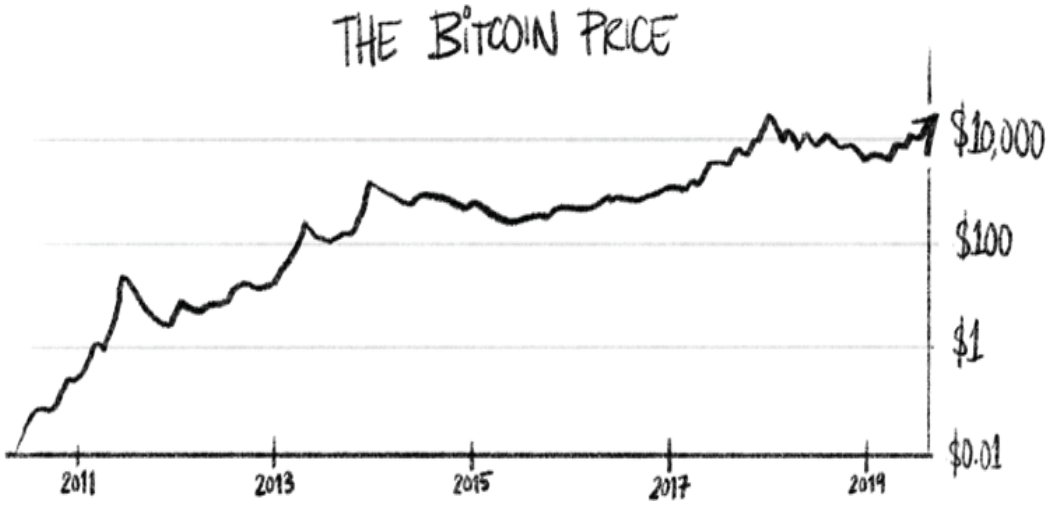
Tout le monde veut savoir : Pourquoi le bitcoin a -t-il une telle valeur? Pourquoi son prix a-t-il tant augmenté? Pourquoi est-il si volatile? Pourquoi bitcoin vaut-il quelque chose si, contrairement au dollar américain, il n'est pas soutenu par une économie, ou plus cyniquement, par des menaces d'amendes et de prison?

Le prix d'un actif varie lorsque il y a un déséquilibre entre acheteurs et vendeurs. Pour bitcoin, ces déséquilibres sont déterminés par quelques facteurs qui diffèrent à long, moyen et court terme.

Perspective long terme

Au cours de la dernière décennie, le prix du bitcoin a augmenté d'une fraction de centime à un sommet historique avoisinant les 20 000 $. En août 2019, un bitcoin coûtait près de 11 000 $.

Prix du bitcoin de sa création à aujourd'hui (échelle logarithmique)



Bitcoin est rare. Comme expliqué dans le chapitre 2, son offre est établie à 21 millions d'unités. Un offre fixe et un rythme d'émission transparent attirent les acheteurs alors que l'alternative, la monnaie fiduciaire, est universellement sujette à l'inflation, ce qui signifie que la même quantité d'argent achète moins de biens chaque année. À long terme, il est probable que de plus en plus de personnes soient attirées par bitcoin car aucun gouvernement ne peut en imprimer davantage, censurer les transactions ni les confisquer facilement.

La valeur totale de tous les bitcoins minés est seulement 200 milliards USD. En revanche, la valeur de tout l'or extrait est estimée à environ 9 000 milliards de dollars. À seulement 2 % de la valeur de l'or, le marché du bitcoin est trop petit, et donc, plus sensible aux fluctuations des prix. Le volume quotidien échangé est également relativement faible : environ 10 milliards de dollars par jour contre 300 milliards de dollars par jour pour l'or. En raison de la faible liquidité, c'est-à-dire le montant qui peut être facilement acheté ou vendu au cours d'une période donnée, même les petits acheteurs ou vendeurs peuvent avoir un impact important sur le prix. Plus l'adoption du bitcoin va croître, plus il deviendra une classe d'actifs mondiale et sa volatilité va diminuer. Cela pourrait prendre plusieurs décennies.

.

Perspective à moyen terme

En observant le cours du bitcoin sur plusieurs mois ou années, le constat semble clair : les principaux facteurs de la variation des prix sont les coûts du minage, la demande des acheteurs institutionnels et le halving.

Le minage a des coûts : équipement, exploitation de data centers, frais d'électricité,... Ces coûts sont généralement payés en monnaie fiduciaire. Par conséquent, la plupart des mineurs vendent régulièrement une partie ou la totalité des bitcoins qu'ils extraient pour payer les coûts opérationnels, qui s'élèvent approximativement à 250-300 millions de dollars par mois, soit 40-50 % de la valeur des bitcoins extraits mensuellement au moment de la rédaction de cet article.

La demande du bitcoin à moyen terme provient généralement des acheteurs institutionnels, de particuliers fortunés et et des fonds de dotation qui souhaitent s'exposer aux cryptomonnaies. Ils commencent généralement par bitcoin.

Un autre facteur important influant sur le prix à moyen terme est le halving. Comme décrit dans le chapitre 2 , la récompense de bloc est divisée par 2 tous les quatre ans. Bitcoin a eu deux halving jusqu'à présent, en 2012 et 2016. Les deux événements ont créé un déficit de l'offre qui a occasionné à son tour une augmentation de la volatilité.

L'évolution du prix du bitcoin a tendance à attirer plus de spéculateurs, qu'il s'agisse d'investisseurs particuliers cherchant à en acheter pour une valeur de 100 dollars ou d'investisseurs institutionnels en achètent pour des millions de dollars. Cette situation amène le prix du bitcoin à s'apprécier en plus de l'attention croissante des médias et la peur de rater le train (FOMO) qui ajoutent de l'huile sur le feu. Cette dynamique a créé de grandes bulles qui se sont soldées par des effondrements de prix de 80 % ou plus. Il est tout à fait possible que ces genres de cycles se répètent après les futurs halvings.

Perspective à court terme

L'absence d'autorité centrale entraîne un effet secondaire important : la volatilité.

La nature des exchanges a un impact sur la volatilité du cours du bitcoin à court terme. Il existe plusieurs types d'exchanges tels que les *plateformes fiat-to-crypto*, qui facilitent la conversion de la monnaie fiduciaire en bitcoins, les les plateformes pair-à-pair (P2P), qui mettent en contact direct acheteurs et vendeurs et les plateformes crypto-to-crypto, qui supportent uniquement les échanges entre cryptomonnaies. Comme les traders cherchent à tirer profit de la volatilité, certaines plateformes rendent possible le trading à effet de levier, qui consiste à inciter les utilisateurs à négocier jusqu'à 100 fois le montant de leur mise.

Les plateformes d'échange des cryptomonnaies existent principalement sur Internet. Elles fonctionnent chaque minute de l'année et sont accessibles aux investisseurs particuliers. En revanche, les marchés traditionnels sont généralement ancrés dans des grands centres financiers comme Londres, New York, ou Hong Kong. Ces derniers permettent la négociation directe pendant environ 7.5 heures du lundi au vendredi, et sont principalement utilisés par les courtiers et non les investisseurs particuliers.

Etant donné que n'importe qui peut envoyer et recevoir des bitcoins grâce à un simple ordinateur et une connexion Internet, il est relativement facile pour un entrepreneur de créer une plateforme d'échange. Bitcoin n'étant pas considéré comme un titre, les plateformes sur lesquelles il est échangé peuvent être soumises à des normes réglementaires moins strictes que les marchés traditionnels.

Par ailleurs, les plateformes d'échange crypto-crypto recherchent souvent des juridictions moins hostiles comme Malte, les Seychelles ou les Philippines car elles n'ont pas besoin de comptes bancaires en monnaie fiduciaire et leur équipes ont la possibilité d'opérer à distance. Déposer de l'argent sur une plateforme d'échange revient à faire confiance à cette dernière pour la garde sécurisée de ses fonds. Malheureusement, plusieurs plateformes sont mal gérées. Les cas de malversations ou d'incompétence bien documentés et ayant entraîné des vols à grande échelle comprennent Mt. Gox, Bitfinex, et Quadriga. Ensemble, ils ont perdu la trace de dizaines de milliers de bitcoins (plusieurs milliards de dollars).

Avertissement aux lecteurs : Un certain nombre de plateformes d'échanges ont été piratées ou ont perdu les bitcoins de leurs clients. Les lecteurs doivent faire preuve de prudence lorsqu'ils les utilisent et ne devraient risquer qu'un nombre de bitcoin qu'ils peuvent se permettre de perdre .

Le fait que bitcoin soit adapté au trading de détail en ligne contribue à sa volatilité à court terme. Alors que les banques centrales cherchent généralement à minimiser la volatilité, les traders la trouvent plus rentable.

Dans les délais d'une minute à un mois, la volatilité du cours du bitcoin peut être extrême. Le 1er janvier 2019, un Bitcoin s'échangeait à $3500. En Août la même année, il coûtait presque 11 000 $. Les fluctuations quotidiennes pouvant atteindre 20 % ne sont pas anormales. Cela peut être terrifiant pour les investisseurs mais c'est un paradis pour les spéculateurs qui profitent du mouvement des prix.

Contrairement aux marchés traditionnels des actions ou de la dette, bitcoin n'a pas de fondamentaux commerciaux qui déterminent un consensus sur son prix. Bitcoin n'a pas d'employés, aucune performance du produit et aucun flux de trésorerie. L'absence des indicateurs de performance à court terme signifie que les investisseurs mettent l'accent sur les éléments techniques du trading qui sont souvent à somme nulle. Pour ces spéculateurs, le trading des cryptomonnaies est une autre forme de poker en ligne qui se joue dans le confort de leurs salons et à leur convenance.

Comme pour les marchés traditionnels, le prix du bitcoin peut réagir à des nouvelles sensibles. Cependant, il ne grimpe ni ne chute pas forcément avec les bonnes ou mauvaises nouvelles. Par exemple, en 2013, des hackers ont piraté Mt.Gox, la plus grosse plateforme d'échange à l'époque. Une baisse significative des prix s'en est suivie. Cependant, en 2018, 40 millions de dollars ont été dérobés de Binance, la plus importante bourse d'aujourd'hui; après ce coup, le prix du bitcoin a progressé à la hausse.

Plus bitcoin va gagner en valeur et en liquidité, sa volatilité va probablement diminuer. Cela est similaire aux fluctuations de prix des actions célèbres contre des actions moins connues. Par exemple, il est beaucoup plus difficile pour un trader particulier de faire bouger le prix d'Apple que le prix d'une action à un centime.

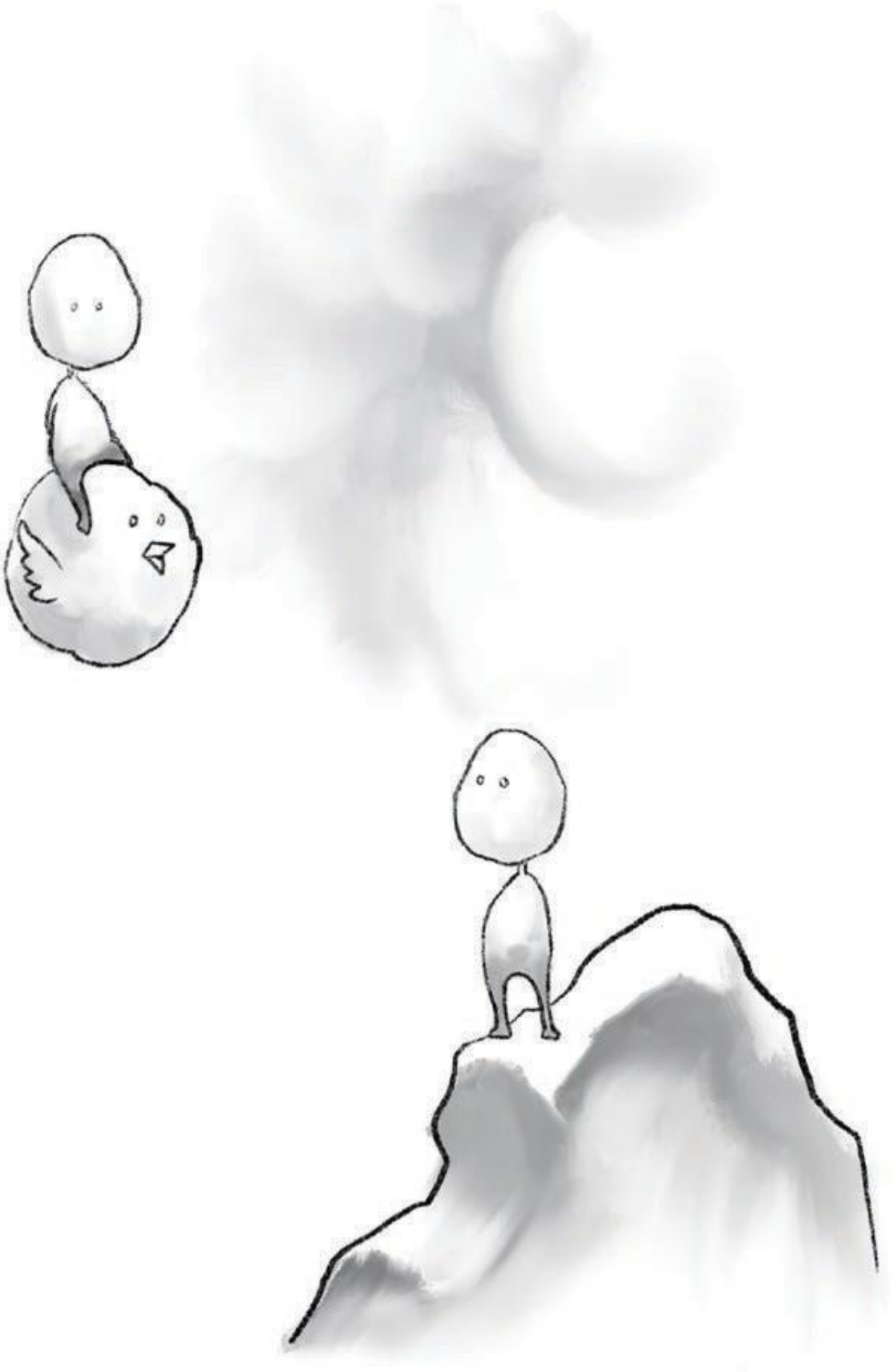
Bitcoin est un actif unique et très risqué pour les traders. L'attrait du bitcoin pour les spéculateurs combiné à son manque de liquidité et la possibilité de le trader avec effet de levier ajoutent une importante volatilité de son cours à court terme.

Résumé

Depuis la création du bitcoin, son prix s'est apprécié à la suite d'une demande de plus en plus croissante et surtout grâce à son offre fixe. À court terme, son cours est sujet à la spéculation, à la manipulation de marché et à une forte volatilité.

En fin de compte, la valeur et la volatilité du bitcoin résident à la fois dans son offre fixe et sa nature décentralisée.

Si Bitcoin évolue au-delà de son rôle de réserve de valeur et en vient à représenter l'unité de mesure de l'économie numérique (comme la monnaie fiduciaire l'est pour l'économie physique aujourd'hui), il deviendra un moyen de paiement et une unité de compte. À ce stade, la volatilité pourrait diminuer car dans ce cas bitcoin sera plus ancré sur l'échange de valeur plutôt que la spéculation. En attendant, son prix restera soumis au gré des forces du marché décrites dans les sections moyen et court terme de ce chapitre et continuera à fluctuer de façon spectaculaire.



CHAPITRE 4

Pourquoi Bitcoin compte pour les droits humains

Avec l'invention de Bitcoin, les individus sont maintenant en mesure de consolider le fruit de leur travail en stockant la valeur sous forme d'information numérique. Cela permet d'éviter que les États ou les entreprises contrôlent arbitrairement la façon dont les citoyens économisent ou transfèrent l'argent. Les ramifications de cette révolution monétaire en matière de droits humains se font déjà sentir et continueront de s'intensifier dans le monde entier, en particulier dans les dictatures mais aussi dans les démocraties libérales.

Le premier chapitre présente l'histoire de personnes, du Nigeria au Venezuela, qui ont dû faire face à une inflation élevée, à la surveillance financière, à l'inaccessibilité des services bancaires et à des infrastructures économiques défaillantes.

Il ne s'agit pas d'histoires isolées. Selon les données de Human Rights Foundation, près de la moitié de la population mondiale vit sous l'autoritarisme. Cela représente environ 4 milliards de personnes, du Cuba à la Biélorussie, de l'Arabie Saoudite au Vietnam, qui sont sévèrement réprimées par leur gouvernement. Nombre d'entre elles sont des réfugiés économiques ou des prisonniers politiques. Ces personnes ne bénéficient d'aucun État de droit ni de la possibilité de réclamer pacifiquement des réformes. Même les gouvernements américains et européens oppriment financièrement leurs citoyens par la surveillance et une inflation croissante.

Le renflouement des banques, les interventions militaires extérieures, le renforcement de la sécurité aux frontières et les aides sociales subventionnées ne sont que quelques-unes des activités douteuses rendues possibles par l'impression de la monnaie du néant..

Quand les citoyens sont forcés d'utiliser des plateformes de paiement centralisés comme le Chinois WeChat qui microtrace des millions de vies, quand le compte bancaire d'un groupe de défenseurs de droits humains est gelé par un dictateur, ou quand les sanctions contre un pays punissent les populations pour les crimes que leurs dirigeants non élus ont commis, Bitcoin peut constituer une porte de sortie.

L'invention de Satoshi peut grandement aider les centaines de millions de personnes qui n'ont pas de comptes bancaires ou de cartes d'identité officielles nécessaires pour accéder aux services financiers de base. Avec un simple téléphone et une connexion internet, les personnes les plus vulnérables de la planète peuvent recevoir des bitcoins de n'importe qui, rapidement et à moindre coût, sans aucune possibilité de censure ou de confiscation.

Bitcoin est en train de changer la donne en ce qui concerne les paiements, les transferts de fonds transfrontaliers et peut améliorer de nombreux autres aspects de la société. Il a créé un véritable marché mondial de biens et services et peut ouvrir la voie à des règles du jeu plus équitables.

Devenir sa propre banque

Dans des endroits comme le Bahreïn, la Russie et le Zimbabwe, le gouvernement exerce un contrôle total sur le système bancaire. Comme conséquences, il y a dans ces pays des niveaux élevés de détournement de fonds et de corruption. Bitcoin pose les bases d'un monde où les Etats et les entreprises ont moins de contrôle et les individus plus de liberté de faire des choix indépendants.

Chaque personne qui détient des bitcoins a un contrôle total sur ces derniers. De plus, lorsque un bitcoin est envoyé, il n'y a pas d'intermédiaire qui puisse censurer la transaction ou divulguer les informations personnelles de l'expéditeur. Cela offre une protection contre les voleurs, les entreprises malveillantes et l'espionnage des gouvernements. Aucune autre monnaie ou société de paiement ne peut se vanter d'offrir un tel niveau de sécurité.

Cacher de l'argent liquide sous un matelas a longtemps été un moyen pour les personnes vivant dans des économies brisées de garder leurs avoirs. L'inconvénient évident est que la monnaie liquide est difficile à sécuriser et peu pratique à transférer. Si les autorités se pointent à la porte, elles peuvent physiquement saisir l'intégralité de l'argent liquide qu'elles trouvent dans une maison. En comparaison, le bitcoin est facile à stocker et à sécuriser car la clé privée ou le mot de passe secret peuvent être sauvegardés sur un papier, un ordinateur, une clé USB; elle peut même être mémorisée. Il est également possible de nier la propriété des bitcoins car les autorités n'ont aucun moyen facile de les saisir physiquement.

Se protéger de l'inflation

L'iran et le Somaliland impriment de la monnaie de façon illimitée, asséchant l'épargne durement économisée par des populations déjà très pauvres.

Bien entendu, l'inflation est un phénomène auquel toutes les banques centrales s'adonnent. Généralement, elles considèrent que de petites injections de liquidités dans l'économie sont souhaitables, car cela permet de maintenir les marchés en mouvement. Les vieilles démocraties arrivent à faire preuve d'une certaine retenue, mais comme nous l'avons vu, l'inflation peut rapidement devenir incontrôlable.

Selon les indices des prix à la consommation, de 2018 à 2019, les prix ont augmenté de 1,7 % en Allemagne et de 1,9 % aux États-Unis. Dans de nombreux pays, les prix des biens à la consommation ont beaucoup plus augmenté : 3,75 % au Brésil, 5 % en Inde, 11 % au Nigeria, 20 % en Turquie et un énorme 47 % en Argentine. Les habitants des pays où la hausse des prix est supérieure à 10 % ont vécu une dépréciation brutale de leurs revenus et de leur épargne.

Le cas extrême est le Venezuela. En raison de l'impression monétaire incessante, d'une corruption systématique et de la mauvaise gestion de l'économie, les prix ont augmenté de 2 300 000 % en 2018 - une hyperinflation si grave qu'elle a rendu l'épargne impossible. L'argent commence à s'évaporer quelques heures après son arrivée sur un compte bancaire. Cela oblige les Vénézuéliens à vivre au jour le jour, en investissant l'argent, dès qu'ils en gagnent, dans les biens essentiels.

Les Vénézuéliens vivent sous un régime autoritaire. Ils ne peuvent pas participer à des élections libres et équitables qui leur permettraient de demander des comptes au gouvernement. Au cours des dernières années, plus de 4 millions de citoyens, qui représentent plus de 10 % de la population du pays, ont fui vers les pays voisins, comme le Brésil et la Colombie, dans ce qui est devenu l'une des crises de réfugiés les plus graves au monde.

Outre le fait d'éviscérer l'économie locale, le régime vénézuélien a imposé un contrôle sévère des capitaux pendant près de deux décennies. Il est extrêmement difficile d'envoyer l'argent tant à l'intérieur qu'à l'extérieur du pays. Le principal moyen d'envoyer de l'argent est de passer par des intermédiaires qui disposent des comptes dans deux pays : un particulier peut donner des pesos colombiens à un intermédiaire ayant un compte au Venezuela, qui transfère ensuite le montant équivalent en bolivars vénézuéliens à la destination finale.

Même cette solution de contournement est maintenant interrompue car les banques, sous la pression du gouvernement, signalent les personnes qui utilisent leurs comptes vénézuéliens depuis l'étranger.

Référez-vous au premier chapitre : le régime vénézuelien ne veut pas que sa population puisse avoir accès à une monnaie plus saine que le bolivar.

Une autre option consiste à demander à la famille ou aux amis vivant aux États-Unis d'envoyer des dollars américains dans une ville frontalière en Colombie via Western-Union. Le destinataire doit quitter, pas sans risques, le Venezuela pour se rendre dans la ville colombienne afin de retirer les dollars US puis rentrer clandestinement au Venezuela avec l'argent bien caché dans ses vêtements. Une telle opération est , inutile de le préciser, longue et dangereuse car les frontières terrestres et les aéroports sont inondés de fonctionnaires corrompus toujours prêts à confisquer l'argent liquide.

La solution : utiliser Bitcoin pour le transfert d'argent au-delà des frontières. Les Vénézuéliens peuvent demander par message texte du bitcoin à leur familles ou amis à l'étranger et recevoir les fonds quelques minutes plus tard à des frais insignifiants. Une telle transaction ne peut être censurée ni tracée facilement.

Pour les personnes vivant dans des économies stables, bitcoin peut sembler volatile. Cependant, pour les Vénézuéliens, même une brusque fluctuation de 20 % de son cours est légère comparée à la récente dépréciation (2 300 000%) du bolivar.

Une fois les bitcoins reçus sur un téléphone ou un ordinateur, ils peuvent être facilement transformés en monnaie locale grâce à LocalBitcoins.com, un site de type eBay qui met en contact les acheteurs et vendeurs de bitcoins dans plus de 100 pays. Les bitcoins fraîchement reçus peuvent être proposés à la vente sur le site et trouver immédiatement un preneur. En 15 minutes, un vénézuelien peut vendre du bitcoin et obtenir des bolivares sur son compte bancaire. Ce système est utilisé chaque jour pour déplacer des millions de dollars à l'intérieur et à l'extérieur du Venezuela. En mi-2019, bitcoin était déjà devenue une économie parallèle de dernier recours pour les personnes vivant dans des économies complètement brisées comme le Venezuela.

Accès universel à la monnaie

Il est facile pour un citoyen d'une démocratie stable d'ouvrir un compte bancaire. Mais ce n'est pas le cas pour plusieurs milliards de personnes dans le monde. Certains exemples sont frappants. En Afghanistan et en Arabie saoudite, les femmes sont empêchées par les hommes d'ouvrir leurs propres comptes bancaires, elles sont effectivement privées de leur liberté financière.

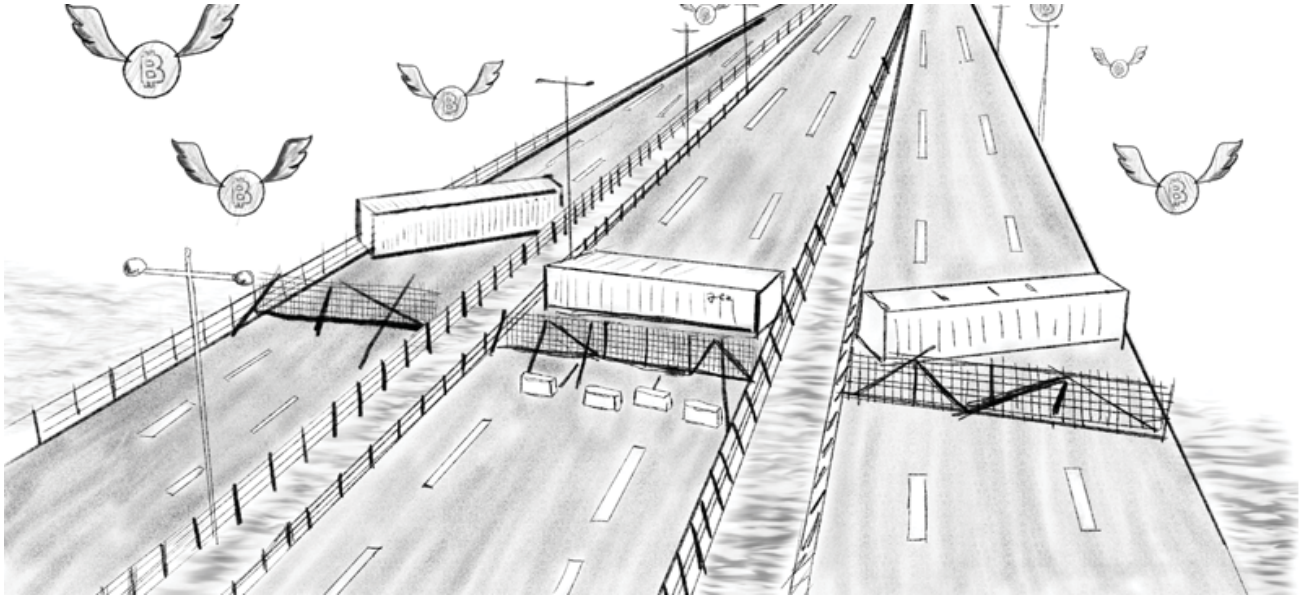
Bitcoin peut devenir une bouée de sauvetage pour elles. En 2014, Roya Mahboob, un entrepreneur dans le milieu de la tech afghan, a fait face à un défi majeur : il ne pouvait plus payer ses employées femmes. Chaque fois qu'il leur payait en liquide, les membres de leur famille récupéraient l'argent. Les hommes ne les laissaient pas ouvrir des comptes bancaires. Des réseaux comme PayPal n'étaient pas disponibles dans le pays. Un ami à Roya a évoqué la possibilité d'utiliser bitcoin pour faire les paiements, ce qui a été fait. Depuis, ces femmes persécutées ont retrouvé une souveraineté financière.

Une de ces jeunes femmes a dû fuir l'Afghanistan suite à une menace de mort. Mais elle a pris ses bitcoins avec elle, stockés sur son téléphone. Elle a voyagé à travers l'Iran et la Turquie pour finalement s'installer en Allemagne.

Là, elle a échangé ses bitcoins, qui s'étaient heureusement appréciés de façon spectaculaire pendant qu'elle faisait son long voyage, en euros pour commencer une nouvelle vie. Cela démontre à quel point le bitcoin peut aider les opprimés non bancarisés à des moments où ils n'ont aucune autre option.

Le fait pour l'infrastructure Bitcoin et les échanges pair-à-pair de se développer dans les années à venir aura un impact majeur sur l'aide extérieur et l'assistance humanitaire. L'image la plus frappante de ce qui ne va pas dans ce secteur est peut-être la photo qui est sortie de la frontière vénézuélienne en février 2019, lorsque le régime Maduro a empêché l'aide étrangère d'entrer dans le pays en barricadant le pont frontalier avec des semi-remorques.

On ne voit pas sur la photo les millions de dollars en bitcoins qui s'échangeaient en ce moment là dans les deux sens, hors de tout contrôle gouvernemental.



Le système d'aide extérieur actuel présente des vulnérabilités flagrantes. Qu'il s'agisse d'un gouvernement qui envoie de l'aide à un autre gouvernement, d'une organisation philanthropique qui fait un don à une ONG ou d'un particulier qui envoie de l'argent à sa famille en cas d'urgence médicale, l'argent n'arrive à destination qu'après avoir transité par plusieurs tiers.

Même dans la situation la plus élémentaire, il y a au moins trois intermédiaires : la banque de l'expéditeur, la banque centrale et la banque du destinataire. Il y a souvent plus d'intermédiaires, parfois jusqu'à sept. Chacun d'entre eux peut ralentir le processus, geler l'opération ou même voler l'argent. Dans un discours en 2012, l'ancien Secrétaire général de l'ONU Ban Ki-moon a déclaré que pendant l'année précédente la corruption avait « empêché 30 % de toute l'aide au développement d'atteindre sa destination finale ».

Les recherches effectuées par les organisations comme GiveDirectly et la Banque mondiale ont démontré que les transferts directs en espèces sont la façon la plus efficace de fournir de l'aide.

Bitcoin rend possible les transferts sans autorisation à toute personne sur la planète en quelques minutes. Le destinataire n'a pas besoin d'un compte bancaire ou d' une identification officielle, juste un accès à internet.

Une récente étude de Pew a révélé que 45% des personnes dans les économies émergentes possèdent déjà un smartphone, un nombre qui ne cesse d'augmenter. Pour comprendre l'impact potentiel de Bitcoin dans cet espace, il faut savoir que dans un pays comme les Philippines, seul 20% d'adultes ont accès à un compte bancaire.

Pour être utilisé comme un rail de paiement, les détenteurs du bitcoin doivent être en mesure de l'échanger contre la monnaie locale. A présent, il n'est pas encore pratique d'utiliser bitcoin comme outil d'aide humanitaire car il est encore, dans certains endroits, difficile à dépenser pour obtenir des biens et services. Cependant, selon une analyse détaillée des données de marché consacrée au bitcoin et effectuée par Matt Ahlborg, il est de plus en plus facile d'échanger des bitcoins en devises locales dans les pays émergents de l'Asie de l'Est à l'Afrique de l'Ouest.

De plus, lorsque les banques traditionnelles ferment leur portes, le réseau bitcoin, lui, fonctionne sans interruption. Etant donné que son infrastructure mondiale donne accès à un système financier de plus en plus liquide, la possibilité pour le bitcoin de servir d'alternative pour les personnes qui ont besoin d'aide va considérablement augmenter dans le temps.

Il existe déjà des réseaux maillés et des systèmes satellitaires qui permettent d'envoyer et recevoir des bitcoins sans accès à Internet. Des ingénieurs travaillent sur les innovations nécessaires pour rendre une tâche difficile aux gouvernements s'ils tentent d'empêcher aux citoyens d'accéder au bitcoin, une monnaie qu'ils ne sont capables ni de confisquer facilement et moins encore d'augmenter l'offre.

Une société sans cash

L'idée d'une société sans cash est souvent présentée comme très commode. Mais du point de vue des droits humains, elle présente de nouveaux dangers et donne aux gouvernements et banques un pouvoir sans précédent.

L'utilisation du cash est l'une des meilleures façons de protéger la vie privée. Lorsqu'une chose est payée en cash, seuls l'acheteur et le vendeur sont au courant de la transaction. Dans ces conditions, il devient difficile aux gouvernements de tracer les transactions et aux entreprises de suivre les comportements d'achat. Avec le cash, les paiements anonymes sont possibles, un peu comme quand les billets de banque sont introduits dans une boîte à dons de charité.

Malheureusement, l'argent liquide disparaît petit à petit partout dans le monde. Dans des pays comme le Venezuela ou le Somaliland, hyperinflation oblige, les billets de banque sont devenus si inutiles qu'ils doivent être pesés en kilos pour en évaluer la valeur. Pendant ce temps, dans les zones urbaines avancées telles que Stockholm et Shanghai, les résidents font presque tous les paiements de façon électronique. On estime que seulement 8 % de toutes les transactions mondiales sont encore effectuées avec des pièces de monnaie ou des billets de banque. D'ici 2030, le nombre de personnes utilisant le cash dans leur vie quotidienne sera proche de zéro.

Comme nous l'avons vu au premier chapitre, cette perspective peut être effrayante pour les manifestants qui, dans des endroits comme Hong Kong, comptent sur l'argent liquide pour acheter des tickets de transport en commun ou des cartes SIM jetables afin protéger leur vie privée et lutter contre la surveillance. Sans le cash ou son équivalent numérique, coordonner les manifestations politiques tout en assurant sa sécurité personnelle deviendra presque impossible.

En Estonie, le gouvernement est en train de rendre les transports publics gratuits. Cela semble merveilleux mais reste problématique: les passagers ne peuvent obtenir des trajets gratuits qu'en utilisant leur carte d'identité, ce qui permet au gouvernement de suivre leurs déplacements. Si les Estoniens n'ont peut-être pas à avoir peur d'un tel système, les citoyens des pays aux gouvernements autoritaires voisins, comme la Russie ou la Biélorussie, ont de sérieuses raisons de l'être.

Entre-temps, le Parti communiste chinois a le contrôle des systèmes avec plus d'un milliard d'utilisateurs comme Alipay ou WeChat. Les autorités ne se contentent pas d'exercer une surveillance et un contrôle sur l'argent des gens; elles régulent également les actions et les opinions de leurs citoyens par le biais d'un système de crédit social. Avec un tel système, comme celui mis en place en Chine, les citoyens sont cotés non seulement sur leur santé financière, mais aussi sur leurs opinions politiques, leur identité et leur cercle social. Le gouvernement encourage le comportement loyal des citoyens et punit les fauteurs de troubles en les empêchant de voyager à l'étranger, d'avoir accès à une connexion internet rapide, d'envoyer leurs enfants dans des bonnes écoles ou d'obtenir de bons taux d'emprunt. Ces systèmes de crédit social n'en sont encore qu'à leurs débuts, mais ils sont sur le point de donner un contrôle sans précédent au gouvernement chinois et constituent le plus grand projet d'ingénierie sociale de l'histoire de l'humanité.

Des tendances similaires, bien que moins affligeantes, commencent à apparaître même dans les démocraties occidentales, avec les sociétés de cartes de crédit et les commerçants qui vendent les historiques des transactions à des annonceurs pour le profit.

Bitcoin vs Big Brother

Ce que les gens achètent révèle plus que ce qu'ils disent. Les transactions révèlent énormément de choses sur qui sont les gens, ce qu'ils font, où ils vont et quand, ce qu'ils aiment ou n'aiment pas, etc.

Plus les dépenses sont tracées, plus les individus sont susceptibles d'être confrontés à un résultat Orwellien.

Il y a dans les sociétés démocratiques un débat qui émerge au sujet du rôle des sociétés comme Facebook dans l'émission des monnaies privées. Facebook propose d'introduire Libra à des centaines de millions de personnes via les comptes de médias sociaux existants sur WhatsApp, Instagram, ou Messenger. Alors qu'un projet comme Libra pourrait très bien faciliter l'accès aux services financiers à un grand nombre de personnes actuellement non bancarisées, nombreux craignent que Facebook n'enregistre les activités de paiement des utilisateurs, n'influence leur choix ou limite leurs capacités d'effectuer des paiements pour l'expression d'opinions politiques particulières.

Pour arrêter Big Brother, tout le monde doit réduire son empreinte de données. Moins les informations liées à l'identité sont diffusées et partagées entre les entreprises et les gouvernements, plus les individus sont difficiles à surveiller, à manipuler et à contrôler.

Une société sans cash est une société de surveillance. Qu'il s'agisse du modèle WeChat contrôlé par le gouvernement ou du modèle Libra contrôlé par une entreprise, ces derniers peuvent suivre toute l'activité économique pour le profit, l'oppression ou pire.

Et si l'avenir pouvait être différent? Et si le cash pouvait exister sous forme numérique? Bien qu'actuellement les transactions bitcoin ne sont que pseudonymes, il y a beaucoup de travail en cours dans la communauté des développeurs pour apporter plus de vie privée au protocole Bitcoin et à ses utilisateurs. Dans un proche avenir, en achetant quelque chose en ligne, un billet de bus ou de métro, ou en s'abonnant à des magazines politiques ou des podcasts, personne n'aura plus à divulguer son identité au moment de faire le paiement.

Rendre les transactions bitcoin plus confidentielles avec Lightning Network

Les consommateurs perdent de plus en plus leur vie privée. Une solution existe grâce à Lightning, un réseau de paiement en cours de développement sur Bitcoin. Les systèmes de paiement traditionnels ne garantissent aucune confidentialité. Chaque intermédiaire financier constitue une brèche de sécurité potentielle. Bitcoin est différent dans la mesure où il n'y a pas d'intermédiaires de sorte qu'au moins, en principe, cette vulnérabilité pourrait être éliminée. Les détails clés des transactions bitcoin sont malheureusement enregistrés sur sa blockchain, que tout le monde peut consulter. Des chercheurs ont cherché à savoir s'il existe un moyen de masquer ou d'obscurcir les détails spécifiques des transactions bitcoins et cela est possible avec Lightning.

Le Lightning Network est une solution en *Layer 2* qui n'enregistre pas directement les détails de chaque transaction. Son objectif est d'augmenter la capacité du bitcoin à traiter instantanément plus de transactions. L'amélioration de la confidentialité est un effet secondaire à l'objectif principal de Lightning qui vise à rendre Bitcoin plus scalable.

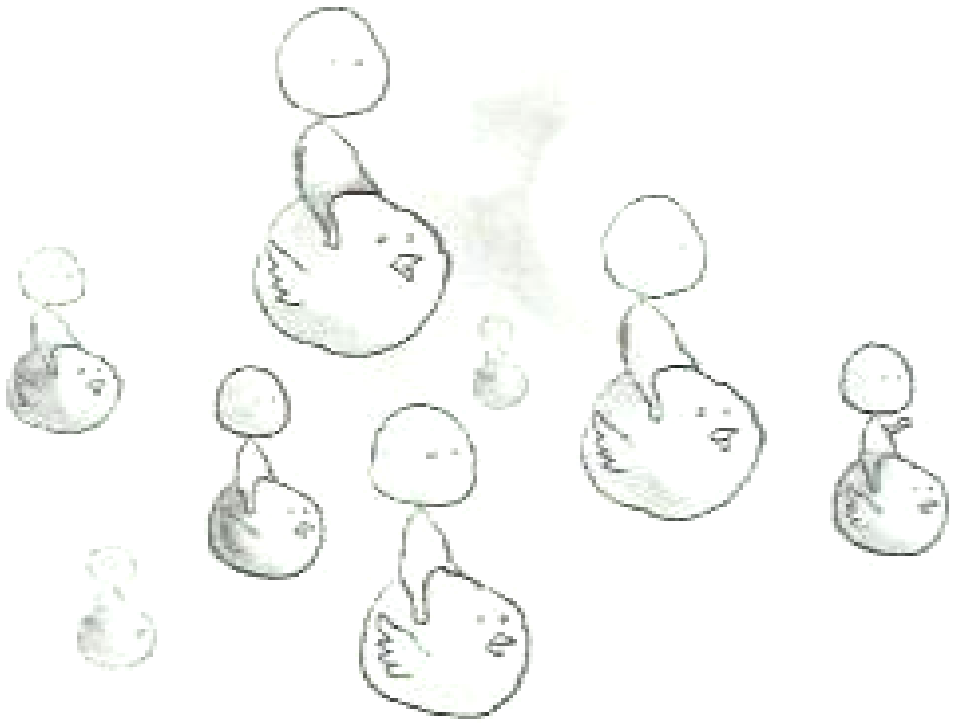
Comme Bitcoin, cette innovation technique est open-source, ne requiert aucune permission et est accessible à tous, quels que soient la localisation, l'âge, le revenu, le genre ou la citoyenneté. Lightning Network pourrait aider à prévenir un avenir dans lequel la confidentialité serait coûteuse et donc uniquement accessible aux plus fortunés.

Même dans une société sans cash, il devrait bientôt être possible d'utiliser Lightning sur un téléphone pour acheter anonymement des billets de transport afin d'assister à une manifestation sans peur d'être pisté ou tout simplement pour acheter des livres politiques en ligne. Avec ce protocole, le distributeur de billets de métro ou Amazon ne saura rien sur l'identité des acheteurs et n'aura aucune possibilité de divulguer leurs données ou les partager avec les gouvernements.

Cela dit, Lightning n'est pas une panacée pour la défense de la vie privée. L'anonymisation des informations de paiement n'est qu'une étape vers une confidentialité totale car les lacunes de confidentialité telles que les portes dérobées sur les téléphones, le pistage par géolocalisation et les caméras de surveillance devraient également être supprimées.

Nassim Taleb, *l'auteur de Black Swan*, a parlé de bitcoin comme «une police d'assurance contre un avenir Orwellien». Alors que la surveillance et la disparition du cash sont devenues une tendance mondiale, ce sombre avenir semble se presser sur nous.

La technologie n'améliore pas toujours la liberté dans le monde. Au contraire, l'intelligence artificielle et l'analyse du big data privent systématiquement les individus de leurs libertés, en particulier dans des pays comme la Chine. L'historien et auteur de S*apiens*, Yuval Noah Harari, a averti que la technologie de l'information moderne tend à favoriser la tyrannie, mais que cette même technologie peut être utile pour la liberté lorsqu'elle est délibérément conçue dans ce but. Bitcoin, lorsqu'il est amélioré grâce aux protocoles comme Lightning Network, peut devenir un outil important dans la lutte universelle pour les droits humains.



CHAPITRE 5

Un récit de deux futurs

Nous sommes en 2039

Les 20 dernières années ont vu les guerres se multiplier partout dans le monde. Les pays se battent pour détrôner le dollar américain et le renminbi chinois de leurs positions dominantes. Parfois, ces turbulences dégénèrent en conflits très violents. Les pays riches souffrent d'un déclin politique et d'une récession économique insoluble. Pendant ce temps, les pays pauvres sont proches de l'effondrement total alors que les crises économiques consécutives consolident la richesse et le pouvoir de l'État et des entreprises.

Les géants de la tech tels que Alibaba, Tencent, Facebook, Google et Amazon contrôlent le marché mondial mais aussi, après plusieurs séries de pressions gouvernementales et de procès antitrust , ils ont accepté de transmettre les données des utilisateurs en échange d'une protection du marché. Les entreprises partagent avec les gouvernements du monde entier des informations complètes sur ce que tout le monde achète, écoute, publie et même les données de localisation. Elles sont devenues des satellites de l'État. La vie privée n’existe plus.

Cette situation donne aux gouvernements un contrôle sans précédent sur leurs citoyens. Le fossé entre les riches et les pauvres continue de se creuser à mesure que l'effet Cantillon s'amplifie. Ceux qui ont des liens avec le régime prospèrent de manière disproportionnée. La surveillance numérique est devenue la norme; la critique des gouvernements autoritaires se fait de plus en plus rare. Le contrôle de la monnaie par le gouvernement et les entreprises donne à ces derniers le pouvoir de censurer la parole car les créateurs de contenu dissidents ne peuvent plus être payés ou soutenus pour bien faire leur travail.

Penser différemment est désormais synonyme de dissidence. Les policiers à travers le monde utilisent l'internet des objets (IoT), les données relatives aux implants médicaux, le pistage téléphonique, l'historique des transactions et les requêtes de recherche pour localiser et punir les dissidents. L'opposition est pratiquement impossible car le cash a disparu et tous les achats (y compris pour les tickets de métro, les journaux et les masques qui pourraient dissimuler l'identité d'une personne) sont

numériques et régulièrement monitorés par les autorités. L'État et les multinationales sont devenus plus puissants que jamais.

Nous sommes en 2039

Une économie mondiale dynamique continue de prospérer. De plus en plus de personnes dans le monde épargnent, accumulent des richesses, sont en mesure de se payer un logement et créent de nouvelles entreprises. Les entrepreneurs de ce que l'on appelait autrefois les pays du tiers-monde sont devenus le moteur de l'innovation dans l'économie mondiale. Il est plus facile que jamais de changer de juridiction. Les gouvernements sont en concurrence car les citoyens choisissent le meilleur endroit où vivre, travailler et payer leurs taxes. Les impôts sur les revenus ont diminué alors que la qualité des infrastructures, des services et l'enseignement augmente en raison d'une concurrence entre les pays.

La prolifération de nouveaux produits et services fournis par un nombre croissant de petites entreprises a entraîné plus d'innovation qu'on ne l'aurait cru possible. Plusieurs multinationales qui dominaient le marché ont été detrônés par des nombreux petits acteurs. Actuellement, tout le monde peut payer n'importe quel produit anonymement et sans besoin d'une quelconque autorisation.

La plupart des régimes autoritaires ont été renversés ou affaiblis à mesure que les citoyens deviennent plus aptes à contourner le contrôle draconien de capitaux et à préserver individuellement leur richesses au lieu de la confier aux élites. Les gouvernements ont été contraints de passer du contrôle à la concurrence; les individus sont plus libres que jamais.

À quoi ressemblerait un monde plus basé sur Bitcoin?

Il a toujours été risqué de prédire l'avenir. Ce sont deux visions alternatives vu la trajectoire que prend le monde actuel. Ni l'un ni l'autre n'est susceptible de se matérialiser, mais les individus ont le plein contrôle sur la direction que prendra leur société.

Le système monétaire se situe au centre du carrefour. Bitcoin a le potentiel de séparer l'argent et l'État. Il vaut la peine de se demander comment l'adoption mondiale de celui-ci pourrait-elle changer la société?

L’émergence d’une économie sans frontières

Depuis le 20e siècle, l’économie est largement contrôlée par les États-nations. La transition vers la monnaie numérique a permis aux gouvernements d’exercer un contrôle sans précédent sur l'économie, notamment par l’augmentation de la masse monétaire pour financer leurs initiatives.

Par ailleurs, à mesure que l'ère numérique progresse, les économies ont commencé à transgresser les États. Au début du 21e siècle, cela était évident puisque les consommateurs commençaient à acheter des biens produits à l'autre bout du monde. Des entreprises ont embauché les pigistes des Philippines au Nigéria en tant que développeurs de logiciels, assistants virtuels ou même radiologues à distance. Les partenaires commerciaux pouvaient être séparés par des milliers de kilomètres. La communication est devenue numérique et instantanée.

Cependant, effectuer des paiements transfrontaliers était encore lent et coûteux. Le paiement des biens en ligne reposait toujours sur les canaux traditionnels, et le règlement en dollars entre institutions financières prenait encore plusieurs jours. Le système monétaire ne s'était pas encore adapté à un monde de plus en plus connecté.

L'émergence du Bitcoin est l'étincelle qui lancera la prochaine vague d'évolution dans l’univers de la finance.

Les biens d’origine numérique, tels que le contenu des réseaux sociaux et les jeux vidéo représenteront une part très importante de l'économie. Bitcoin sera de plus en plus utilisé comme moyen de paiement dans les transactions transfrontalières car la monnaie fiat deviendra de plus en plus encombrante. Les micro transactions en bitcoin, leur validation rapide et la base d'utilisateurs croissante obligeront les commerçants à libeller les prix en bitcoin.

Les économies autour du bitcoin sont de petite taille aujourd'hui, un peu comme les communautés qui discutaient sur AOL dans les années 1990 - mais à mesure qu'elles se développent, elles érodent davantage le contrôle des États sur l’économie. Au fur et à mesure que la richesse provient de réseaux sans frontières et est libellée dans une monnaie sans frontières détenue par des particuliers, elle deviendra plus facile à déplacer et s’affranchira de l'économie physique d'un seul État-nation.

Les gouvernements face au vrai prix de la guerre

Lorsque le bitcoin deviendra omniprésent, la capacité de l'État à imprimer plus d'argent pour financer la guerre sera beaucoup plus limitée. Les guerres ne seront plus financées aussi facilement qu'elles l'ont été au cours des cent dernières années. Si des guerres surviennent, elles seront plus limitées et moins longues.

Des conflits prolongés comme l'intervention russe en Syrie et en Ukraine ou l'occupation américaine de l'Irak et l'Afghanistan pourraient alors appartenir au passé car de telles opérations ne seront plus faciles à financer. La guerre entre les États deviendra, encore plus, une option de dernier recours qu'elle ne l'est aujourd'hui. Les gouvernements seront beaucoup plus incités à trouver des moyens moins coûteux pour mettre fin aux conflits.

L'autoritarisme va coûter plus cher

Les États autoritaires auront du mal à se positionner dans un environnement plus difficile à contrôler. Avec des particuliers au contrôle du transfert d'argent, les citoyens les plus productifs de tous les pays se déplaceront plus simplement, avec leur richesse, dans les juridictions concurrentes si les conditions locales ne sont pas acceptables. Pour ne pas laisser ces citoyens productifs s'échapper, les gouvernements devront appliquer des contrôles sévères aux frontières ou abdiquer en leur donnant une voix dans la gouvernance.

Les dictatures ne disparaîtront pas tranquillement, mais elles seront contraintes à un choix: faire face à une fuite massive de capitaux ou accorder plus de liberté aux citoyens. Grâce aux réseaux d'information, les œuvres libérales (de littérature et de cinéma) parviennent plus facilement aux personnes vivant sous les régimes les plus tyranniques comme l'Érythrée et la Corée du Nord. Ce phénomène sera accéléré par une monnaie facile à transférer et à sécuriser au même titre qu'une information numérique.

Les actifs deviendront correctement évalués

Bitcoin est une réserve de valeur accessible à tous, quel que soit leur statut social, leur appartenance ethnique ou leur emplacement géographique. En réaction à l'inflation de la monnaie fiduciaire, plusieurs personnes choisissent de stocker une partie de leurs avoirs dans l'immobilier, les actions et les métaux précieux, qui sont tous plus centralisés et donc plus difficiles d'accès que bitcoin. Dans un monde où conserver la richesse en bitcoin est la norme, les bulles spéculatives dans ces actifs ne seront plus aussi répandues.

Par exemple, il y aura moins de cas de bulles immobilières induites par l'inflation car les étrangers seront moins nombreux à acheter plusieurs logements dans une ville sans la moindre intention d'y vivre. Avec bitcoin comme principale alternative, il ne sera plus attrayant d'acheter des actifs stables à l'étranger. Les prix ne monteront plus en flèche et beaucoup plus de personnes auront la possibilité de se payer un logement dans leur propre ville.

La finance décentralisée arrive

La domination américaine, européenne et chinoise disparaîtra à mesure que les pays régleront leurs transactions en bitcoin, une réelle monnaie de réserve mondiale à la place de monnaies régionales comme l'USD, l'EUR ou le CNY. Le fait pour la main d'œuvre d'être libre de se mouvoir entraînera plus de concurrence. Cela va donner plus de valeur aux travailleurs.

Alors que chaque individu saura comment devenir sa propre banque, les banques américaines, européennes et chinoises perdront leur influence oppressive. Ce phénomène permettra aux particuliers d'épargner d'une manière plus sûre au fil du temps. La richesse va s'accumuler dans les pays exportateurs de main-d'œuvre, les entreprises nationales auront plus de chances de se développer tout en construisant des infrastructures innovantes.

Les grandes banques auront moins de pouvoir

Les banques, qui sont devenues des gros poissons grâce à des relations privilégiées avec les gouvernements et du contrôle qu'elles exercent sur l'argent de populations vont soit faire faillite, soit devenir beaucoup plus petites. Le principe "too big to fail" ne sera plus la norme. Et les banques et les grandes entreprises ne vont plus compter sur les renflouements gouvernementaux chaque fois qu'elles commettent des erreurs, comme lors de la crise financière de 2008.

Sans ces avantages, les banques et les multinationales devront se concentrer sur la fourniture de services à leurs clients, plutôt que de solliciter les subventions auprès des gouvernements. Les petites banques et entreprises seront à mesure, grâce à la nature sans frontières de transactions en bitcoin, de servir les clients dans le monde entier, une énorme opportunité pour détrôner les géants ossifiés par le passé.

Déclin de Big Brother et du capitalisme de surveillance

Aujourd'hui, les informations de paiement sont à la fois exploitées par les entreprises à la recherche du profit et utilisées par les gouvernements pour espionner les individus. Internet s'étant développé comme un marché ouvert par défaut, les normes de confidentialité ont mis du temps à protéger les informations de plus en plus personnelles et importantes qui affluent sur la toile. En conséquence, les données personnelles sont constamment reconditionnées, analysées et utilisées à l'insu et sans aucune autorisation des internautes.

Avec l'avènement et l'adoption des paiements Lightning en plus du bitcoin, la plupart des petits achats quotidiens seront déconnectés de l'identité. Lors d'un achat en ligne, de l'abonnement à un magazine politique, d'un don à une organisation de la société civile ou du paiement d'un médicament, personne d'autre que le consommateur ne connaîtra tous les détails de la transaction. Il n'y aura aucun processeur de paiement pour divulguer des informations car les transactions sont pair à pair, le commerçant ne voyant que le paiement. En l'absence d'informations d'identification dans cet environnement, il sera beaucoup plus difficile pour les systèmes de surveillance de suivre le comportement des consommateurs ou de prédire leurs actions.

Le début de la souveraineté individuelle

Bitcoin est un phénomène similaire, dans son impact potentiel, à la démocratie et à Internet: deux évolutions qui ont respectivement renversé la tyrannie du pouvoir politique et le contrôle des entreprises sur la pensée. Grâce à la démocratie, les citoyens contrôlent collectivement le pouvoir du gouvernement et à travers Internet, les citoyens moyens ont une voix plus forte et un accès plus libre à la connaissance.

Dans le même ordre d'idées, bitcoin va briser le monopole monétaire dont jouissent les États et les entreprises. Dans un siècle, les individus se souviendront de 2019 comme une époque dépassée, où les quelques privilégiés avaient une main sur l'ensemble de l'économie. Ce sera l'équivalent d'étudier le système féodal monarchique ou la propagande d'État. Cette évolution va se dérouler en trois phases à mesure que le bitcoin deviendra la monnaie mondiale.

Phase 1: Réserve de valeur

Bitcoin sera premièrement adopté en tant que réserve de valeur. A ce stade , les épargnants du monde entier vont chercher à se protéger contre l'inflation causée par leurs gouvernements. Aujourd'hui, cela se produit non seulement dans les économies touchées par l'hyperinflation comme celles du Venezuela et du Zimbabwe, mais également dans des endroits plus stables comme les États-Unis et l'Europe où bitcoin a, sur plusieurs années, surperformé les monnaies fiduciaires locales. Vers la fin de cette phase, les fonds de pension et les institutions financières traditionnelles commenceront à ajouter du bitcoin à leurs portefeuilles, et plus tard, ce sont les gouvernements qui vont commencer à ajouter du bitcoin à leurs réserves.

L'adoption au cours de cette phase se développera plus lentement et de manière organique à mesure que les gens prendront conscience des avantages du bitcoin.

Phase 2: Moyen de paiement

Lorsque suffisamment de commerçants se rendront compte que toute monnaie en dehors du bitcoin est une réserve de valeur inférieure, ils voudront être payés en bitcoin. Cela sera similaire à ce qui se passe au marché noir au Vénézuela.

En effet, les marchands refusent les bolivars pour être payés en dollars américain. À mesure que plus de commerçants, d'entrepreneurs et d'employés vont préférer bitcoin, sa demande augmentera de la même manière que l'explosion de celle du dollar américain à la suite de l'introduction du système de convertibilité de l'USD en or de Bretton Woods.

Au début, cela ne se produira pas dans des économies développées comme les États-Unis; ça va se produire dans celles brisées par une inflation galopante et la corruption. Ces pays seront probablement gouvernés par des régimes oppressifs qui réduisent l'utilité des réserves de valeur faciles à confisquer comme les billets de dollars et l'or. Les gens dans de tels endroits vont utiliser bitcoin pour s'opposer à la saisie de leur richesse et, si nécessaire, pour s'enfuir complètement.

Dans cette phase, des logiciels bien conçus, des technologies de règlement plus rapide, une infrastructure améliorée et des innovations en matière de vie privée seront mis en avant. Les utilisateurs de Bitcoin pourront effectuer des transactions instantanées et privées, ce qui rendra l'espionnage beaucoup plus difficile.

Phase 3: Unité de compte

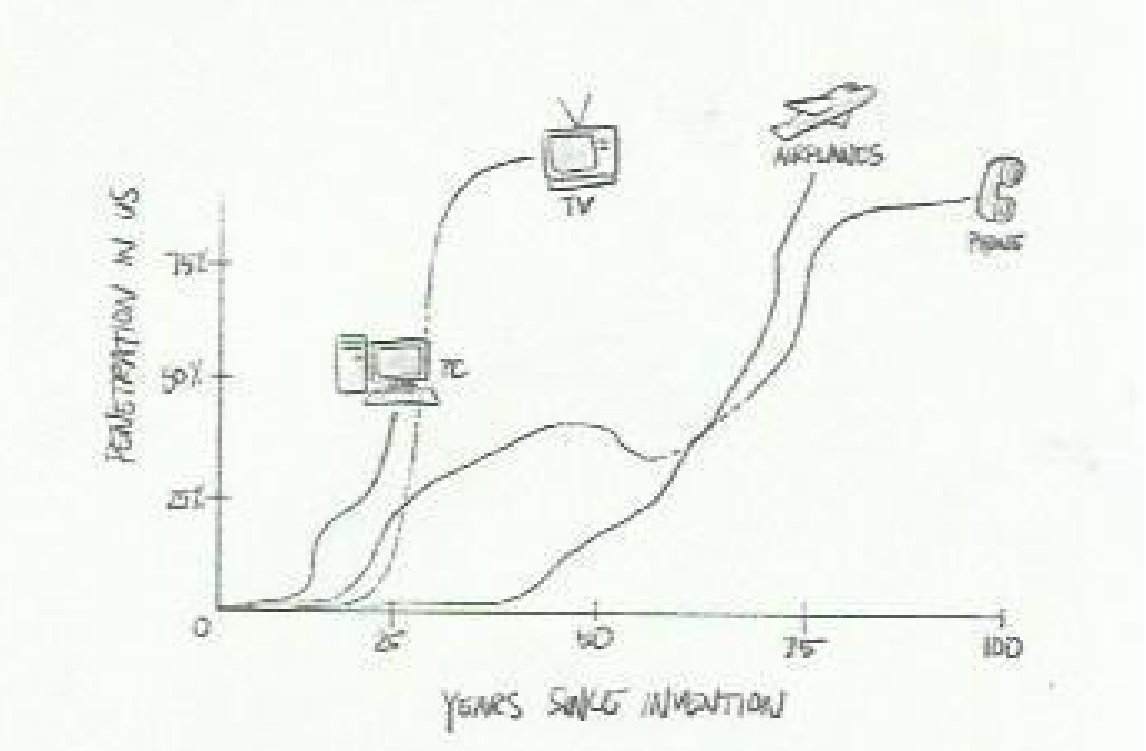
Quand plus de gens seront en possession de plus de bitcoins que leur monnaies locales, les prix absolus des biens et services seront évalués en bitcoin à la place des monnaies locales ou du dollars américain. À ce stade, il y aura des opportunités d'arbitrage très lucratives. Contracter un prêt dans les devises qui se déprécient rapidement suite à l'inflation et les convertir en bitcoin deviendra très rentable.

Ce sera le début de l'hyperbitcoinisation, une période où l'USD et le CNY perdront leurs positions privilégiées laissant la place au bitcoin qui deviendra la monnaie de règlement mondiale. Cela va, à son tour, provoquer une hyperinflation de la plupart d'autres devises car les prêts seront très coûteux pour prévenir l'arbitrage. Avec bitcoin comme réserve de valeur par excellence, il y aura une dépréciation substantielle de nombreuses autres devises.

Il est encore tôt

La plupart des technologies qui transforment le monde sont d'abord rejetées par la masse. Pensez à l'électricité qui a été considérée comme très dangereuse; au téléphone, que personne ne voulait acheter; à la voiture, qui ne pouvait sûrement pas fonctionner sur des routes pavées; à l'avion, qui ne pouvait pas être sûr; aux micro-ondes, qui suppriment supposément toute valeur nutritive des aliments; au téléphone portable, qui aurait causé le cancer; ou à Internet, qui était voué à l'échec. Rappelez-vous des propos de Paul Krugman, le chroniqueur du New York Times, qui écrivait en 1998 que "d'ici 2005, il deviendra clair que l'impact d'Internet sur l'économie n'a pas été plus grand que le fax".

Toute technologie fondamentale, du réfrigérateur à la carte de crédit, suit une courbe d'adoption et fait face à beaucoup de scepticisme au début. Un jour ou l'autre, la courbe progresse de façon exponentielle, prenant la forme d'un S, et la technologie se propage. Il est difficile d'imaginer une idée plus juste ou démocratique que le fait pour n'importe qui aujourd'hui - quel que soit son lieu de vie, son sexe, sa langue, son âge, son niveau d'éducation ou sa richesse - puisse s'impliquer de manière significative dans le devéloppement de Bitcoin, une technologie innovante qui est encore au plus bas de sa courbe d'adoption.



Bitcoin est actuellement loin de ce qu'il doit devenir en termes de facilité d'utilisation, de scalabilité, de prise de conscience du public et d'intérêt commercial. Il n'y a pas assez d'entreprises qui se construisent autour de Bitcoin; pas assez d'étudiants qui s'y concentrent; pas assez d'enseignants; pas assez de marchands l'acceptant comme moyen de paiement; pas assez de fondations philanthropiques pour soutenir son développement et pas assez d'autorités publiques qui prennent au sérieux sa capacité de contribuer à la protection vie privée. Il est nécessaire d'accroître l'intérêt, l'engagement et la pensée critique dans le secteur.

Moins de 1% de la population mondiale a déjà possédé des bitcoins. Si le temps et les ressources nécessaires sont investis dans le développement des portefeuilles faciles à utiliser, des plateformes d'échanges et des supports éducatifs, Bitcoin a le potentiel de faire une réelle différence pour des milliards de personnes dans le monde. Bitcoin peut aider n'importe qui d'obtenir plus de liberté financière, mais il aidera probablement en premier lieu ceux qui en ont le plus besoin.

Les populations au Nigeria, en Turquie, aux Philippines, au Venezuela, en Iran, en Chine, en Russie ou au Palestine n'ont pas les mêmes libertés, la même protection des droits humains ni la même confiance dans leur système financier comme ceux de l'occident. Pour eux, bitcoin est un moyen pratique pour se mettre à l'abri ou même d'échapper aux pouvoirs autoritaires.

La désobéissance, le silence et l'exil sont des nouvelles formes de protestation. Pour changer les choses, un individu n'a pas besoin de se coordonner avec des milliers de personnes partageant les mêmes idées pour inonder les rues pendant un jour ou une semaine. Ces personnes peuvent exporter leurs richesses aussi facilement qu'elles peuvent envoyer un e-mail. Les protestations peuvent désormais se produire à partir d'une personne. Au début, l'adoption sera comme un filet d'eau, puis un ruisseau et finalement une inondation.

Le futur est entre vos mains

Bitcoin est une invention si profonde qu'il offre des nouvelles alternatives à de nombreux problèmes du système monétaire et économique actuel. Les inégalités, les monopoles des certaines multinationales et l'autoritarisme sont en partie alimentés par le contrôle de la monnaie par l'État. A mesure que le monde découvre Bitcoin et la façon dont il rend possible la souveraineté individuel, le pouvoir va se décentraliser de manière significative partout dans le monde.

A la place de régimes autoritaires, les gouvernements seront contraints de tendre vers le respect de la dignité humaine, de la valeur et du talent. A la place des multinationales déconnectées, il y aura des entreprises plus petites dont le seul but sera de rendre service aux clients. Bien qu'il ne soit pas possible d'atteindre les mêmes résultats, Bitcoin va uniformiser les règles du jeu en permettant aux gens de mieux conserver la valeur qu'ils créent.

Quoi de plus juste que l'idée que tout ce qu'il faut pour participer à la prochaine révolution financière soit l'accès à un smartphone bon marché et à Internet? Aucune banque, aucun régulateur, aucune autorisation n'est requise pour faire partie de ce futur. En reprenant le contrôle de la richesse des caprices de ceux qui la contrôlent, chaque individu sera plus libre de façonner son destin.

Bitcoin rend l'humain plus libre d'une manière que l'on n'aurait jamais cru possible au début du 21e siècle.

Faites circuler ce livre pour contribuer à faire passer ce message.

Questions et Réponses sur Bitcoin

Au cours des dernières années, les débutants et les sceptiques ont posé plusieurs questions sur le Bitcoin. Cette partie du livre tente de répondre aux plus importantes et fréquentes, en abordant certains mythes, défis, inconvénients et confusions courantes autour du Bitcoin. Cette section n'est en aucun cas exhaustive; elle vise à fournir suffisamment d'informations fondamentales pour assurer un bon départ tout esprit curieux.

Qui est Satoshi Nakamoto?

Satoshi Nakamoto est le créateur anonyme du Bitcoin.

Au cours des deux premières années de l'histoire du Bitcoin, Satoshi Nakamoto était un membre actif de la communauté. Il a fréquemment posté en ligne des réflexions à propos de la technologie Bitcoin et son impact social tout en contribuant à son développement technique. Fin 2010, Satoshi a disparu.

Satoshi possède probablement des centaines de millions de dollars en bitcoins et tout le monde peut le voir sur la blockchain. Ses pièces n'ont jamais bougé, ce qui laisse penser que la disparition du père du bitcoin pourrait être permanente. Au moment de la rédaction de ces lignes, l'identité de Satoshi n'a jamais été révélée, ce qui a fait de cette histoire l'un des plus grands mystères du 21ème siècle .

Qui contrôle Bitcoin?

Il n'y aucune autorité centrale chargée du Bitcoin. Il n'y a ni PDG, ni conseil d'administration, ni société de contrôle. L'un des attributs les plus forts du Bitcoin c'est le fait que son créateur n'est plus impliqué dans le projet.

Il existe des milliers de validateurs de transactions partout dans le monde. Ces derniers vérifient la blockchain et stockent l'historique complet des transactions en bitcoin. Ils sont appelés *nœuds complets*.

Comme indiqué au chapitre 2, les mineurs du monde entier se font concurrence pour produire des blocs. La validité de ces blocs est vérifiée par les nœuds complets. Le logiciel utilisé pour exécuter ces nœuds est écrit par des développeurs Bitcoin. Et bien entendu, les transactions au sein de ces blocs sont initiées par les utilisateurs à partir des plateformes d'échanges, portefeuilles et processeurs de paiement. Tous ces participants sont essentiels au fonctionnement du réseau mais aucun d'entre eux ne le contrôle.

Si un développeur décide de créer un logiciel de nœud complet radicalement différent, peu de personnes vont l'utiliser. Si un mineur tente d'introduire frauduleusement un nouveau bloc de transactions qui ne répond pas aux exigences de validation, les nœuds complets rejetteront ce bloc. Si les mineurs tentent un coup d'État pour imposer des nouvelles fonctionnalités sur le réseau, ils échoueront car ils ne peuvent imposer aux utilisateurs l'utilisation des logiciels qu'ils ne veulent pas exécuter.

Ainsi, tout changement sur Bitcoin nécessite un consensus. En ce sens, son modèle de gouvernance est similaire à une démocratie, avec des pouvoirs et des contre-pouvoirs. Les mineurs sont comme la branche exécutive du gouvernement, gérant les opérations et appliquant les règles; les développeurs comme le pouvoir législatif, élaborant et adoptant de nouvelles lois et les utilisateurs sont la branche judiciaire, ils s'assurent que les deux autres branches ne font rien d'inconstitutionnel.

Bitcoin n'est-il pas trop volatil?

Bitcoin a connu une énorme volatilité depuis sa création en 2009. Vu sur une période plus longue, il s'est considérablement apprécié, passant de moins de 0.001$ à plus de 11 000 $ au moment de la rédaction de ce bouquin. Comme expliqué au chapitre 3, plusieurs facteurs ont poussé son prix (à long terme) à la hausse et continueront probablement de le faire.

Dès sa création, Satoshi Nakamoto a défini la politique monétaire du bitcoin. Aucune personne ou groupe ne peut décider de créer plus de bitcoins ou de modifier son plan d'émission car les nœuds complets rejetteront un tel changement.

En conséquence, bitcoin sera plus vulnérable aux manipulations de marché car il ne dispose d'aucun mécanisme de correction de la banque centrale. Une banque centrale a le pouvoir d'imprimer une nouvelle masse monétaire ou de racheter la plus

grande partie de celle en circulation afin de maintenir la stabilité des prix. Étant une monnaie décentralisée et non régulée, bitcoin continuera d'être volatil à mesure que sa demande va augmenter dans le monde.

La réalité économique est la suivante: les monnaies doivent choisir entre une stabilité à court terme (qui passe par la centralisation) ou le potentiel d'appréciation des cours à long terme (qui passe par la décentralisation). Satoshi Nakamoto a choisi la décentralisation.

Plus important encore, la volatilité du bitcoin ne l'a pas empêché d'avoir une valeur réelle en tant qu'actif refuge pour les personnes coincées dans des systèmes financiers défaillants. Les cas d'usages du bitcoin incluent la protection contre les sanctions économiques, l'hyperinflation, le contrôle des capitaux et la surveillance. Pour l'instant, la volatilité quotidienne est un compromis que les détenteurs des bitcoins ont été prêts à payer.

Qu'est-ce qui soutient la valeur actuelle du bitcoin?

La réponse courte est que les gens soutiennent bitcoin. Assez d'investisseurs l'achètent, cela lui donne de la valeur. Vous pouvez vous référer au chapitre 3 pour une explication détaillée de ce qui donne au bitcoin un prix historiquement haussier. Il existe une demande mondiale pour le bitcoin en tant qu'actif rare, utile et ayant un usage technologique qu'aucun autre outil financier ne peut avoir.

Comment faire confiance au bitcoin?

Le monde moderne regorge des systèmes complexes dont peu de gens comprennent le fonctionnement, mais leur font confiance. Les soins de santé sont fournis aux personnes qui ne comprennent pas la médecine, les prévisions météorologiques publiées pour les non-météorologues, les ordinateurs portables utilisés par des personnes qui ne sont pas ingénieurs et les voyageurs n'ont pas besoin de comprendre l'aérodynamique pour prendre l'avion.

Les normes pour accorder la confiance aux nouveaux systèmes monétaires devraient être plus strictes car il y a fréquemment d'abus de cette confiance, dont plusieurs sont documentés dans ce livre. Mais en fin de compte, une expertise en la matière ne sera pas nécessaire pour utiliser ou faire confiance au bitcoin. A terme, envoyer et recevoir des bitcoins sera aussi simple que l'envoi ou la réception d'un e-mail. Pour l'instant, les personnes intéressées par bitcoin doivent absolument faire leurs propres recherches. De nombreuses bonnes sources d'informations sont répertoriées au niveau de ressources supplémentaires vers la fin de ce bouquin, notamment le code source de Bitcoin Core, d'autres livres, des sites Web et des podcasts.

Bitcoin est-il fiable ?

Lorsqu'il est utilisé correctement, bitcoin est beaucoup plus sûr, plus robuste et protège mieux la vie privée que tout processeur de paiement centralisé. MasterCard et Visa, par exemple, tombent en panne de temps en temps. Bitcoin, lui, a été opérationnel pendant 99,98% de son histoire depuis son lancement en janvier 2009.

Mais aussi, les sociétés de cartes de crédit vendent régulièrement les informations des utilisateurs et se font souvent pirater. N'étant contrôlé par personne, Bitcoin ne peut vendre aucune information sur ses utilisateurs. Contrairement aux processeurs de paiement et à de nombreuses banques, Bitcoin n'a pas été piraté depuis que son prix a dépassé 0,10 USD en 2010. Personne n'a jamais volé un seul bitcoin sur le réseau. Son track record est juste remarquable.

Pourquoi plusieurs plateformes d'échange ont été piratées?

Les crypto-bourses ou exchanges sont très populaires, à la fois en tant que places de marché permettant aux investisseurs d'acheter leurs premiers bitcoins mais également, en tant que plateformes facilitant la spéculation sur le cours du bitcoin contre la monnaie fiduciaire ou d'autres crypto-monnaies. En conséquence, les bourses détiennent, au nom de leurs clients, de grandes quantités de bitcoins et de monnaies fiat. Cela en a fait des cibles privilégiées pour les pirates informatiques. Les plateformes d'échange gardent également les copies des identifiants personnels, des passeports et

des adresses personnelles de leurs clients dans le cadre de leurs procédures KYC («Know Your Customer»).

Les attaques peuvent se produire à la fois en interne et en externe. Les attaques internes proviennent parfois des employés ayant un accès privilégié aux systèmes des plateformes et qui se servent de cette position pour voler les fonds des clients. Les attaques externes sont menées par des pirates. Ces derniers utilisent passent par la vulnérabilité d'un logiciel, une faible sécurité opérationnelle ou une ingénierie sociale pour dérober les bitcoins des coffres des plateformes.

De nombreux exchanges ont été attaqués que ce soit en interne ou par une opération coordonnée de l'extérieur. Parmi les tristes exemples on peut citer Mt.Gox au Japon, Bitfinex à Hong Kong, Bitstamp dans l'Union Européenne et plus récemment Quadriga au Canada. Chaque pirartage a abouti à des millions de dollars en bitcoins perdus. Ces hacks constituent un avertissement fort pour les utilisateurs qui permettent à des entités tierces de garder leurs bitcoins en leur place. Les clients qui négocient en bourse peuvent retirer leurs bitcoins périodiquement des plateformes vers les portefeuilles personnels afin d'éviter toute perte potentielle due au piratage.

Bitcoin est-il utilisé par les criminels pour le blanchiment d'argent?

Oui. Les criminels ont utilisé le bitcoin pour le blanchiment d'argent et les activités illégales et continueront de le faire. Le cas le plus connu est celui de Silk Road, un marché sur le darknet où bitcoin était utilisé pour acheter et vendre des drogues considérées comme illégales aux États-Unis.

Bitcoin étant une technologie sans permission, tout le monde peut l'utiliser comme le téléphone mobile ou Internet. Rares sont ceux qui remettent en question la légitimité de ces technologies omniprésentes aujourd'hui ou appellent à leur interdiction parce qu'ils sont utilisés par des acteurs malveillants. De nombreuses personnes adressent un scepticisme hostile à l'égard des nouvelles technologies dès leur naissance.

Quoi qu'il en soit, la majorité de la criminalité financière dans le monde d'aujourd'hui est facilitée par le système financier traditionnel, par l'intermédiaire de banques et de sociétés de transfert de fonds réglementées. La plupart des fraudes sont commises par les gouvernements et les multinationales, et non par des individus voyous. Les gouvernements démocratiques ont mis en place des règles anti-blanchiment (AML) pour faire pression sur les banques afin qu'elles bloquent

certaines transactions. Pourtant, plus de 1000 milliards de dollars continuent d'être blanchis par le système bancaire chaque année. Pour ne citer qu'un exemple, des rapports ont récemment révélé qu'un seul bureau de Danske Bank au Danemark avait blanchi pas moins de 230 milliards de dollars, soit plus que la valeur marchande de tous les bitcoins en circulation au moment de la rédaction de ce bouquin.

Ainsi, bien que certains criminels aient utilisé bitcoin, la plupart d'entre eux préfèrent passer par la monnaie fiduciaire pour faire tourner leurs activités illicites.

Bitcoin est-il une pyramide de Ponzi?

Une pyramide ou un schéma de ponzi promet aux investisseurs des bénéfices importants avec très peu de risques. Ces genres de systèmes obtiennent ces rendements pour leurs premiers investisseurs en les payant avec l'argent collecté auprès des derniers investisseurs. Il n'y a pas de véritable mécanisme de rentabilité, si ce n'est d'essayer d'attirer le plus grand nombre possible de nouveaux investisseurs afin de rembourser ceux qui les ont précédés. Ces systèmes s'effondrent lorsqu'il n'y a plus de nouveaux investisseurs.

Bitcoin n'est pas une pyramide de Ponzi. Derrière bitcoin, il n'y a aucun groupe qui essaie d'attirer des nouveaux acheteurs pour rembourser les anciens. Cependant, les personnes qui orchestrent les stratagèmes de ponzi peuvent accepter bitcoin comme moyen de paiement de la même manière qu'elles le font avec toutes les autres formes de monnaies.

Bitcoin est-il une bulle?

Une bulle se produit quand des investisseurs spéculateurs achètent en masse un actif à un prix bien au-delà de ce que justifie sa valeur fondamentale. Les bulles éclatent toujours dès que la confiance en l'actif derrière se perd et quand plus personne n'est prêt à l'acheter au prix demandé. Parmi les exemples historiques on peut citer les tulipes hollandaises dans les années 1500, la South Sea Company dans les années 1700 et les actions Dotcom au début des années 2000.

Le chapitre 3 a décrit certains des principaux moteurs de la volatilité des prix du bitcoin. En raison de la volatilité naturelle d'un actif qui a une politique monétaire rigide, de chocs d'offre réguliers, de l'instabilité et de l'effondrement d'autres crypto-monnaies, de la manipulation du marché et du trading à effet de levier , il y a eu plusieurs pics de prix qui ont été suivis de crashs importants. C'est une tendance qui va probablement se poursuivre.

Si l'on considère sa valeur sur le long terme et la nature décentralisée du bitcoin, sa valeur devrait naturellement augmenter à mesure que plus de personnes l'adoptent. Contrairement aux tulipes ou aux actions Dotcom, la valeur du bitcoin s'est rétablie à plusieurs reprises et a suivi une tendance à la hausse après chaque krach majeur.

Qu'est-ce que Tether et comment affecte-t-il bitcoin ?

Tether, ou USDT, est une cryptomonnaie censée être indexée sur le dollar américain. Pour y parvenir, la société à l'origine du projet a promis d'adosser chaque USDT en circulation à un dollar américain détenu sur son compte bancaire. Cela a facilité la spéculation sur les crypto-monnaies car la plupart de personnes réfléchissent encore en fiat. Le fait d'avoir l'USDT a permis à n'importe qui sur les plateformes d'échange crypto-crypto de négocier activement bitcoin contre le dollar américain.

Cependant, en avril 2019, le conseiller général de Tether a révélé que la société ne disposait que des dollars américains ne pouvant soutenir que 74 % des USDT en circulation. Si l'ancrage du dollar de Tether se brise, l'effondrement de son prix peut entraîner une volatilité du bitcoin à court terme. Par ailleurs, il existe un certain nombre de concurrents à Tether qui sont bien placés pour remplir son rôle.

Les gouvernements peuvent-ils interdire ou arrêter bitcoin ?

Puisqu'il n'y a aucune entreprise, aucun ensemble de serveurs centralisés et aucune équipe unique derrière Bitcoin, il n'existe aucun moyen pratique pour arrêter son réseau. Bitcoin est un protocole open-source, ce qui signifie que son code source est en accès libre sur Internet. Bitcoin est très difficile à corrompre ou à modifier car il est surveillé en permanence par des milliers de personnes à travers le monde. Grâce à un nœud complet, tout le monde peut télécharger, utiliser, copier et exécuter le logiciel Bitcoin et valider son registre. Plus les nœuds sont nombreux sur le réseau, plus il devient résilient.

Les gouvernements peuvent rendre le bitcoin plus difficile à utiliser mais cela ne peut devenir qu'un jeu de taupe. Considérez une expérience d'échange de monnaie fiduciaire contre bitcoin dans un pays comme la Chine. Comme mentionné au chapitre 1, les Chinois ne peuvent que convertir l'équivalent de 50 000 USD de leur CNY chaque année mais continuent d'utiliser bitcoin pour les transferts d'argent à l'étranger.

Même un grand État riche et policier ne peut pas empêcher ses citoyens d'utiliser bitcoin. Son protocole n'ayant aucun point de défaillance unique, aucun gouvernement ne peut arriver à le désactiver.

Bitcoin est similaire à Internet. Un gouvernement peut empêcher sa population d'accéder à certaines parties d'Internet, c'est ce que montre le grand pare-feu chinois, mais les citoyens censurés utilisent des outils comme les VPN pour contourner ces restrictions. Aucun gouvernement ne peut bloquer l'accès à Bitcoin sans supprimer l'accès à Internet lui-même, un coût que peu de gouvernements, hormis la Corée du Nord, semblent prêts à assumer.

Les régimes autoritaires pourraient interdire la possession de bitcoin, mais l'application d'une telle mesure serait extrêmement difficile. En raison de sa nature numérique, cacher les bitcoins est relativement facile. Il existe plusieurs options de garde très difficiles à découvrir et à pénaliser. Les bitcoins peuvent être stockés sur un téléphone, un périphérique USB ou même dans son esprit.

En revanche, l'or, les biens immobiliers, les actions et la monnaie fiduciaire sur les comptes bancaires sont, pour les gouvernements, tous relativement faciles à localiser et à confisquer.

Bitcoin est-il légal?

D'un point de vue général, oui. Depuis août 2019, sa possession n'est pas interdite dans tous les pays à l'exception de la Namibie, l'Algérie, la Bolivie, l'Irak, le Maroc, le Népal, le Pakistan, les Émirats arabes unis et du Vietnam. D'un point de vue réglementaire, bitcoin a parcouru un long chemin: au cours des 10 dernières années, il est passé du statut de monnaie des criminels du darknet à une reconnaissance du FMI, des membres du Congrès américain et de Wall Street.

En Chine, le gouvernement a exercé un contrôle sévère sur les plateformes d'échange de crypto-monnaies et la création de nouveaux jetons, mais bitcoin est légalement reconnu comme une propriété numérique. Même en Iran, le minage est désormais une industrie légalisée.

Sur le continent africain, les gouvernements de nombreux pays n'ont pris aucune position publique sur le sujet. Dans des endroits comme le Nigéria et le Kenya, les fonctionnaires mettent en garde contre l' utilisation du bitcoin sans toutefois mettre en place une réglementation concrète. L'Afrique du Sud est actuellement le seul pays africain où le bitcoin est officiellement accepté et réglementé.

Au Canada, aux États-Unis et dans l'Union Européenne, la possession et l'utilisation de bitcoin sont légales.

Quelques pays ont créé un cadre de réglementation spécifique pour les entreprises qui souhaitent exploiter les plateformes d'échange des cryptomonnaies. Il s'agit notamment du Japon, de Malte, des Philippines et de la Thaïlande.

Les implications fiscales sont plus compliquées et déterminées par la manière dont chaque gouvernement classe bitcoin. Si une autorité fiscale le considère comme un bien, les particuliers seront imposés en conséquence sur son acquisition, sa liquidation, son appréciation et sa dépréciation comme pour un bien immobilier.

A l'avenir, si certains gouvernements veulent conspirer pour interdire le bitcoin, il est peu probable qu'ils parviennent à un accord. Même si certains pays réussissent à instaurer une interdiction, d'autres ne le feront pas et accueilleront les mineurs, les entrepreneurs et les négociants des bitcoins. Il y aurait une migration de talents et de richesses vers les juridictions crypto-friendly, ce qui obligerait les gouvernements restrictifs à repenser leurs politiques.

Le minage de bitcoin est-il un gaspillage d'énergie nocif pour l'environnement?

En juin 2019, le réseau Bitcoin consommait environ 73 térawattheures d'électricité par an. C'est plus de consommation qu'un pays comme l'Autriche (69 térawattheures par an) mais c'est beaucoup moins que la Chine (6100 térawattheures par an) ou les États-Unis (3900 térawattheures par an), les deux plus gros consommateurs d'énergie.

Les critiques s'empressent à souligner qu'il s'agit d'une énorme quantité d'énergie. Bien que cela soit techniquement vrai, ce n'est pas suffisant pour déterminer si Bitcoin gaspille de l'énergie ou qu'il est nocif à l'environnement. Les sources d'énergie généralement utilisées par les mineurs et le rendement que rapporte l'industrie du minage peuvent indiquer un certain contexte.

Prévenir le gaspillage d'énergie par le minage

Le minage de bitcoin peut aider à valoriser l'excédent d'énergie. L'exploitation minière du bitcoin est à la fois une industrie très mobile et à faible marge. Les sociétés spécialisées dans le domaine sont particulièrement motivées et capables de rechercher l'électricité la moins chère possible. Souvent, les sources d'énergie les moins chères se trouvent dans des endroits éloignés ou inaccessibles où il existe une surproduction d'énergie par rapport aux besoins locaux.

Le minage du bitcoin se fait en grande partie en Chine, où les centrales électriques produisent collectivement un excédent de 200 térawattheures à n'importe quel moment. Puisqu'il n'est pas possible de stocker autant d'énergie (le plus grand parc de batteries au monde ne peut contenir qu'environ 0,5% de cette quantité) - et qu'il n'est pas possible de la transmettre efficacement aux régions éloignées - cette électricité reste généralement inexploitée. Plutôt que de gaspiller ce potentiel, les centrales électriques peuvent se procurer du matériel de minage et transformer cet excédent d'énergie en nouveaux bitcoins. Cela est possible dans tous les endroits où une source d'énergie génère trop d'énergie pour une utilisation immédiate.

La dépendance du minage aux énergies renouvelables

Aujourd'hui, le minage est réalisé à majorité avec de l'énergie renouvelable. Cela a un coût minime pour l'environnement. Selon les dernières estimations, environ 75% du minage se fait actuellement avec des sources d'énergie hydroélectriques, solaires, éoliennes et géothermiques. Environ 50% du minage par énergie verte est effectué dans dans une région chinoise alimentée par des centrales hydroélectriques.

Les centrales hydroélectriques ont une grande capacité de production d'énergie mais restent souvent sous-utilisées. Le minage de bitcoin utilise généralement cette capacité excédentaire dégagée par les centrales.

Les mineurs s'installent souvent à côté des centrales hydroélectriques, ce qui réduit leurs coûts d'opérations. Les revenus générés rendent la production et la recherche d'énergie hydroélectrique plus rentables, ce qui encourage son utilisation. C'est de cette façon que le minage du bitcoin subventionne l'hydroélectricité.

Le minage peut également inciter à une plus grande production d'énergie solaire, éolienne et géothermique.

Le minage pour une monnaie sûre et accessible

Les mineurs assurent la sécurité du réseau. Comme nous l'avons vu au chapitre 2, l'électricité requise par ces derniers pour rechercher la preuve de travail et proposer des blocs valides rend la fraude très coûteuse. Plus il y a de nombreux mineurs de bitcoins, plus il devient difficile d'attaquer le réseau. L'énergie utilisée pour sécuriser la blockchain du bitcoin peut être comparée au coût de création et de maintenance d'un coffre-fort hautement sécurisé qui protège plus de 200 milliards de dollars d'actifs.

Bitcoin n'est peut-être qu'une option financière parmi tant d'autres en occident mais dans d'autres régions du monde, les services de paiement comme Vennmo ou ApplePay n'existent pas. Considérer le minage comme un gaspillage d'énergie revient à sous-estimer l'utilité que Bitcoin apporte à la sous-classe technologique. Une partie de cette énergie sert au traitement des transactions de personnes qui n'ont pas de compte bancaire, d'identité, ou qui ne veulent pas que leur activité financière soit étroitement surveillée par les gouvernements. Les banques et les cartes de crédit peuvent dépasser

l'utilité du bitcoin dans un endroit comme les États-Unis, mais ne font rien pour un travailleur migrant non bancarisé à Dubaï ou un Iranien vivant sous les sanctions de l'ONU.

Utilisation d'énergie et innovation technologique

Bitcoin est une innovation technique majeure qui a rendu possible de nombreuses choses, décrites dans ce livre, que le système monétaire traditionnel ne peut permettre. Historiquement, chaque nouvelle technologie utilise plus d'énergie que l'ancien système qu'elle remplace. Par exemple, considérons le remplacement du cheval par la voiture; la tente de campagne par l'hôpital moderne; du lavage sauvage par la machine à laver; de la glacière par le réfrigérateur, des lampes à huile par les lampes électriques. Le coût d'électricité de chaque innovation technique est compensé par l'amélioration de la qualité de vie. Plus la civilisation va progresser, plus chaque individu va dépenser beaucoup plus d'énergie. L'innovation améliore la vie sociale et ne peut être adoptée sans quelques compromis.

Dans le cas du bitcoin le compromis est l'utilisation de l'électricité en échange d'un système monétaire équitable, pratique et sûr. Bitcoin utilise beaucoup d'énergie, mais stimule l'innovation dans le secteur des énergies renouvelables. Il est très utile en particulier pour les pauvres, les opprimés et remplace un système ancien et défectueux qui gaspille encore plus d'énergie.

Et si quelqu'un avec un supercalculateur ou un ordinateur quantique piratait le réseau Bitcoin?

En théorie, le réseau Bitcoin peut être compromis par un attaquant disposant d'une puissance de calcul monstrueuse. Pratiquement, c'est très difficile à faire.

En utilisant le matériel actuel, un attaquant doit financer, construire et exploiter une installation minière pour un coût de plus d'un milliard de dollars, puis trouver un fournisseur d'énergie avec une puissance équivalente à 8 barrages Hoover. Les mêmes ressources lorsqu'elles sont consacrées honnêtement au minage constituent une entreprise extrêmement rentable. Une telle attaque est donc économiquement irrationnelle.

Au moment d'écrire ces lignes, voici ce qui est vrai au sujet de l'informatique quantique:

1. Les ordinateurs quantiques sont extrêmement lents par rapport aux ordinateurs conventionnels de plusieurs ordres de grandeur.

2. Les ordinateurs quantiques sont extrêmement coûteux à construire et leur coût va rester prohibitif pendant un certain temps.

3. Les algorithmes quantiques les plus connus représentent une véritable évolution mais il faudrait encore plusieurs milliards d'ordinateurs fonctionnant pendant des milliards d'années pour craquer la cryptographie utilisée dans Bitcoin.

Même si les scientifiques découvraient des nouveaux algorithmes quantiques susceptibles de briser la cryptographie moderne, cette même innovation serait alors intégrée au protocole Bitcoin.

En d'autres termes, les utilisateurs et la communauté de développeurs Bitcoin seraient en mesure d'avoir une longueur d'avance sur les attaquants quantiques. Si la communauté Bitcoin est vigilante contre les possibilités d'attaques à grande échelle, son l'utilisateur moyen n'a pas à s'inquiéter.

Comment Bitcoin reste-t-il décentralisé?

L'une des propriétés les plus importantes de Bitcoin c'est le fait pour n'importe qui dans le monde d'avoir la possibilité de télécharger une copie complète de l'ensemble de son registre et vérifier par lui même que l'historique est correct.

Comme indiqué dans le deuxième chapitre, cette pratique consiste à exécuter un nœud complet. La facilité d'utilisation d'un nœud est essentielle pour garder le réseau résistant à la censure. Si l'ensemble du réseau comptait sur une poignée d'entreprises ou un petit groupe de personnes riches pour gérer des nœuds complets, ils pourraient avoir la possibilité de se mettre d'accord pour modifier le registre ou même voler des bitcoins.

Heureusement que chaque utilisateur peut, en exécutant un nœud complet, vérifier l'exactitude de données afin de ne pas avoir à faire confiance à quelqu'un d'autre. S'il était impératif d'acheter un équipement coûteux et d'avoir une connexion Internet extrêmement rapide pour exécuter un nœud complet, cela obligerait les plus pauvres à faire confiance aux tiers. Le réseau se centraliserait naturellement autour des pays développés et d'entreprises high-tech.

Comme les exigences pour exécuter un nœud complet sont très faibles, plusieurs milliers d'utilisateurs sur différents continents, complètement inconnus les uns des autres, vérifient en permanence la blockchain Bitcoin. De plus, le matériel requis pour opérer un nœud complet est disponible sur le marché et sa configuration reste accessible aux utilisateurs non techniques. Cela permet à tout celui qui le souhaite d'opérer facilement un nœud complet à domicile. Actuellement, plusieurs scientifiques d'institutions telles que le MIT et Stanford travaillent sur la conception des solutions qui permettront de faire tourner un nœud complet directement sur un téléphone portable. Cela va renforcer la décentralisation du Bitcoin.

Bitcoin protège-t-il la vie privée ?

Une idée fausse et très répandue est que les transactions en bitcoins sont anonymes. En réalité, ces dernières sont pseudonymes et, avec suffisamment d'analyse, il est possible de les lier à l'identité des utilisateurs. Malgré cela, un utilisateur averti, avec une une sécurité opérationnelle appropriée, a la possibilité de masquer ses transactions pour échapper à la surveillance. Cependant, avec suffisamment de temps et de ressources, un État ou une entreprise motivée peut toujours retrouver les traces d'un individu à partir de ses transactions bitcoin.

Cela dit, bitcoin offre une bien meilleure confidentialité que les systèmes de paiement traditionnels. Avec ce dernier, il est possible d'acheter en ligne sans révéler les données personnelles comme le nom, le compte bancaire ou l'adresse personnelle, ce qui est très différent du système bancaire grâce auquel gouvernements, entreprises et commerçants demandent, vendent ou provoquent régulièrement la fuite de données personnelles de leurs clients.

Des travaux visant à renforcer la confidentialité tout en réduisant le coût des transactions sont en cours sur Bitcoin. C'est notamment le Lightning Network, Taproot, Graftroot et les signatures de Schnoor. Avec cela, Bitcoin a le potentiel de

devenir une excellente technologie de protection de la vie privée et un outil capable de rendre la surveillance économique encore plus difficile.

A ses débuts, Internet était complètement ouvert et public. Alors que les utilisateurs et les entreprises avaient besoin de plus de transactions privées, les ingénieurs ont ajouté des couches de confidentialité au protocole d'origine. La communication privée est désormais possible grâce aux applications qui envoient des messages chiffrés. Bitcoin suit un chemin similaire.

Comment Bitcoin peut-il répondre aux besoins de 7 milliards de personnes?

En 1989, quand les scientifiques ont inventé le World Wide Web pour fonctionner sur Internet, l'idée que les utilisateurs pourraient un jour échanger des photos, et encore moins des vidéos semblait techniquement impossible. A mesure que la technologie évoluait, Internet a été capable de supporter des applications autrefois impensables et gourmandes en ressources telles que le partage vidéo et la diffusion directe des conférences. 300 heures de vidéo sont téléchargées chaque minute sur YouTube et 5 milliards autres regardées chaque jour. Tout comme Internet, il existe de nombreuses façons de faire évoluer Bitcoin.

Comme indiqué au chapitre 4, les capacités de Bitcoin sont actuellement renforcées par Lightning Network. En plus d'améliorer la confidentialité des transactions, Lightning rend Bitcoin plus scalable.

Des millions de transactions peuvent être traitées sur Lightning Network chaque seconde. Bitcoin est en passe de connaître une croissance exponentielle alors que les réseaux de paiement traditionnels comme Visa évoluent de manière linéaire en ajoutant de plus en plus de serveurs. Bitcoin pourrait révolutionner la monnaie et permettre la création des produits entièrement nouveaux grâce aux micro paiements aussi granulaires qu'un millième (1/1000) de satoshis.

Grâce à une combinaison de transactions occasionnelles lentes, ultra-sécurisées et résistantes à la censure sur la blockchain et celles groupées, instantanées et moins coûteuses sur Lightning, Bitcoin peut devenir un système de paiement mondial. Cette vision mérite d'être poursuivie, car elle permettrait de retirer

le pouvoir sur la finance de mains des gouvernements et entreprises pour le remettre entre celles de citoyens.

Bien qu'il soit difficile d'imaginer aujourd'hui un bitcoin répondant aux besoins des milliards de personnes n'est pas moins un concept farfelu que le streaming vidéo à des milliards de téléspectateurs ne l'était aux débuts d'Internet.

Bitcoin favorise-t-il une extrême inégalité de richesse?

Les personnes impliquées dans Bitcoin dès son apparition ont accumulé plusieurs bitcoins. La blockchain a cependant montré que de nombreux utilisateurs de 2009 à 2012 ont vendu leurs bitcoins au cours de la même période. Plusieurs acheteurs de 2011, quand le cours était à 1 $, ont vendu leur bitcoin à 4 ou à 30 $ quelques mois plus tard.

De nombreux utilisateurs de l'époque n'ont pas été à la hauteur de supporter la volatilité et l'incertitude des premiers jours ou ont perdu leurs clés privées, perdant définitivement leurs bitcoins. Ceux qui ont tenu bon ont soutenu l'écosystème dès ses débuts et croient réellement au potentiel de Bitcoin pour changer le monde.

Aujourd'hui, il existe quelques milliers d'adresses qui stockent la majorité des bitcoins en circulation. Certaines appartiennent à des individus qui sont devenus très riches et le reste, la majorité, appartiennent aux entreprises qui utilisent de telles adresses pour garder les fonds de leurs clients (c'est le cas de Coinbase, Binance, etc). Comme il n'y a pas de corrélation entre ces adresses et les utilisateurs de plateformes d'échanges, il est difficile de savoir la réelle répartition de cette richesse.

Le but du bitcoin n'a jamais été de mettre fin aux inégalités économiques. Quiconque affirme cela ne fait que tromper. Cependant, en tant que réserve de valeur universellement accessible à tous et qui ne peut être dévaluée par les gouvernements, bitcoin donne aux épargnants une chance équitable de conserver leurs avoirs dans le temps, contrairement au système monétaire traditionnel.

S'il n'y aura que 21 millions de bitcoins, comment seront-ils utilisés à l'échelle mondiale?

Les monnaies traditionnelles sont généralement divisibles en 100 sous-unités appelées cents ou centimes. 1 dollar US et 1 euro peuvent être divisés en 100 cents, le Yen en 10 jiao ou 100 fen et CZK (couronne tchèque) en 100 haler.

En revanche, chaque bitcoin peut être divisé en 100 000 000 (cent millions) d'unités plus petites. L'unité la plus petite du bitcoin est appelée satoshi (ou sat, en abrégé), le nom de l'inventeur de Bitcoin. Ainsi, l'offre totale de bitcoin est de 2,100,000,000,000,000 satoshis. Pour le contexte, c'est plus divisible que l'USD, dont la masse monétaire M2 est de 1 500 000 000 000 000 cents au moment de la rédaction de ce bouquin. La divisibilité du bitcoin est supérieure ou égale à celle de l'USD.

Comme exercice de réflexion, diviser tous les satoshis existants entre 7 milliards de personnes donne 300 000 sats par personne. Cela semble être suffisant pour satisfaire les activités économiques de chaque personne si le bitcoin devient la monnaie dominante du monde.

Comment puis-je me permettre d'acheter un bitcoin avec un prix si élevé?

Bitcoin est divisible, il est donc possible d' acheter une petite fraction de 5 $ ou même 25 $ qui équivaut respectivement à 0,00044 bitcoins et 0,0022 bitcoins à ce jour.

Comment acquérir des bitcoins?

Les principaux moyens d'obtenir des bitcoins sont:

1. le minage
2. l'achat
3. les gains

Le minage

À ce stade de l'histoire de Bitcoin, son minage est une activité à très faible marge. Tout comme l'extraction de l'or, l'équipement, les contacts au sein de l'industrie et les connaissances pour exploiter une ferme de manière rentable nécessitent des années d'expérience et des millions de dollars de capital. En tant que tel, le minage est devenu un secteur dominé par des entreprises disposant de ressources et d'un savoir-faire importants. Il est devenu impossible pour des personnes inexpérimentées de rentabiliser l'activité. Pour les nouveaux utilisateurs, bitcoin sera moins cher à acheter qu'à miner.

Acheter des bitcoins

Il existe plusieurs façons d'acheter des bitcoins, certaines plus respectueuses de la vie privée que d'autres. Les ATM bitcoin et le trading pair-à-pair sont plus rapides et relativement privés.

Les investisseurs peuvent également s'inscrire sur les plateformes d'échanges en ligne, dont plusieurs sont répertoriés dans les ressources supplémentaires. Les nouveaux clients sont tenus de soumettre leurs informations personnelles. Le processus d'approbation peut prendre de quelques minutes à quelques jours. Les plateformes d'échanges sont des entreprises qui agissent comme des banques en conservant les bitcoins et la monnaie fiduciaire de leurs clients. Les utiliser implique donc de renoncer à une certaine confidentialité, mais les clients peuvent s'assurer de la propriété de leurs bitcoins en les retirant de ces plateformes vers leurs portefeuilles personnels.

Gagner des bitcoins

En utilisant un portefeuille Bitcoin ou Lightning, n'importe qui peut directement en recevoir comme paiement pour de biens ou de services. Les employés peuvent recevoir une partie de leur salaire en bitcoin à la place de la monnaie fiduciaire.

Comment utiliser un portefeuille Bitcoin?

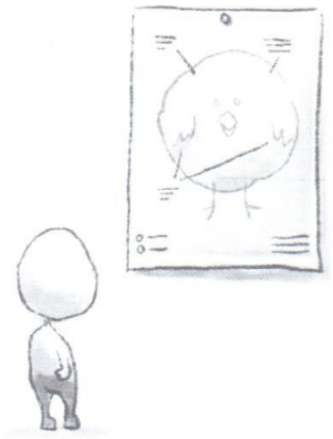
Il existe plusieurs types de portefeuilles bitcoin parmi lesquels les portefeuilles matériels, les portefeuilles de bureau, les portefeuilles mobiles et en ligne. Chacun d'entre eux a des compromis différents en matière de sécurité, expérience utilisateur et de confidentialité qu'il est important pour les utilisateurs d'analyser.

Un moyen raisonnablement sûr de stocker des bitcoins consiste à utiliser un portefeuille non dépositaire, répertorié dans la rubrique portefeuilles matériels dans les ressources supplémentaires. En attendant, le moyen le plus pratique pour un débutant est de télécharger un portefeuille mobile gratuit;certains sont cités dans les ressources supplémentaires.

Après le téléchargement, la première étape de la configuration d'un portefeuille Bitcoin consiste à créer une sauvegarde. Ceci consiste à écrire et garder en sécurité une liste de mots qui aident à récupérer son portefeuille en cas de perte de son appareil mobile. Étant donné que cette suite de mots, également appelée phrase de récupération peut être utilisée pour recréer le portefeuille, elle doit être soigneusement sécurisée. Chaque utilisateur d'un portefeuille doit y penser de la même manière qu'un lingot d'or ou un diamant. La phrase de récupération est très importante et doit être protégée en conséquence. À mesure que l'écosystème se développe, les nouveaux portefeuilles se concentrent sur la réduction de la complexité. Cela passe par l'amélioration de l'expérience utilisateur, la sécurité et la confidentialité.

Une fois qu'un portefeuille est configuré, il peut générer des adresses uniques pour chaque nouveau paiement. Cela diffère de la manière dont fonctionnent les paiements bancaires habituels, où un client ne se voit généralement proposer qu'un seul numéro de compte. Bitcoin apporte une meilleure confidentialité en permettant l'utilisation de plusieurs adresses uniques à partir d'un même portefeuille.

Comme mentionné dans la partie où nous expliquons pourquoi plusieurs plateformes d'échange ont été piratées, les investisseurs qui se servent des services de garde sont exposés au risque de piratage. Retirer ses fonds vers des portefeuilles personnels après l'achat atténue ce risque.



Ressources Supplémentaires

Le Livre Blanc du Bitcoin

Bitcoin A Peer-to-peer Electronic cash system, par satoshi nakamoto. C'est est le chef-d'œuvre original qui a défini bitcoin, la révolution financière des dix dernières années.

Le Code source

Bitcoin Core est le code source de référence du logiciel de nœud complet. Créé à l'origine par Satoshi Nakamoto, Bitcoin Core a bénéficié de contributions de plus de 500 développeurs à travers le monde.

Livres

The Internet of Money (vol 1 & 2), par Andreas M. Antonopoulos. Ce livre plonge en profondeur dans le «pourquoi» du Bitcoin. C'est un régroupement d' essais et conférences de l'auteur.

Programming Bitcoin, par Jimmy Song : un guide technique pratique de l'un des principaux enseignants sur la programmation sur Bitcoin. Il a été rédigé à l'intention des développeurs qui souhaitent construire des applications autour de Bitcoin ou contribuer à son évolution technologique.

The Bitcoin Standard de Saifedean Ammous fournit une histoire économique de la monnaie et une explication de la façon dont Bitcoin offre une alternative aux banques centrales.

Inventing Bitcoin , par Yan Pritzker : un guide sur le fonctionnement de Bitcoin étape par étape. Une formation en mathématiques de niveau secondaire est un pré requis pour le lire.

Bitcoin money: A Tale of Bitville Discovering Good Money, par The Bitcoin Rabbi : un livre pour enfants avec des personnages colorés. Il vise à aider les enfants à en apprendre davantage sur le Bitcoin.

Mastering Bitcoin: Programming the Open Blockchain, par Andreas M. Antonopoulos : un guide complet de la programmation avec et pour Bitcoin.

Sites Web et publications

Bitcoin.org contient des informations utiles sur comment se lancer dans l'aventure Bitcoin, ainsi que de la documentation et des liens vers d'autres ressources. L'utilisation de Bitcoin.com n'est pas recommandée car le site web associe intentionnellement d'autres crypto-monnaies à BTC dans le but d'inciter ses clients à en acheter à la place.

Bitcoin.page est un véritable trésor de ressources éducatives et d'informations sur Bitcoin soigneusement sélectionnées par Jameson Lopp.

Bitcoin Wiki est une ressource publique pour la communauté des utilisateurs, des développeurs, des entreprises et toute personne intéressée par Bitcoin.

Coin Center est une organisation à but non lucratif basée aux États-Unis dont l'activité se concentre sur enjeux politiques auxquels sont confrontés Bitcoin et d'autres crypto-monnaies. Ils publient constamment des explications perspicaces en termes simples sur divers sujets.

Bitcoinmining.com propose les ressources nécessaires sur le minage de Bitcoin, comment ça fonctionne, ce qu'il faut pour se lancer et et un comparatif de différents matériels.

Global Coin Search travaille sur les tendances crypto entre les États-Unis et l'Asie.

Podcasts

Thales from the Crypt est un podcast animé par Marty Bent pour parler de Bitcoin avec des intervenants intéressants.

What Bitcoin Did est une émission présentée deux fois par semaine par Peter McCormack. Il fait des interviews avec les entrepreneurs et les influenceurs de la communauté Bitcoin.

The Stephan Livera Podcast est une émission axée sur des entretiens éducatifs et des échanges sur l'économie et la technologie du Bitcoin.

Noded est un podcast animé par Michael Goldstein et Pierre Rochard. Il s'intéresse aux nouveaux développements techniques sur Bitcoin.

Off The Chain est un podcast d'Anthony Pompliano qui explore la façon dont les investisseurs du nouveau et de l'ancien système financier pensent des actifs numériques comme bitcoin.

Unchained and et Unconfirmed sont des podcasts hebdomadaires où Laura Shin interviewe des grands noms de la cryptosphère.

Let's Talk Bitcoin présente les idées et les personnes impliquées dans la crypto à travers une série d'entretiens et d'échanges avec un groupe d'hôtes réguliers.

The bitcoin Knowledge podcast est une émission dans laquelle Trace Mayer interroge d'éminents contributeurs Bitcoin pour aider ses auditeurs à mieux comprendre la proposition technologique de Bitcoin.

Plateformes d'échange en ligne

Disclaimer : bien que cette section mentionne des sites, des applications ou des services spécifiques au sein de l'écosystème Bitcoin, cela ne doit pas être interprété comme un conseil d'investissement. Comme pour les autres parties de ce livre, le lecteur est encouragé à faire ses propres recherches.

Fiat-crypto

Bitfinex : lancé à en 2014, la plateforme est basée à Hong Kong.

CashApp : Une application de Square. Elle est disponible sur iOS et Androïd. C'est un moyen facile d'acheter des bitcoins à l'aide d'une carte de débit.

Kraken : Exchange américain et Européen sur le marché depuis 2014.

Crypto-crypto

Binance : Basé à Malte et lancé depuis 2017

BitMex : basé aux Seychelles et lancé en 2014

Bittrex : un exchange américain qui existe depuis 2016.

Marchés pair-à-pair

LocalBitcoins: Exchange P2P finlandais créé en 2012. Il propose l'échange des bitcoins.

Paxful : Exchange P2P américain. Il propose l'échange des bitcoins depuis 2015.

Bisq : Un exchange P2P axé sur la confidentialité depuis sa création en 2014.

Portefeuilles

Custodial (les utilisateurs ne contrôlent pas les clés privées)

Blockchain.info

CashApp

Coinbase

Non-Custodial (les utilisateurs contrôlent les clés privées)

BreadWallet (iOS)
Bitcoin Core : Portefeuille de bureau

Casa Keymaster : Application multisig sur Android et iOS avec prise en charge des portefeuilles physiques.

Samourai : disponible sur Android

Wasabi : Portefeuille de bureau

Portefeuilles physiques ou **Hardware Wallets** (les utilisateurs contrôlent les clés privées)

ColdCard

Ledger

Trezor

Solutions pour noeuds complets

Casa Node : Noeud complet supportant Lightning et Bitcoin

Nodl : Noeud complet Bitcoin et Lightning

Glossaire

adresse - L'équivalent d'un numéro de compte bancaire, une adresse bitcoin permet de recevoir des bitcoins. Chaque adresse a une clé privée correspondante qui permet au propriétaire de dépenser son bitcoin en signant numériquement une transaction.

bancor - l'unité de monnaie mondiale proposée à Bretton Woods en 1944.

Bitcoin - un protocole qui rend possible le fonctionnement du système monétaire créé par Satoshi Nakamoto.

bitcoin - l'unité de valeur sur le réseau Bitcoin. Chaque bitcoin correspond à 100 000 000 satoshis.

block - un groupe de transactions bitcoin regroupées grâce à une preuve de travail. Un bloc équivaut à une page du grand livre comptable de Bitcoin. Chaque 10 minutes en moyenne, un nouveau bloc est créé.

blockchain - un système de registre distribué mis au point par Bitcoin. La blockchain référence la quantité de bitcoins contenue sur chaque adresse. Une blockchain est composée de blocs.

technologie blockchain - systèmes créés pour utiliser l'innovation blockchain de Bitcoin dans une certaine mesure. Il n'y en a eu aucune qui ait été largement adoptée à part Bitcoin et une poignée d'autres crypto-monnaies.

BTC - symbole/ticker utilisé pour représenter bitcoin sur les plateformes d'échange, dans les commerces et sur les portefeuilles. XBT est aussi utilisé pour désigner bitcoin.

autorité centrale - une agence ou une organisation qui prend des décisions dans un système donné.

centralisé - un système avec un point de défaillance unique. Il peut s'agir, par exemple, d'un système géré par une personne, une fondation, une entreprise ou un gouvernement.

Exchange crypto-crypto - une plateforme d'échange qui permet uniquement le trading entre crypto-monnaies.

décentralisé - un système sans point de défaillance unique.

signature numérique - la preuve qu'un utilisateur ou un signataire connaît la clé privée liée à une adresse bitcoin. Elle est conceptuellement similaire à la signature d'un chèque pour confirmer qu'une personne est titulaire d'un compte, à la différence qu'elle

ne dévoile pas l'écriture manuscrite de la personne. Lors de l'envoi des bitcoins, l'expéditeur signe la transaction, prouvant la propriété, sans révéler la clé privée.

Dollar standar - le système de domination monétaire de l'USD dans le commerce mondial. Il a été lancé en 1944 après Bretton Woods et prolongé en 1971 à travers le pétrodollar.

Monnaie fiduciaire - une monnaie émise par une banque centrale.

Exchange fiat-to-crypto - une plateforme qui permet l'échange direct de la monnaie fiduciaire en cryptomonnaie.

FOMO - «Fear Of Missing Out», un terme souvent utilisé pour décrire les décisions d'achat irrationnelles.

Noeud complet - logiciel utilisé pour vérifier les transactions et l'intégrité de la blockchain.

Gold standard - un système monétaire mondial où la valeur d'une monnaie fiduciaire était soutenue par une quantité d'or en réserve.

Halving - un événement sur le réseau Bitcoin où tous les 4 ans, la récompense du minage pour un bloc diminue de moitié.

KYC - Know Your Customer ou «Connaître son client», une pratique imposée par les gouvernements aux banques. Ces derniers collectent plusieurs informations personnelles sur leurs clients afin de leur fournir un service financier. Ces informations sont ensuite fournies aux gouvernements par le biais de lois telles que la loi américaine sur le secret bancaire.

Effet de levier - une pratique qui permet à un trader de négocier jusqu'à 100 fois le montant de son capital.

Lightning network - un système développé pour permettre au réseau Bitcoin de traiter des millions de transactions par seconde. Cette innovation ajoute également une importante confidentialité significative aux transactions bitcoin.

liquidité - le montant d'échanges sur un actif au cours d'une période donnée

mineur - un individu ou un groupe (appelé «pools de minage») qui utilise des ordinateurs spécialisés pour rechercher la preuve de travail afin de créer de nouveaux blocs.

récompense minière - les bitcoins qu'un mineur reçoit pour avoir validé les transactions tout en sécurisant le réseau Bitcoin.

Carte Octopus - une carte de paiement électronique pour étudiants à Hong Kong.

transaction hors chaîne - une transaction qui n'est pas directement enregistrée sur blockchain Bitcoin, comme c'est le cas avec les transactions sur Lightning Network.

transaction on-chain - une transaction traitée et enregistrée directement sur la blockchain Bitcoin.

Exchanges pair-à-pair - une plateforme d'échange qui nécessite la mise en relation de personnes qui souhaitent exécuter une transaction

clé privée - similaire à un mot de passe pour un compte bancaire, une clé privée déverrouille la possibilité de transférer des bitcoins à partir d'un portefeuille donné. La propriété des clés privées équivaut à celle des bitcoins.

preuve de travail - le processus par lequel les mineurs prouvent qu'ils ont dépensé de l'énergie pour proposer un nouveau bloc valide et prêt à être ajouté à la blockchain.

blockchain publique - une blockchain qui peut être téléchargée, consultée et validée par n'importe qui.

sat / satoshi - la plus petite unité de bitcoin. 100 000 000 satoshis équivaut à 1 bitcoin.

Satoshi Nakamoto - le créateur de Bitcoin.

portefeuille - une application ou un périphérique matériel qui permet aux utilisateurs d'envoyer et recevoir des bitcoins.

livre blanc - un rapport faisant autorité, souvent académique, destiné à informer pleinement le lecteur sur un sujet particulier. Le document original décrivant Bitcoin et ses détails techniques a été présenté sous ce format par Satoshi Nakamoto en octobre 2008.

Remerciements

Les auteurs tiennent à remercier les personnes suivantes pour le temps et l'expertise qu'elles ont consacrée à ce qui aurait, autrement, été une initiative beaucoup plus difficile:

Leigh Cuen
Sam Corcos
Nick Foley
Irl Nathan
Jane Song Lee
June Park
Rodrigo Linares
Jan Čapek
Nick Neuman
Tomiwa Lasebikan

Nous tenons également à remercier les personnes suivantes pour leur soutien pendant notre book sprint :

Bill Barhydt
Daniel Buchner
Cryptograffiti
Jill Carlson
Juan Gutierrez
Han Hua
Ben Richman
Bill Tai
Mike Youssefmir
Sébastien Lhuilieri

Les personnes suivantes nous ont à la fois informé et inspirés au fil des années:

Nick Szabo
Andreas Antonopoulos
Jameson Lopp
Elizabeth Stark
Marek Palatinus
Pavol Rusnak
Michelle Lai

Les organisations suivantes nous ont encouragé à écrire ce livre:

Blockchain Capital
BloomX
BuyCoins Africa
Casa
Human Rights Foundation
Open Money Initiative
L'Université du Texas

Et bien sûr, nous sommes très reconnaissants à Tim Chang pour nous avoir laissé utiliser sa magnifique maison, et surtout, à nos familles et nos proches pour nous avoir encouragés.