

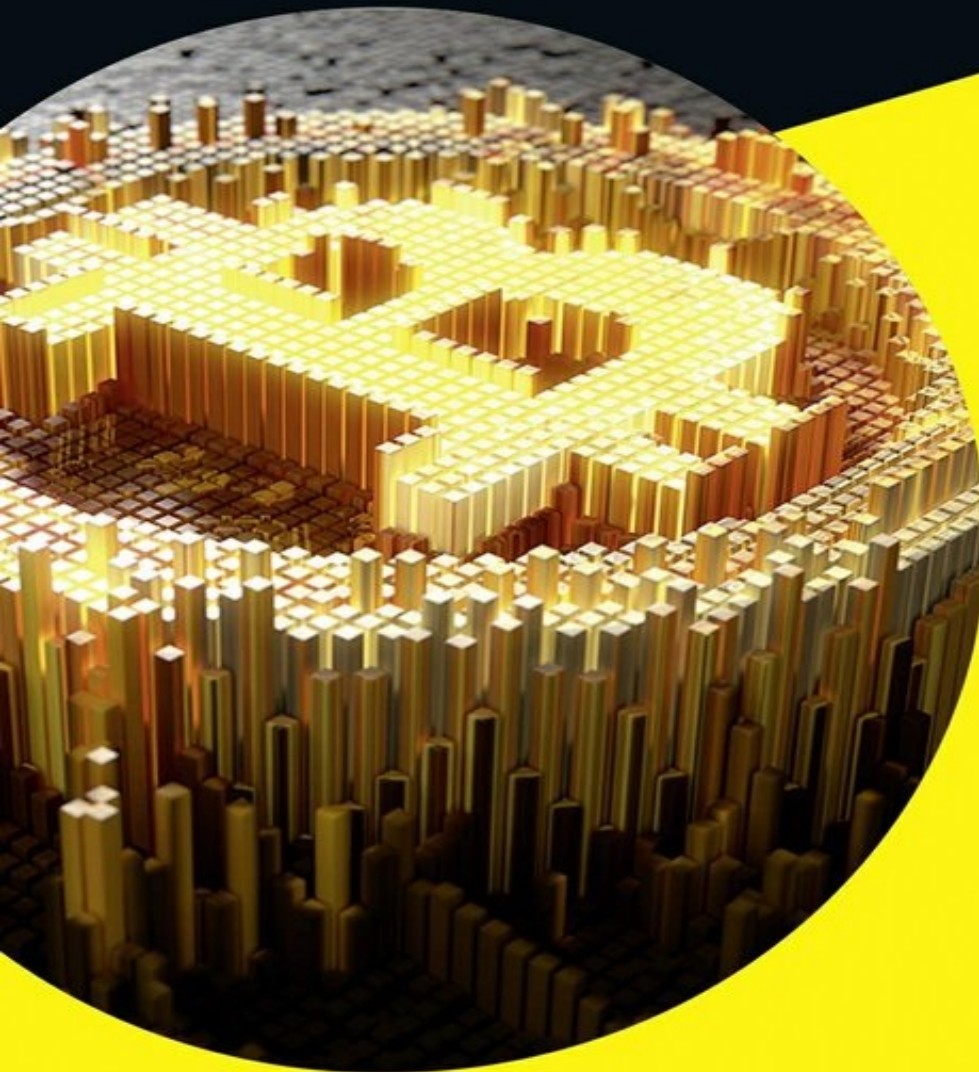


**Avec les Nuls, tout devient facile !**

# Bitcoin

pour

# les nuls



**Qu'est-ce que le bitcoin ?**

•

**Créer votre  
porte-monnaie  
de bitcoins**

•

**Découvrir l'utilisation  
des bitcoins pour payer**

•

**Agir contre les hackers,  
et sécuriser vos bitcoins.**

**Prypto**



# Bitcoin

pour

# les nuls

Prypto

FIRST  
 Editions

## **Bitcoin pour les Nuls**

Titre de l'édition originale : *Bitcoin For Dummies*

Pour les Nuls est une marque déposée de Wiley Publishing, Inc.  
For Dummies est une marque déposée de Wiley Publishing, Inc.

Collection dirigée par Jean-Pierre Cano

Traduction : Philip Escartin

Mise en page : Marie Housseau

Edition française publiée en accord avec Wiley Publishing, Inc.

© Éditions First, un département d'Édi8, 2017

Éditions First, un département d'Édi8

12 avenue d'Italie

75013 Paris

Tél. : 01 44 16 09 00

Fax : 01 44 16 09 01

E-mail : [firstinfo@efirst.com](mailto:firstinfo@efirst.com)

Web : [www.editionsfirst.fr](http://www.editionsfirst.fr)

ISBN : 9-782-412-02901-5

ISBN numérique : 9782412033524

Dépôt légal : 3<sup>e</sup> trimestre 2017

Cette œuvre est protégée par le droit d'auteur et strictement réservée à l'usage privé du client. Toute reproduction ou diffusion au profit de tiers, à titre gratuit ou onéreux, de tout ou partie de cette œuvre est strictement interdite et constitue une contrefaçon prévue par les articles L 335-2 et suivants du Code de la propriété intellectuelle. L'éditeur se réserve le droit de poursuivre toute atteinte à ses droits de propriété intellectuelle devant les juridictions civiles ou pénales.

Ce livre numérique a été converti initialement au format EPUB par Isako [www.isako.com](http://www.isako.com) à partir de l'édition papier du même ouvrage.

# Introduction

---

Bienvenue dans Bitcoin pour les nuls ! Bitcoin ? Vous avez dit « Bitcoin » ?!... « Je vous assure mon cher cousin que vous avez dit Bitcoin ! ». Bref ! Tout cela pour dire qu'il est légitime de se poser la question de savoir quels sont les principes et les notions qui recouvrent la monnaie numérique appelée aussi crypto-monnaie. Est-ce une monnaie destinée à l'Internet ? Est-ce une chose à laquelle vous pouvez souscrire sans honte d'en parler ? Force est de constater que beaucoup d'informations sur les bitcoins sont très superficielles. Vous avez probablement lu des articles narrant l'histoire de personnes ayant fait faillite à cause de cette monnaie venue d'ailleurs, ou ayant procéder à des achats illicites sur des marchés frauduleux. Mais peut-être vous a-t-on narré de fabuleuses histoires où des gens ont fait fortune grâce à ce drôle d'argent.

N'ayez aucune crainte, cher lecteur ! Ce livre lève le voile sur le grand mystère bitcoin pour vous en présenter les tenants et les aboutissants dans le monde réel. Il explique posément ce qu'est le bitcoin et les

possibilités de cette technologie perturbante, tout en exposant ses potentiels avantages pour nous tous. Le bitcoin pourrait modifier nos vies au même titre que l'a fait Internet il y a quelques décennies.

Ce livre vous dit tout ce que vous avez toujours voulu savoir sur le bitcoin sans jamais oser le demander.

## À propos de ce livre

---

Bitcoin pour les nuls raconte l'histoire de cette fascinante technologie et en explore le concept et la finalité. Nous verrons comment se constituer un portefeuille de manière à gérer vos bitcoins en toute sécurité. Nous vous expliquerons alors comment obtenir des bitcoins, ce que vous pouvez en faire, et comment gagner de l'argent avec. Nous évoquerons les cadres légaux et réglementaires, et verrons comment exploiter cette crypto-monnaie afin que vous jugiez de l'utilité d'y consacrer du temps et... de l'argent.

Nous allons ouvrir le capot de ce véhicule particulier afin de voir ce qu'il a dans le ventre. Nous détaillerons le fonctionnement des transactions dans l'environnement du bitcoin et approfondirons la technologie de la chaîne de blocs. Nous consulterons notre boule de cristal pour sonder le futur du bitcoin et du système de la chaîne de blocs, et spéculerons sur les

changements qu'ils risquent d'engendrer dans nos vies. Pour asseoir notre propos, nous vous renverrons vers des ressources en ligne afin que vous puissiez rester informé des nouveautés dans ce domaine et que vous pénétriez la communauté très active qui soutient le bitcoin. Rejoignez-nous dans cet incroyable parcours !

## Nos présomptions

Nous partons du principe que nos lecteurs sont avides de connaissances sur la crypto-monnaie. Nous souhaitons que cette lecture vous passionne au point de vous constituer un portefeuille, de commencer à utiliser des bitcoins, et de répandre cette bonne parole auprès de vos amis et de vos collègues. Bien entendu, nous sommes conscients que si vous avez acheté ce livre, c'est pour agir en personne informée, donc responsable.

Nous supposons que vous disposez d'une expérience suffisante en informatique et en Internet. De facto, nous sommes convaincus que la navigation sur le Web n'a plus de secret pour vous, et que vous savez comment mettre en œuvre des procédures de sécurité pour protéger votre argent virtuel en ligne. Nous sommes conscients que vous n'êtes pas un expert en informatique, et que votre découverte des bitcoins sera au niveau de celle d'un néophyte.



# Les icônes utilisées dans ce livre

Pour identifier certaines informations essentielles, nous avons mis au point un système d'icônes destinées à attirer votre attention sur des points particuliers.



Nos conseils vous seront servis sur un plateau. Cette icône identifie des astuces permettant de tirer le meilleur parti des bitcoins en nous appuyant sur l'expérience d'utilisateurs initiés. Ces conseils vous feront gagner en efficacité.



Avec cette icône, nous insistons sur des informations importantes à mémoriser, et qui vous serviront à un moment ou à un autre.



Cette icône attire votre attention sur des erreurs ou des pièges. Nous savons qu'en matière d'argent, vous agirez certainement en bon père ou en bonne mère de famille. Toutefois, l'excès d'enthousiasme qui peut nous gagner à certains moments nécessite des mises en garde. Donc, méfiance lorsque vous voyez cette icône. Lisez impérativement le paragraphe auquel elle renvoie.



Les finances en ligne, l'Internet, et la crypto-monnaie emploient des termes étranges et reposent sur des techniques complexes à appréhender. Il s'agit d'un univers aux termes parfois abscons et mystérieux, pour



ne pas dire inquiétants. Ainsi, il peut être utile de disposer de quelques connaissances ésotériques, même si elles n'ont pas de lien direct avec l'optimisation des bitcoins. Bien entendu, si la technique ne vous intéresse pas, oubliez les paragraphes de cette icône. La méconnaissance de leurs informations ne vous fera courir aucun risque.

## Et maintenant ?

---

Comme pour tous les livres de la collection pour les nuls, faites comme vous le sentez. En effet, chaque chapitre est indépendant des autres. De ce fait, pour éviter de répéter les mêmes informations, vous trouverez de nombreux renvois vers les chapitres qui traitent plus en détail d'un sujet évoqué.

Si vous ne savez pas où commencer, le bon ordre des choses vous guidera logiquement vers le premier chapitre de la première partie. Sinon, voici quelques suggestions :

- » Le [Chapitre 9](#) est un excellent point de départ, car il indique si la crypto-monnaie est utilisée légalement dans votre pays.
- » Si vous souhaitez foncer tête baissée et créer un portefeuille de bitcoins afin d'acquérir et de dépenser cette crypto-monnaie, allez directement au [Chapitre 5](#).

- » Vous pouvez également commencer au [Chapitre 10](#) qui communique des informations sur la sécurité et indique des précautions à prendre pour gérer sereinement les bitcoins.
- » Le [Chapitre 12](#) explique ce que vous pouvez faire avec un portefeuille de bitcoins, c'est-à-dire dépenser, dépenser, dépenser et... dépenser.

À vous de jouer ! Commencez au début si vous souhaitez aborder tranquillement le sujet des bitcoins. Nous espérons que vous prendrez autant de plaisir à lire ce livre que nous en avons eu à l'écrire.

# Les fondamentaux du bitcoin

## DANS CETTE PARTIE...

- » Se familiariser avec le concept de bitcoins, leur réalité, et leur fonctionnement.
- » Découvrir comment se procurer des bitcoins et où les stocker (ou pas).
- » Apprécier les avantages et les inconvénients d'une crypto-monnaie en tant que système monétaire et technologique.
- » Tout savoir sur l'exploitation, le financement, le négoce, et le gain des bitcoins.

# Chapitre 1

## Présentation du bitcoin

---

### DANS CE CHAPITRE

- » En connaître un peu plus sur le bitcoin
  - » Comprendre en quoi le bitcoin peut vous être profitable
  - » Rester prudent et économiser vos sous
- 

Donc... le bitcoin est une nouvelle forme d'argent – une monnaie électronique. Mais comment est-ce que cela fonctionne ? OK. Asseyez-vous confortablement, et commençons par les fondamentaux, c'est-à-dire les trois aspects du bitcoin :

- » **Origine** : D'où viennent les bitcoins.
- » **Technologie** : Comment cela fonctionne en coulisses.
- » **Monnaie** : Utiliser des bitcoins comme de l'argent.

Explorer chacun de ces aspects vous aidera à comprendre le bitcoin (ou BTC). Ne vous inquiétez pas. Dans un premier temps, nous allons rester à la surface de choses que nous approfondirons plus tard.

# L'origine du bitcoin

---

L'aspect le plus important du bitcoin est sans doute le concept qui le sous-tend. Cette crypto-monnaie a été créée par le développeur Satoshi Nakamoto. Plutôt que de concevoir une nouvelle méthode de paiement en ligne, Satoshi a constaté que les systèmes de paiement existant posaient des problèmes.

Le concept de bitcoin est simple à expliquer : pendant la crise financière de 2008, tout le monde a compris la fragilité économique du système. Encore aujourd'hui, beaucoup ressentent ces effets en termes de perte de valeur de leur monnaie fiduciaire.

Alors que le système financier global était au bord de la rupture, de nombreuses banques centrales s'engagèrent dans un assouplissement quantitatif – c'est-à-dire, pour faire simple, à faire tourner la planche à billets. Les banques centrales inondèrent les marchés de liquidités et de réductions des taux d'intérêt proches de zéro, dans le but d'éviter de revivre la Grande Dépression des années 1930. L'impact de ces décisions fut énorme, avec des fluctuations importantes sur les monnaies que l'on a appelées guerres des devises – une course à la dévaluation compétitive de telle sorte qu'une économie puisse devenir plus viable en réduisant le prix de ses

marchandises et de ses services par rapport à ses voisins et à la concurrence mondiale. La réponse des banques centrales resta dans la droite ligne de leur politique face à ce genre de situation : les gouvernements devaient renflouer les banques affectées, et imprimer des billets dévalorisant encore plus l'offre monétaire existante.

En renflouant les banques, il y eut un net transfert de la dette au Trésor public, qui se répercuterait inévitablement sur le contribuable. Ces techniques aboutirent à un grand sentiment d'injustice sociale. Parallèlement à cela, personne ne pouvait évaluer les effets à long terme de cet assouplissement quantitatif. Une inflation ? Une dévaluation ? Il paraissait cependant très clair que les banques centrales, supposées agir indépendamment des gouvernements, plongeraient de nombreuses économies dans l'inconnu, tout en se préparant à dévaluer leur monnaie juste pour panser les plaies. En procédant de la sorte, elles renflouèrent encore une fois les mêmes institutions et banques dont le comportement irresponsable était à l'origine de cette crise majeure.

La seule option « raisonnable » aurait été de laisser le système s'effondrer comme en Islande, qui s'est placée en défaut de paiement de sa dette, et a subi un bouleversement économique consécutif à cet

événement. C'est dans ce contexte qu'apparut la notion de bitcoin : un système financier décentralisé n'appartenant pas à l'élite des décideurs mondiaux.

Satoshi Nakamoto conclut qu'il était temps de mettre en œuvre un nouveau système monétaire très différent de l'infrastructure actuelle et pouvant devenir une force perturbatrice. L'idée sous-jacente était que le bitcoin pouvait remplacer cette infrastructure financière trouble, et cela malgré le fait que de nombreuses banques se penchent aujourd'hui sur la technologie qui gère le bitcoin. En effet, elles en mesurent le potentiel et envisagent de l'adopter pour leur propre usage. Elles sont tout à fait libres de procéder ainsi puisque le cœur de la technologie du bitcoin, appelée chaîne de blocs (voir le [Chapitre 7](#)), est open source, donc analysable et adaptable par tout un chacun.

Le bitcoin pourrait alors apparaître comme un moteur idéologique. Pourtant, c'est bien plus que le simple fait d'utiliser une monnaie associée comme nouveau moyen de paiement. Cette crypto-monnaie est davantage une manière d'utiliser sa technologie sous-jacente et de découvrir son potentiel dans le temps. De ce fait, la façon dont vous envisagez d'employer cette technologie ne dépend que de vous. Elle peut être adaptée à des besoins financiers spécifiques. Vous devez simplement rester ouvert à la technologie elle-même.



En effet, l'interaction qui existe entre la finance et la technologie se confronte à bien des problèmes. Nous avons tous été impactés par la crise bancaire du 21<sup>e</sup> siècle, et beaucoup de pays ont bien du mal à se remettre de ce fiasco financier. Le développeur du bitcoin, Satoshi Nakamoto, fut victime de ce manque de clairvoyance des banques centrales et réfléchit longtemps à une solution alternative. L'infrastructure financière dominante étant fragile, une nouvelle proposition viable semblait la bienvenue, qu'il s'agisse ou non du bitcoin.



L'idée du bitcoin développée par Satoshi Nakamoto était de lui faire jouer un rôle majeur : la décentralisation. Cela signifie que nous faisons tous partie de l'écosystème du bitcoin. De facto, nous y jouons un rôle actif à notre niveau. Plutôt que de nous en remettre à un gouvernement, une banque, ou à un intermédiaire, le bitcoin est la propriété de tous dans un système appelé peer-to-peer. Ainsi, nous sommes tous un maillon de la chaîne que constitue ce réseau. Sans utilisateur individuel, pas de bitcoins. Plus il y a de gens qui adoptent cette crypto-monnaie, mieux elle fonctionne. Le bitcoin a besoin d'une communauté en perpétuelle expansion qui l'utilise comme un moyen de paiement de marchandises et de services, ou bien qui les propose en échange de bitcoins.



L'esprit de liberté qui règne sur la monnaie électronique œuvre en faveur du développement d'activités qui acceptent le bitcoin comme monnaie d'échange. Ajoutez à cela que les affaires existantes peuvent offrir le bitcoin comme méthode de paiement alternative, s'ouvrant ainsi à des clients potentiels à l'échelle mondiale.

## Un peu de technique

Comme vous pouvez vous y attendre avec un système de paiement peer-to-peer, le moteur technologique du bitcoin est une force avec laquelle nous devons aujourd'hui compter. De nombreux domaines peuvent utiliser la chaîne de blocs du bitcoin comme un outil très puissant du secteur financier, car le bitcoin ne se limite pas à sa seule acception monétaire.



Le bitcoin présente des options technologiques sans précédent et des possibilités que nous ne pouvons imaginer il y a encore quelques années. Et bien d'autres implications sont encore à découvrir dans notre vie quotidienne, comme cela est expliqué au [Chapitre 3](#).



La technologie du bitcoin a été largement sous-estimée dans le passé et, pour être honnête, a connu une histoire mouvementée. Plusieurs plateformes furent créées afin de rendre le bitcoin plus accessible et

utilisable, mais sans forcément connaître de conclusion heureuse, notamment en matière de sécurité. De nouveaux outils comme celui-ci nécessitent un apprentissage pour chacun d'entre nous. Pour cette raison, le bitcoin a eu du mal à prendre son envol.

Le potentiel de cette crypto-monnaie concerne de nombreux aspects de la vie. Les précurseurs, venant du secteur financier, furent intrigués par l'aspect open ledger (livre ouvert) de cette technologie. Cela signifie que tout le monde peut voir, en temps réel, où se déroule chaque transaction financière du réseau. Bien que cela puisse paraître un peu effrayant, le fait de pouvoir contrôler cela est en fait particulièrement rassurant. Aucune de ces implémentations n'a besoin d'être liée aux finances en elles-mêmes, sachant qu'il existe de nombreuses voies à explorer dans ce secteur.



L'acceptation du bitcoin comme moyen de paiement impose l'exploration de nombreuses choses. Bien que l'intégration d'une option de paiement par bitcoins soit facile à mettre en place sur un site Web, il n'en va pas de même des cartes de paiement en magasin. Cependant, plusieurs organismes de paiements vous aideront volontiers à transformer vos transactions bitcoin en monnaie locale. Pour rendre cette transaction encore plus séduisante, les paiements s'effectuent sur votre compte bancaire le premier jour

ouvrable suivant la transaction, et non pas une semaine plus tard comme c'est le cas aujourd'hui avec les cartes de crédit. Enfin, sachez que les frais inhérents aux paiements par bitcoins sont plus faibles que ceux d'une carte bancaire.

## Le bitcoin comme outil monétaire

Plus il sera utilisé et plus le bitcoin sera appréhendé comme une monnaie. Comme vous l'imaginez, il est assez difficile de convaincre des magasins d'accepter le bitcoin au même titre que l'euro, tout comme il est compliqué de faire entrer dans l'esprit des gens que l'on peut aujourd'hui payer avec de l'argent électronique.

Pourtant, les avantages pour les commerçants sont très clairs : le bitcoin réduit considérablement les frais et d'autres coûts. Mais, si personne ne visite votre magasin parce que vous utilisez le bitcoin comme moyen de paiement, il n'y a aucun intérêt à l'utiliser. C'est donc au consommateur de prendre le train en marche.



Pour que le bitcoin devienne un véritable outil monétaire, vous pouvez mettre en œuvre des supports de paiements usuels :

- » des cartes bitcoin prépayées ;
- » des cartes de débit en bitcoins.

La carte rassure. Elle peut être approvisionnée en bitcoins – ou liée à un portefeuille de bitcoins existant (voir le [Chapitre 5](#)) – vous permettant de dépenser votre argent électronique partout où les cartes bancaires sont acceptées. Le commerçant paiera les frais comme pour une transaction par carte bancaire classique et il recevra le paiement en euros.

Le bitcoin est encore loin d'être un moyen de paiement principal. Les commerçants doivent être persuadés de sa nécessité. De notre côté, nous pensons que le moment est venu de convaincre le consommateur d'abandonner progressivement l'argent liquide et les cartes bancaires pour régler leurs achats avec des bitcoins via leurs périphériques mobiles. Cela ne va pas se produire du jour au lendemain. Par conséquent, l'utilisateur actuel de bitcoin doit être patient.

## Bitcoin et commerçants

En tant que commerçant, préparez-vous à accepter le bitcoin comme moyen de paiement en ligne ou en boutique. Vous n'aurez aucune modification à apporter à votre infrastructure actuelle. Vous avez simplement besoin d'une connexion à Internet.



Voici quelques avantages liés au bitcoin dans un commerce :

- » Vous réduisez les frais de transaction.
- » Les paiements en bitcoins peuvent être convertis en monnaie de votre choix, et les fonds sont déposés sur votre compte bancaire le premier jour ouvrable suivant la transaction. Si vous utilisez un bon organisme de paiement, on ne vous comptera qu'une petite marge de conversion. Comparez cela avec les transactions effectuées par cartes bancaires où vous attendez une semaine avant d'être crédité et avec un minimum de 3 à 5 % de frais.
- » Le bitcoin est une monnaie mondiale. Elle fonctionne de manière identique dans tous les pays. Où que vous alliez, le symbole bitcoin est le même partout.
- » La valeur du bitcoin est calculée jusqu'à la huitième décimale, contrairement à l'argent liquide qui n'est divisible qu'au centième, ou centime. Par exemple, en euros, vous allez payer 11,99 €. En bitcoin, vous paierez 11,98765432 BTC. Certes, cela ne paraît pas être un gain significatif, mais cette valeur augmentera exponentiellement dans les années à venir, ce qui permettra d'obtenir des prix plus précis dans le futur.
- » Accepter les paiements par bitcoins augmente le nombre de vos clients potentiels sur une échelle mondiale puisque le bitcoin est universel et ne

demande donc aucune conversion en fonction du pays d'utilisation.

- » L'échange direct de bitcoin à bitcoin permet de conserver une même valeur pendant la transaction, rien ne vous empêchant de procéder, plus tard, à une conversion dans la monnaie de votre choix.

## Bitcoin et consommateurs

En tant que consommateur, les avantages du bitcoin sont assez simples. Tout d'abord, vous n'avez plus besoin d'argent liquide pour acheter marchandises et services. Le liquide n'est pas très pratique. Il embarrasse votre portefeuille de billets de banque et autres pièces de monnaie, et représente une incitation à la dépense (ou bien c'est moi qui aie un problème). De plus, l'argent liquide peut être contrefait... eh oui ! les faux billets, ça existe.

Le bitcoin est une alternative viable et fiable pour payer des produits et des services avec votre compte bancaire ou des cartes de crédit et bancaires, pour les raisons suivantes :

- » Plutôt que de s'appuyer sur les services fournis par un établissement centralisé, comme une banque, le bitcoin permet d'effectuer un paiement n'importe quand et pour n'importe quoi, sans se soucier des heures ouvrables, des week-ends, et des vacances.



- » Les paiements en ligne sont immédiatement traités.
- » Le bitcoin est une monnaie électronique sans frontière, opérant identiquement en Europe, en Amérique du Nord, en Afrique, en Asie, en Amérique latine, et en Australie. N'importe quel habitant de cette planète peut utiliser le bitcoin pour payer ses achats.
- » De nombreux efforts sont faits pour booster l'utilisation du bitcoin par les commerçants, combinés à une nouvelle manière de dépenser des bitcoins (par exemple, comme vous le faites avec des cartes de crédit).

## **Le fonctionnement des bitcoins**

La crypto-monnaie change radicalement notre façon d'appréhender l'argent. Les crises financières ont rendu les gens si méfiants que certains envisagent de se tourner vers des solutions alternatives. Le bitcoin, avec sa transparence et sa décentralisation, semble disposer des atouts nécessaires à ce revirement d'idéologie.

D'abord, le bitcoin passe outre le système financier actuel, évitant de recourir ainsi aux services bancaires. Bien qu'en Occident il semble normal de posséder un compte en banque, la mentalité est totalement

différente en Afrique, par exemple, où entre 50 et 90 % de la population se passe des banques. Ces personnes sont-elles contraintes de ne pas ouvrir ce type de compte ? Pas du tout ! Nous oublions simplement que dans nos pays il semble obligatoire d'ouvrir pareil compte.

Depuis un certain temps, la société évolue vers un écosystème dépourvu d'espèces : de plus en plus de personnes utilisent un compte bancaire et des cartes de crédit pour régler leurs achats de biens et de services, que ce soit en ligne ou non. Les paiements par mobile se développent, marquant progressivement la fin des cartes bancaires. Depuis quelques années, les bitcoins sont utilisables avec des périphériques mobiles.



Nous commençons à comprendre le concept de chaîne de blocs et de ses futures implications. Une chaîne de blocs (voir le [Chapitre 7](#)) peut faire beaucoup de choses ; il suffit de trouver les bonnes pièces du puzzle et de les assembler.

Voici quelques exemples de ce qu'est capable d'accomplir la technologie du bitcoin (consultez le [Chapitre 3](#) pour plus de détails) :

- » Prendre en charge le *marché des transferts* (transfert de fonds entre deux parties) et décider de l'issue de chacun de ses aspects.

- » Envoyer de l'argent à l'autre bout du monde en quelques secondes.
- » Convertir de l'argent en n'importe quelle devise locale.
- » Se passer d'un compte en banque et ainsi faire du bitcoin un outil d'une incroyable puissance dans les régions du monde qui ne se basent pas uniquement sur des services bancaires.

Mais que se passe-t-il lorsque vous vivez dans une région sans banque et sans accès à Internet ? Il existe une solution : certains services permettent d'envoyer des messages vers n'importe quel numéro de téléphone pour utiliser des bitcoins ou toute autre monnaie électronique. Une fois encore, le bitcoin affirme sa toute-puissance, là où les services bancaires ne règnent pas en maîtres.

Mais, la démonstration la plus incroyable de la force du bitcoin est sans doute le réseau bitcoin lui-même. Toutes les transactions sont consignées et surveillées en temps réel, donnant aux utilisateurs un accès sans précédent aux données financières des quatre coins du monde. Mieux encore, la chaîne de blocs permet de suivre la source et la destination des paiements, même si l'argent se déplace en temps réel.

# Utilisation anonyme des bitcoins

---

L'anonymat de la monnaie électronique est une des notions les plus difficiles à comprendre. Le bitcoin est-il vraiment anonyme ? La réponse est assez simple : « non, pas totalement ». En effet, un certain niveau d'anonymat est associé à l'utilisation des bitcoins et des monnaies électroniques en général. Chaque fois que vous utilisez des bitcoins pour transférer des fonds, vous pouvez masquer votre identité derrière l'adresse de votre portefeuille de bitcoins (voir le [Chapitre 5](#) pour en savoir davantage sur la notion de portefeuille). Ces adresses sont composées d'une chaîne complexe de chiffres et de lettres (à la fois en majuscules et en minuscules) ne permettant pas de savoir qui vous êtes, et où vous êtes. De ce point de vue, le bitcoin offre un certain niveau de protection qu'aucun autre moyen de paiement ne vous procure.

Cependant, les adresses de portefeuille sont consignées dans un registre public – la chaîne de blocs – qui surveille tous les transferts entrants et sortants. Par exemple, si nous vous envoyons 0,01 BTC, n'importe qui dans le monde peut suivre le transfert de l'adresse du portefeuille A à celle du portefeuille B. Bien entendu, personne ne sait à qui appartiennent ces adresses, mais la transaction elle-même peut être connue de tous.



Une fois que quelqu'un connaît l'adresse publique de votre portefeuille, il peut la suivre sur le site Web [www.blockchain.info](http://www.blockchain.info). Il en voit alors les opérations présentes et passées. En conclusion, si une personne peut connaître l'adresse publique de votre portefeuille, il n'y a pas un total anonymat dans l'utilisation des bitcoins.

Ce scénario connaît quelques aménagements quand il s'agit d'échange de bitcoins (voir le [Chapitre 2](#)). En effet, lorsque vous vendez vos bitcoins, il devient difficile de connaître leur provenance.

## Anonymat tierce partie

Il existe plusieurs manières de garder son anonymat en matière de bitcoins. L'une d'entre elles est très conviviale. En général, nous avons tendance à croire que tous ceux qui souhaitent garder l'anonymat ont quelque chose à se reprocher. Par exemple, ils ne souhaitent pas payer des taxes, ou bien ils veulent acheter des marchandises ou des services interdits dans leur juridiction. En utilisant des services comme un portefeuille en ligne, vous pouvez répartir votre « argent » sur différentes adresses qui n'ont aucun lien les unes avec les autres. Le souci est qu'avec une telle pratique, si votre argent est perdu pendant la procédure de transfert, il n'y a aucun moyen de le

récupérer. Toutefois, ne vous inquiétez pas sur la perte de vos bitcoins. Nous expliquons, au [Chapitre 5](#), comment les gérer ainsi que votre portefeuille.



Posez-vous toujours la question de savoir s'il est ou non aussi important que cela d'utiliser vos BTC de manière anonyme ou pas.



L'un des plus gros problèmes de l'utilisation de services externes pour rendre vos transactions anonymes est que vous devez vous en remettre à un tiers. Or, la monnaie électronique est faite pour se passer des intermédiaires et ainsi donner tout pouvoir aux utilisateurs dans le contrôle de leurs transactions. Faire confiance à un tiers pour votre argent est antinomique avec l'idée du bitcoin. De plus, toute recherche d'anonymat crée des soupçons sur la nature de l'utilisation de cette monnaie. En réalité, dès lors que vous utilisez des bitcoins, vous bénéficiez d'une certaine forme d'anonymat puisque seule l'adresse publique du portefeuille est révélée. Le [Chapitre 5](#) présente les meilleures méthodes pour gérer vos fonds.

## Protection de la vie privée

Il est possible de protéger votre vie privée lorsque vous utilisez des bitcoins. Cela demande quelques efforts et

une planification :

- » Vous pouvez générer une nouvelle adresse pour chacune de vos transactions.
- » Vous pouvez éviter de poster votre adresse publique dans un lieu public.

## Générer un nouveau portefeuille

Lorsque vous recevez des fonds d'un nouvel utilisateur, vous pouvez leur assigner un portefeuille flambant neuf qui ne sera pas obligatoirement lié à des adresses existantes. Ce type d'adresse jetable permet d'isoler les transactions les unes des autres, protégeant ainsi votre anonymat.

Toutefois, selon la manière dont vous stockez vos fonds – c'est-à-dire le type de client bitcoin et le système d'exploitation que vous utilisez – vous pourrez changer d'adresses. Par exemple, si vous installez le client Bitcoin Core sur votre ordinateur de bureau ou portable, vous pouvez créer une nouvelle adresse chaque fois que vous envoyez des fonds à quelqu'un.



Un changement d'adresse survient dès que vous avez une certaine quantité de bitcoins vers un portefeuille et que vous en envoyez moins que la valeur totale en votre possession. Par exemple, vous avez 3 bitcoins et voulez en dépenser 0,25. Vous souhaitez légitimement que



l'on vous rende la « monnaie », c'est-à-dire 2,75 bitcoins, dans votre portefeuille. Le client Bitcoin Core (ainsi que d'autres clients de bureau) permet d'envoyer cette monnaie vers une nouvelle adresse. Ainsi, il n'existe plus de lien direct entre votre adresse source et la nouvelle, et cela même si vous suivez pas à pas la transaction via la chaîne de blocs.

## **Garder l'adresse de votre portefeuille secrète**

Une autre manière de protéger votre vie privée consiste à ne pas publier l'adresse de votre portefeuille dans un espace public. En effet, si vous utilisez l'adresse de votre site Web, blog, réseau social, ou forum, vous portez atteinte à l'anonymat tant recherché. Une fois que quelqu'un aura découvert l'adresse de votre portefeuille, il pourra facilement remonter jusqu'à vous. Pour cette raison, mettez en œuvre une autre méthode.

## **La fongibilité du bitcoin**

Le plus gros problème du bitcoin est sa fongibilité ou, pour être plus précis, son intangibilité. Fongibilité n'a rien à voir avec les champignons. Il s'agit d'un terme employé pour les produits interchangeables ou

auxquels on peut en substituer d'autres... exactement comme les bitcoins.

La plupart des gouvernements du monde contrôlent le système d'émission de la monnaie. Ainsi, les devises locales sont centralisées et gérées par une banque centrale. Si l'état a besoin de plus d'argent, la banque centrale en émet à la demande en faisant tourner la planche à billets ou en engageant un assouplissement quantitatif.

Donc, par ordre d'un gouvernement ou en toute indépendance, une banque centrale peut instiller des liquidités dans l'économie en réalisant un assouplissement quantitatif. Eh bien sachez que ce n'est pas le cas avec les bitcoins. En effet, les liquidités sont fixées à 21 millions, signifiant que le bitcoin n'est pas fongible, comme les autres monnaies fiduciaires.

## Croire dans le bitcoin

---

Toute nouvelle technologie se heurte à la méfiance des utilisateurs. Dans le cas du bitcoin, vous devez être capable de faire confiance aux deux versants de son utilisation. Le vôtre ne pose pas de souci puisque vous êtes le maître absolu de vos finances. En revanche, avez-vous confiance dans l'argent des autres, et

surtout, croyez-vous que cette monnaie électronique va régner sous peu sur le monde ?



Les chances de voir disparaître le bitcoin sont si minces que vous n'avez vraiment pas de quoi vous inquiéter. Toutefois, s'il y a bien une chose que la vie nous apprend, c'est que nous ne pouvons avoir aucune certitude dans l'existence. Sachez cependant que le réseau du bitcoin est constitué de nombreux utilisateurs individuels, mais aussi de nœuds bitcoin, qui assurent l'activité permanente du réseau. Vous en saurez davantage sur les nœuds au [Chapitre 6](#).

Cela nous amène à un concept du bitcoin auquel les gens font difficilement confiance : la décentralisation. Comme nous l'avons expliqué, le bitcoin est une monnaie électronique décentralisée, c'est-à-dire qu'il n'y a aucun point névralgique de défaillance pouvant conduire à une impossibilité de restaurer le réseau du bitcoin. En effet, chaque individu fait partie intégrante de cet écosystème. Il est donc presque impossible qu'une série de comportements individuels nuisent à l'équilibre du groupe.

Vous pouvez comparer la décentralisation du bitcoin au fonctionnement du moteur de recherche Google. Le moteur en lui-même est sollicité simultanément par des millions d'utilisateurs. Pourtant, il ne semble jamais ralentir. Pourquoi ? Parce que ce moteur de

recherche s'exécute sur un grand nombre de serveurs – de manière décentralisée – le rendant ainsi très difficile à mettre à genoux.

Mais la décentralisation induit une autre méfiance. Comme le réseau est fait d'une multitude d'individus, aucune autorité centrale n'est là pour gérer les comportements sur le réseau. Cela signifie que si vous possédez des bitcoins et que quelque chose tourne mal pour une raison inconnue, qui va vous rembourser ?! Une fois que vos BTC s'en sont allés – parce que vous les avez dépensés ou parce qu'ils ont été perdus – il n'y a aucune chance de les récupérer.

## Faire confiance dans la technologie du bitcoin

La nature humaine nous apprend à faire les choses telles qu'elles ont toujours été faites. Oui, mais voilà, les comportements changent. Quand Internet arriva au début des années 1990, de nombreuses personnes ne crurent pas un seul instant à son développement. Pour beaucoup, il s'agissait d'un amusement entre geeks. Où en est Internet aujourd'hui ? Tout le monde, de vos grands-parents à leurs animaux domestiques, est sur Internet. Que ferions-nous sans lui ?! Il suffit que notre connexion soit coupée ne serait-ce que quelques

minutes pour avoir l'impression d'être dépossédé du monde.

Le bitcoin est souvent comparé aux débuts d'Internet, c'est-à-dire une nouvelle technologie dérangement qui semble un peu trop en avance sur son temps. C'est en partie vrai. Le bitcoin résout un problème technologique auquel la plupart des gens n'auraient jamais pensé. Et ce n'est pas parce que le bitcoin n'apparaît pas comme une évidence, mais simplement parce que l'homme rejette les changements de ses habitudes. En d'autres termes : « ça fonctionne bien comme ça ».

De ce fait, comme pour Internet, le bitcoin mettra du temps à devenir indispensable, même si de nombreux projets et plateformes se développent autour de cette monnaie électronique. Le grand public, quant à lui, n'est pas prêt. Il faudra faire un effort d'informations pour exposer clairement les enjeux du bitcoin et la fiabilité de sa technologie, plutôt que de le présenter immédiatement comme une « monnaie alternative ».

Il existe en revanche de nombreuses personnes qui font confiance à la technologie du bitcoin. La plupart des technologies actuelles se focalisent sur un aspect financier, comme le marché des transferts. La technologie du bitcoin permet d'envoyer de l'argent à n'importe qui dans le monde, et à moindres frais. De ce

fait, les acteurs des transferts de fonds comme Western Union, Moneygram, et même les banques traditionnelles, devront faire face à la concurrence de cette « monnaie de singe », comme on appelle souvent le bitcoin.



Il n'y a que vous qui puissiez accorder votre confiance au bitcoin. Le Bitcoin fut, est, et sera toujours conçu pour vous donner les pleins pouvoirs sur votre argent. Si vous vous sentez prêt à ouvrir vos bras à cette liberté, poursuivez votre lecture. Nous pensons que le jeu en vaut la chandelle.

## Faire confiance au bitcoin en tant que monnaie

Comme nous venons de le voir, il semble difficile d'accepter que le bitcoin puisse remplacer l'euro (ou autre). En revanche, le présenter comme une technique alternative de paiement semble plus adéquat. Ainsi, vous achetez et vendez des services et des produits en échange de bitcoins. Un peu comme votre carte bancaire est détachée du sens premier de la « monnaie fiduciaire ». En effet, vous payez sans voir passer l'argent de mains en mains.

C'est sans doute pour cela que certains commerçants font confiance au bitcoin comme moyen de paiement,

parallèlement aux systèmes traditionnels. En voici les raisons :

- » Pas de frais supplémentaires pour les paiements effectués en bitcoins.
- » Aucune infrastructure spéciale à développer.

En tant que commerçant, vous pouvez intégrer le paiement avec des bitcoins aussi bien dans vos boutiques que sur Internet. Dans tous les cas, il est possible de convertir immédiatement des bitcoins en monnaie locale, et d'avoir les fonds en banque le jour ouvrable suivant l'opération.

Du point de vue du consommateur, utiliser le bitcoin comme moyen de paiement signifie que vous n'avez pas besoin de retirer de l'argent, d'utiliser une carte bancaire ou de crédit liée à un compte en banque. Cependant, pour commencer avec des bitcoins, il faudra en acheter, c'est-à-dire dépenser votre argent actuel. N'ayez aucune crainte. Il existe d'autres manières de gagner des bitcoins sans dépenser vos euros, comme l'explique le [Chapitre 4](#).



Le bitcoin est avant tout une manière de donner aux individus le contrôle de leur argent électronique. Il est disponible à tout moment, quelle que soit la somme. Pourtant, cette liberté fait peur aux gens puisque, depuis quasiment un siècle, ce sont les banques qui en



ont la responsabilité. Alors, très honnêtement, si vous ne souhaitez pas passer du temps à gérer votre argent quand vous le souhaitez et où vous le souhaitez, le bitcoin n'est pas fait pour vous.

En revanche, si vous pensez que vous engraissez le système financier actuel et les banques, le bitcoin est fait pour vous. Personne n'essaie de vous faire croire que le bitcoin va remplacer l'argent local que vous utilisez depuis votre naissance. Il faut simplement comprendre que les deux systèmes peuvent coexister pacifiquement. Toutefois, dès que vous commencerez à voir les avantages et le potentiel du bitcoin pour différentes opérations, vous sentirez monter en vous une grande excitation, et plus important encore, une immense sensation de liberté financière.

## Chapitre 2

# Acheter et stocker des bitcoins

---

### DANS CE CHAPITRE

- » Comment acheter des bitcoins
  - » Trouver un bureau de change
  - » Sécuriser votre monnaie électronique
- 

Ce chapitre vous apprend à débiter dans l'univers du bitcoin : l'importance de votre premier achat, adopter une technique de stockage et de dépense et, bien entendu, calmer votre fièvre acheteuse.

À la fin de ce chapitre, vous devriez être capable de gérer des bitcoins.

Avant de commencer, vous avez besoin d'un ou des deux éléments suivants :

- » Un logiciel portefeuille bitcoin (ou porte-monnaie si cela vous parle mieux) installé sur votre ordinateur. Vous en trouverez un certain nombre à l'adresse <https://bitcoin.org/fr/choisir-votre-porte-monnaie>.

- » Ce même logiciel installé sur un appareil mobile et que vous trouverez à la même adresse.

## Bien commencer : Comment acquérir des bitcoins

---

Pour utiliser cette crypto-monnaie, vous devez en acquérir des unités. Bien qu'il existe plusieurs méthodes pour y parvenir, la plus simple consiste à en acheter.

Comment acheter une monnaie électronique avec de l'argent physique ? Il existe un grand nombre de plateformes de change qui agissent comme les bureaux de change traditionnels où vous échangez des euros contre une monnaie étrangère, et réciproquement.



Une plateforme de change propose des services financiers équivalents à ceux des banques traditionnelles ou d'institutions officiant sur le marché des changes – comme le FOREX.

Vous pouvez posséder un compte auprès de l'organisme qui gère votre argent local, et utiliser ce compte pour gérer des bitcoins. Ainsi, vous enverrez des bitcoins à votre portefeuille préféré, puis les utiliserez comme bon vous semble. Finalement, rien de très différent de

vosre argent liquide qui est prélevé sur votre compte-chèques.

N'oubliez pas que le bitcoin a été conçu pour fonctionner sans frontière, sous la forme d'un système de paiement décentralisé ne nécessitant aucune conversion en monnaie locale. Mais bien que de nombreux produits et services puissent être payés en bitcoin, la nécessité de convertir des BTC en devise locale pour régler une facture reste possible. C'est pour cette raison que nous avons besoin de plateformes de change qui facilitent cette opération.

## S'enregistrer sur une plateforme de change

Une plateforme de change prend la forme d'un site Web. Il existe aussi quelques lieux physiques dont nous traiterons plus loin dans ce chapitre. Vous trouverez également de nombreux fournisseurs de bitcoins. En fonction de votre lieu géographique et de votre devise, certaines plateformes sont préférables à d'autres. À cause de considérations légales, il n'existe pas à ce jour une structure de change adaptée à tous les pays. Nous vous conseillons de consulter la liste de ces plateformes sur le site [bitcoin.org](https://bitcoin.org) ou des sites sur l'actualité du bitcoin comme [bitcoin-france.fr](https://bitcoin-france.fr), [TheBitcoin.fr](https://TheBitcoin.fr), ou Coindesk (pour les anglophiles).

Vous pouvez également visiter les sites suivants :

[www.plus500.fr](http://www.plus500.fr)

[www.coindesk.com/category/companies/exchanges/](http://www.coindesk.com/category/companies/exchanges/)

[www.coursbitcoin.fr/actualit%C3%A9-cours-bitcoin.html](http://www.coursbitcoin.fr/actualit%C3%A9-cours-bitcoin.html)



L'objectif principal de toute plateforme de change est de faciliter le transfert d'une crypto-monnaie de et vers une monnaie physique.

Tout le monde peut créer un compte auprès d'une de ces plateformes sans être contraint d'acheter des bitcoins ou d'en posséder.

Bien qu'elle puisse varier d'une plateforme à une autre, voici la procédure générique en ligne d'un échange de bitcoins :

- 1. Vous ouvrez un compte en donnant quelques informations sommaires.**
- 2. Vous recevez un mail d'activation de votre compte.**
- 3. Une fois le compte activé, la procédure d'enregistrement commence.**



Comme vous pouvez l'attendre d'un bureau de change, il existe des indicateurs majeurs sur le cours du bitcoin. Dans le cas du change, les prix peuvent fluctuer sensiblement comme dans n'importe quel autre

domaine commercial. Certaines plateformes de change vous donneront moins sur les ventes de bitcoins que le cours réel affiché.

D'autres plateformes vous paieront au cours du jour, mais avec une commission de 0,05 à 0,5 % par transaction. Même si le bitcoin fonctionne sur le principe de l'offre et de la demande sur un marché ouvert, acheteurs et vendeurs doivent être mis en relation. La plupart des plateformes de change utilisent un moteur d'échange. Il identifie automatiquement les acheteurs et les vendeurs. Cependant, il existe d'autres options, comme les échanges peer-to-peer locaux étudiés plus loin dans ce chapitre.

Un aspect très important de la gestion des bitcoins est qu'une grande majorité de plateformes changent vos BTC en une monnaie qui n'est pas obligatoirement celle de votre pays. Par exemple, si vous vivez en Chine, votre devise locale est le yuan chinois. Eh bien, vous pouvez tout à fait échanger vos bitcoins pour des euros (EUR), des dollars US (USD), ou des livres anglaises (GBP).



Lorsque vous essayez de faire un retrait sur votre compte bancaire, la valeur peut être convertie en monnaie locale si la banque n'accepte pas les transferts d'argent à l'étranger. Par conséquent, renseignez-vous avant d'effectuer ces types de transfert et soyez préparé

à subir les risques associés à ce genre d'opération.

Les plateformes d'échange sont contraintes, par des lois locales et les régulateurs des services et produits financiers de leur pays, de vous demander des informations personnelles. Elles concernent généralement votre identité, votre adresse, numéro de téléphone (fixe et/ou mobile), et votre pays de résidence. Certaines plateformes demandent votre date de naissance qui fait partie du processus de vérification de votre identité (voir la prochaine section).

## **Vérifier vos parties prenantes : passer l'étape du KYC**

Pour utiliser une plateforme d'échange sans restriction, vous devez subir l'épreuve du KYC (Know Your Customer – ou vérifier vos parties prenantes en français). Cette procédure est bien moins effrayante qu'elle n'y paraît, même si vous devez communiquer des informations très personnelles.

### **Étape 1 : Confirmer votre numéro de téléphone**

La première étape consiste à vérifier votre numéro de téléphone portable. La plupart des plateformes de change de bitcoins vous envoient un code par SMS que

vous devez reporter sur une page spécifique pendant cette procédure de vérification. Ainsi, la plateforme s'assure que vous êtes facilement joignable en cas d'urgence, ou pour récupérer le mot de passe de votre compte.

## Étape 2 : Obtenir un ID personnel

L'étape suivante consiste à vérifier votre identité en fournissant copie d'une pièce d'identité. En fonction de la plateforme utilisée, ces documents vont de la carte d'identité au passeport en passant par le permis de conduire, voire une facture récente, ou bien encore un certificat de naissance.

Ces pièces et leur nombre dépendent du volume de bitcoins que vous souhaitez échanger. Plus ce volume est important, et plus la vérification est stricte, exigeant des informations personnelles encore plus... personnelles. Cette vérification inquiète les utilisateurs débutants. De plus, il faudra attendre entre quelques heures et jusqu'à une semaine que les pièces et les informations soient validées avant de pouvoir vous procurer des bitcoins.



Chaque fois que vous soumettez des documents, vérifiez qu'ils sont bien lisibles afin de ne pas ralentir la procédure de vérification.



## Connaître les taux de change

Le taux de change du bitcoin varie en fonction du cours de la monnaie locale. Il existe aussi de grosses différences d'une plateforme d'échange à une autre.

Le business de ce secteur d'activité est de nature très concurrentielle. Chaque plateforme cherche à attirer le plus de clients possible. Chacune propose donc un modèle commercial propre pour séduire le plus grand nombre. Bien entendu, ce sont parmi les novices qu'il y a un marché juteux, et auprès de qui il faut faciliter l'accès au bitcoin.



Pour obtenir le taux de change le plus attractif, suivez ces quelques conseils :

- » Chaque fois que vous cherchez à changer des bitcoins contre de l'argent physique et inversement, commencez par vérifier le cours du jour. Pour plus de détails, lisez l'encadré « Garder un œil sur le taux de change ». Pendant des années, le prix du bitcoin est resté fixe, supposant alors que vos transactions s'effectueraient en quelques minutes. Par exemple, un utilisateur effectuait le transfert dans les 15 minutes suivant l'achat ou la vente, ce qui permettait de garantir un prix fixe. Tout manquement à ce comportement aurait entraîné une différence de prix à la hausse ou à la baisse.

- » Gardez un œil attentif sur le taux de change du bitcoin vis-à-vis de votre monnaie locale afin de maximiser les profits et réduire les pertes. Le site [Bitcoinwisdom.com](https://bitcoinwisdom.com) est une de nos sources préférées en la matière. Toutefois, il en existe d'autres comme [bitcoin.fr](https://bitcoin.fr), [Crypthead.com](https://Crypthead.com), [Coinmarketcap.com](https://Coinmarketcap.com), ou encore [Investing.com](https://Investing.com). Quelle que soit l'unité que vous choisirez, vous trouverez l'information qui vous convient, et apprécierez l'équivalent dans votre devise. Rendez-vous sur les sites suivants :

<https://bitcoin.fr/Cours-du-bitcoin/>

<https://bitcoinwisdom.com>

<https://cryptrader.com>

<http://coinmarketcap.com/currencies/>

<https://fr.investing.com/currencies/btc-eur>

- » Gardez à l'esprit qu'il y a des frais sur ces transactions. Donc, évaluez-les correctement avant de vous engager. Certaines plateformes d'échange de bitcoins se rétribuent au moment où vous passez l'ordre d'achat ou de vente, tandis que d'autres prennent une commission. Des frais supplémentaires peuvent s'appliquer lorsque vous effectuez un retrait de votre argent physique à la banque ou avec d'autres moyens de paiement.

## GARDER UN ŒIL SUR LE TAUX DE CHANGE

En fonction de la plateforme choisie, plusieurs méthodes de surveillance des taux vous sont offertes. Depuis votre ordinateur, nous conseillons le site Bitcoin Wisdom à [www.bitcoinwisdom.com](http://www.bitcoinwisdom.com). Vous y apprécierez en temps réel les variations du bitcoin dans la majorité des devises les plus importantes (USD, EUR, CAD, RUR, et CNY).

Pour les utilisateurs de smartphone, le scénario est légèrement différent. La plupart des portefeuilles mobiles affichent la valeur monétaire à côté de la valeur du bitcoin dans l'application elle-même (voir le [Chapitre 5](#) pour plus de détails à ce sujet). Cela permet d'avoir une idée du prix de votre crypto-monnaie à un moment donné. N'oubliez pas que vous avez besoin d'une connexion Internet active – soit en données mobiles, soit en Wi-Fi – si vous voulez que le prix affiché reflète la valeur en cours.



Les taux de change du bitcoin fluctuent constamment en réaction immédiate à l'offre et à la demande. Ces dernières années, le volume des transactions du bitcoin a augmenté exponentiellement, avec des hausses importantes sur le marché chinois et américain. Malgré cela, d'autres taux de change locaux dans le monde montent lorsque les marchés majeurs du bitcoin baissent, ou l'inverse.

## Comparer le peer-to-peer et les

## plateformes d'échange

Il existe deux types d'échange : le peer-to-peer et les plateformes régulières.

D'un côté, nous avons donc les plateformes d'échange de bitcoins qui passent les ordres d'achat et de vente des utilisateurs. Cependant, ni l'acheteur ni le vendeur n'ont la moindre idée de l'identité de l'autre partie dans l'opération. Cela donne à tous les utilisateurs un certain niveau d'anonymat, donc de protection de la vie privée. Nous avons ici l'utilisation la plus répandue de l'échange de la monnaie locale en bitcoins.

Cependant, le bitcoin a été créé pour favoriser les transactions peer-to-peer. Contrairement aux autres technologies peer-to-peer, comme les applications torrent, le peer-to-peer dans le domaine du bitcoin signifie une relation un à un (un face-à-face en quelque sorte). Une transaction peer-to-peer signifie que vous interagissez avec des données appartenant à une personne ou à une entité, et non pas avec plusieurs pairs en même temps, comme dans le cas des torrents. L'information dont vous disposez sur cette personne peut aller de l'adresse de son portefeuille bitcoin, à son nom d'utilisateur sur un forum, son lieu géographique, son adresse IP, voire se rencontrer réellement.



Ici, plutôt que de donner des ordres d'achat et de vente, vous traitez directement avec l'acheteur ou le vendeur qui détient les fonds.

Par exemple, vous souhaitez acheter un bitcoin à une personne qui vit dans votre ville. Plutôt que de passer par une plateforme d'échange, mettez en place un transfert peer-to-peer avec cette personne. Il existe des structures qui permettent de créer un compte dans le but de mettre en relation des personnes d'une même zone géographique. C'est le cas de [Gemini.com](https://gemini.com) pour le marché US, ou bien encore [Bitstamp.net](http://www.bitstamp.net) et [Kraken.com](https://kraken.com) pour les marchés internationaux. Visitez-les ici :

<https://gemini.com>

[www.bitstamp.net](http://www.bitstamp.net)

<https://kraken.com>



Tout le monde n'a pas envie de se rencontrer dans la réalité. Beaucoup préfèrent un paiement effectué de manière très standard, comme un virement bancaire ou un transfert PayPal.

En fonction de votre expérience, et dans l'idéologie du bitcoin, le peer-to-peer répondra mieux à vos besoins qu'un échange traditionnel. En règle générale, le peer-to-peer n'exige aucune information sur votre identité et permet de suivre l'historique de vos transactions et

celles des autres utilisateurs. Ainsi, vos chances de réussir cet échange augmentent.



Un des aspects les plus intéressants des échanges bitcoin peer-to-peer est leur discrétion. Comme vous traitez directement avec d'autres personnes, les fonds ne sont pas surveillés par les responsables de la plateforme. Il faut simplement que vous tentiez d'en savoir davantage sur les opérations antérieures de votre interlocuteur.

## Stocker vos bitcoins : sécuriser les échanges

---

La sécurité est l'une des considérations les plus importantes en matière de stockage des bitcoins sur une plateforme de change.

Nous savons que l'idéologie du bitcoin va à l'encontre des systèmes centralisés et des intermédiaires. Mais, bien que les échanges des crypto-monnaies soient décentralisés, les plateformes elles-mêmes, comme des banques, restent des points centraux vulnérables. Cela étant dit, les développeurs du bitcoin n'ont pas les deux pieds dans le même sabot – voir l'encadré « Les gardiens du coffre » pour plus d'informations sur la protection de votre argent virtuel.



Malheureusement pour les utilisateurs de bitcoins à travers le monde, les échanges de cette crypto-monnaie ne sont pas réputés pour leur sécurité. De ce fait, dès qu'une opération est piratée, ou que certains disparaissent avec l'argent, on ne peut plus faire grand-chose, sauf intenter une action en justice en espérant que des investigations seront menées. Bref, on peut toujours rêver. Lorsque vous mettez votre argent en banque, vous êtes protégé par des assurances. En France, le Fonds de Garantie des Dépôts et des Résolutions (FGDR) rembourse jusqu'à 100 000 euros. Ce n'est pas le cas pour le bitcoin.

En stockant vos bitcoins sur une plateforme d'échange, vous n'avez aucune garantie que son activité durera ad vitam aeternam. Il y a peu de risque qu'elle disparaisse, mais sait-on jamais. De plus, êtes-vous certain que cette structure soit suffisamment bien protégée contre des cyberattaques ? Ainsi, vous accordez votre confiance – et vos sous – à une plateforme qui clame haut et fort qu'elle a mis en place des mesures de sécurité draconiennes pour protéger vos données et votre argent.

Heureusement, ces dernières années, les échanges de crypto-monnaie ont vu leur sécurité s'intensifier. Il a fallu du temps avant de comprendre les failles de ce

nouveau système d'échange et adopter les mesures sécuritaires qui s'imposaient.

Aujourd'hui, les échanges sont bien plus sécurisés qu'en 2010, et les possesseurs de bitcoins disposent de plusieurs options pour assurer la sécurité de leurs BTC dans un environnement décentralisé. Cela étant dit, des portefeuilles décentralisés comme en propose [Blockchain.info](https://blockchain.info) ou [Coinbase.com](https://coinbase.com) représentent des solutions mobiles très populaires.

## LES GARDIENS DU COFFRE

Dans le livre blanc original de Satoshi Nakamoto (<https://bitcoin.org/bitcoin.pdf> ou en français ici <https://pt.slideshare.net/nabilbouzerna/bitcoin-a-peertopeer-electronic-cash-system-tra-duction-fr>), vous trouverez des détails sur la technologie du bitcoin et l'amélioration de sa sécurité comparées aux infrastructures bancaires actuelles. Il faudra encore un peu de temps avant de parvenir à une sécurisation équivalente. Par exemple, un outil comme la multisignature n'a été implémenté qu'en 2013.

Dans l'univers du bitcoin, ce système est identique à celui des établissements bancaires. Plutôt que de faire confiance à une seule personne ou entité dans l'accès à un portefeuille, plusieurs « clés » sont données à diverses parties.

Par exemple, Marc et Alice veulent ouvrir un portefeuille joint. Ils décident de donner à Dave, un « arbitre » neutre, une clé privée.



Pendant la procédure de création de ce portefeuille (ou portemonnaie), un total de trois clés privées sont générées : une pour Marc, une pour Alice, et la dernière pour Dave. Si Marc ou Alice veulent, individuellement ou à deux, effectuer une transaction, il leur faudra convaincre Dave du bienfait de cette opération.

Vous comprenez que, pratiquement, une multisignature bitcoin sur un portefeuille signifie que plusieurs parties doivent être d'accord sur le bien-fondé d'une action. Dans ce cas, Marc et Alice, Alice et Dave, ou Marc et Dave doivent tomber d'accord avant de pouvoir utiliser ce portefeuille. Si l'un d'eux souhaite effectuer une transaction et que les deux autres refusent, l'opération ne pourra pas aboutir.

Vous trouverez des informations sur <https://en.bitcoin.it/wiki/Multisignature> et en français à <https://www.ethereum-france.com/comprendre-la-blockchain-ethereum-article-1-bitcoin-premiere-implementation-de-la-blockchain-12/>.

Cela étant dit, comme il n'est pas facile de protéger une plateforme financière, celles des bitcoins ne font pas exception à ce problème. De plus, cela représente un coût en audit, tests de nouvelles fonctionnalités, et bien d'autres choses encore. En effet, la sécurité et la surveillance doivent se faire 24 heures sur 24 et 7 jours sur 7.

Une autre mesure de sécurité des échanges de bitcoins s'appelle le facteur d'authentification. Bien que facultative, nous conseillons aux possesseurs de bitcoins de mettre en place cette

fonction 2FA sur leur portefeuille. (Vous en saurez davantage à ce sujet un peu plus loin dans ce chapitre.)

Les échanges de bitcoins ont commencé par instaurer la multisignature. Si un pirate viole l'intimité d'un échange de bitcoins, le transfert de fonds devient quasiment impossible, exactement comme si un des codétenteurs de clé privée refusait l'opération. Toutefois, tous les portefeuilles ne bénéficient pas de la multisignature (voir plus loin dans ce chapitre).



Tout cela pour vous dire que le stockage à long terme de bitcoins sur une plateforme de change n'est pas très sécurisé. Toutefois, si vous envisagez de dépenser ou de transférer cet argent dans les prochaines 48 heures, vous ne risquez pas grand-chose. En revanche, dès que le stockage se prolonge, les risques augmentent.



Le meilleur moyen de stocker vos bitcoins est d'utiliser un portefeuille que vous contrôlez vous-même, que ce soit sur ordinateur ou un périphérique mobile. Pour plus de détails à ce sujet, consultez le [Chapitre 5](#).



Le bitcoin a été conçu pour donner les pleins pouvoirs à l'utilisateur final, donc sans donner ses fonds à gérer à un tiers. Par conséquent, transférez vos fonds d'une plateforme d'échange ou d'un portefeuille en ligne à un logiciel de portefeuille sur un ordinateur ou un appareil mobile aussitôt que possible.

## Utiliser une double authentification (2FA)

Même si vous envisagez de stocker vos bitcoins sur une plateforme d'échange pendant une assez longue période, vous devez chercher à protéger vos comptes. La plupart des services en ligne (non dédiés au bitcoin) exigent une authentification des utilisateurs basée sur un nom d'utilisateur et un mot de passe. On ne peut pas dire qu'il s'agisse là d'un système très sûr pour protéger vos informations personnelles.

Ces dernières années, il est apparu évident qu'il fallait implémenter davantage de couches de sécurité au sommet des protocoles d'authentification standard. L'une des solutions les plus populaires s'appelle double authentification (2FA) ou authentification à deux niveaux qui exige qu'un « jeton » supplémentaire soit utilisé pour accéder à votre compte. En cas d'erreur de combinaison, un message apparaît.

Il n'est pas rare qu'un tiers non autorisé accède à votre nom d'utilisateur et à votre mot de passe. Ce n'est pas toujours de votre faute, mais bel et bien de certains services en ligne dont les méthodes de sécurisation du stockage de ces informations laissent à désirer. Avec une double authentification, vous augmentez la sécurisation de vos données et de votre argent.

La 2FA peut être utilisée de plusieurs manières, qui ne sont pas toutes prises en charge par les plateformes de change. La méthode 2FA la plus répandue est Google Authenticator. Il s'agit d'une application que vous installez sur un périphérique mobile ou sur un PC. Son utilisation est très simple. Une fois téléchargée et installée sur votre téléphone par exemple, configurez un nouveau compte :

- 1. Connectez-vous au service ou à la plateforme qui doit bénéficier de la protection 2FA.**
- 2. Scannez le code QR associé à l'aide de l'appareil photo du mobile.**
- 3. Utilisez ce code QR pour lier vos éléments d'authentification et les apparier au téléphone.**



Chaque fois que vous ouvrez Google Authenticator, un nouveau code 2FA est généré pour votre compte. Ce type de code reste valide un temps assez bref, après quoi un nouveau code est automatiquement généré. La validité de ce code est automatiquement vérifiée lorsque vous vous connectez. Si vous entrez un code expiré, vous revenez à l'écran de connexion.

Même si la 2FA mobile paraît très pratique, il existe quelques inconvénients à garder à l'esprit :

- » Vous devez toujours avoir votre appareil mobile à portée de mains avec la batterie bien chargée afin de

générer quand il le faut le code 2FA.

- » Si vous perdez votre téléphone ou que vous vous le faites voler, vous perdrez également vos identifiants 2FA. Il est possible de désactiver la sécurité 2FA d'un compte pour l'activer sur un nouveau périphérique en cas d'extrême nécessité.

D'autres méthodes d'authentification 2FA de votre compte incluent des services comme Clef et Authy que vous trouverez sur le service de téléchargement d'applications de votre mobile, avec vérification par SMS. À l'exception de cette vérification par SMS, les autres exigent un matériel supplémentaire pour contrôler vos identifiants. De facto, ils sont moins pratiques.

La vérification par SMS a aussi ses inconvénients. Par exemple, comment faire lorsque vous êtes dans une zone sans réseau ? Lorsque vous voyagez dans un pays étranger, des frais supplémentaires peuvent être facturés à la réception de chacun des codes d'authentification 2FA.



Quelle que soit l'option que vous choisissiez, activez rapidement une authentification 2FA pour vos échanges de bitcoins. Cette technique protégera correctement votre compte, même si elle présente quelques inconvénients pratiques par moment.

# Comprendre la responsabilité

Le sujet de responsabilité dans les échanges de bitcoins est une zone un peu floue. Nous allons faire tout notre possible pour bien l'expliquer.



Le bitcoin est une monnaie électronique non réglementée qui fait tomber tous ses services dans la même catégorie par défaut. Cependant, en fonction de la partie du monde où vous utilisez une plateforme de change, vous devez accepter certaines réglementations.



Au moment de la rédaction de ce livre, il est bien difficile de savoir quelle responsabilité est engagée en cas de piratage d'une transaction ou d'arrêt d'activité soudaine de la plateforme. La plupart des structures les plus importantes et bénéficiant d'une grosse notoriété ont mis en place des systèmes qui vous protègent contre tout risque financier dans les limites d'un certain volume d'argent. L'idée est que si l'échange est violé, ou que les fonds sont perdus alors qu'ils sont stockés sur une plateforme de change, l'échange sera remboursé à ses frais. Cela étant dit, nous vous conseillons d'adopter une approche responsable en ne stockant vos bitcoins que sur des plateformes de change répondant à vos besoins de transactions, sans les considérer comme des structures hyper sécurisées. La prudence est donc de mise.

Certains économistes vont plus loin en disant qu'une plateforme de change est en elle-même une structure de régulation, comme le NASDAQ. Mais aussi important que soit le NASDAQ, aucun fonds n'est remboursé en cas de panne informatique. Les plateformes de change de bitcoins opèrent différemment. Cependant, elles n'ont pas de régulateur bien défini, ce qui ne garantit pas le remboursement d'éventuelles pertes suite à des problèmes de sécurité.



La protection des échanges offerte aux utilisateurs dépend du lieu d'enregistrement et des exigences réglementaires (ou de leur absence) sur les plateformes de change opérant dans une juridiction définie. Stocker vos bitcoins sur une plateforme pendant un jour ou deux n'est jamais une très bonne idée. Si cette structure cesse son activité pour une raison ou une autre, les solutions qui se présentent alors à vous reposent sur les lois de la juridiction où la plateforme est enregistrée. En général, plus les exigences réglementaires sont importantes, meilleure est la protection offerte. Vous pouvez donc vérifier ces informations afin de choisir une plateforme présentant le meilleur niveau de protection juridique.

De plus en plus de plateformes de change procèdent à des audits pour vérifier leur solvabilité de manière à poursuivre leur activité en toute sérénité. L'audit

indiquera si les données des utilisateurs sont suffisamment bien protégées. Nous abordons le sujet des efforts législatifs au [Chapitre 9](#).



Chaque plateforme publie les résultats de l'audit que vous pouvez consulter en contactant son support par e-mail ou par messagerie instantanée. Un responsable sera à même d'apporter des réponses claires à vos questions, notamment en donnant l'identité du cabinet d'audit et en vous indiquant où trouverez ses conclusions.

Au final, n'oubliez pas que toutes les responsabilités incombent à ceux qui utilisent librement des plateformes de change. Le bitcoin met entre vos mains le contrôle de vos finances. Si vous décidez de stocker des bitcoins sur ces plateformes, ils restent sous votre entière responsabilité.

## Crypter vos bitcoins

La sécurité est un aspect très important de l'univers du bitcoin. Sans elle, votre richesse électronique risque d'être dérobée à tout moment. Les développeurs de Bitcoin Core ont pris conscience de ce problème dès le début. Ils ont alors intégré une fonction qui permet de « crypter » votre portefeuille en le protégeant avec



une phrase secrète (consultez le [Chapitre 5](#) pour plus d'informations sur les portefeuilles).



Bitcoin Core est un logiciel bitcoin client destiné aux utilisateurs d'ordinateurs. Tous les portefeuilles bitcoin sont basés sur Bitcoin Core et fournissent une interface utilisateur différente et/ou des fonctionnalités supplémentaires.

## Choisir une phrase secrète

En utilisant une phrase secrète, vous « verrouillez » votre argent qui, de facto, ne peut plus être dépensé. Même si quelqu'un attaque le dispositif où votre portefeuille de bitcoins est établi, il ne pourra rien faire tant qu'il ne connaîtra pas cette fameuse phrase secrète.



Vos informations bitcoin sensibles – c'est-à-dire le fichier appelé wallet.dat qui consigne des données sur le titulaire de vos BTC – ne sont pas cryptées par défaut. Cela signifie que si vous installez simplement le logiciel client sur un ordinateur, il ne bénéficie d'aucune protection. Dès qu'une personne accède à votre ordinateur, elle peut dépenser instantanément votre argent.

Vous devez impérativement crypter votre portefeuille. La dernière version du client Bitcoin Core contient une

fonction de cryptage par phrase secrète. Vous pouvez aussi utiliser un outil externe pour crypter votre fichier wallet.dat. Cette opération est gratuite. Gardez à l'esprit que vous devrez taper cette phrase secrète chaque fois que vous souhaitez accéder à vos fonds ou consulter une transaction. Le cryptage d'un portefeuille de bitcoins le limite à un mode « spectateur » dans lequel vous ne pouvez que regarder les transactions et le bilan, mais sans pouvoir entrer dans les détails.



Tous les utilisateurs devraient crypter leur logiciel client en appliquant un mot de passe très difficile à craquer, donc composé de chiffres, de majuscules et de minuscules, et de symboles tels que @ ou #. Ce mot de passe doit être aussi aléatoire que possible. Toutefois, n'oubliez pas que vous devrez systématiquement le taper manuellement pour utiliser toutes les possibilités de votre portefeuille.

Si vous souhaitez crypter un portefeuille mobile, la procédure est sensiblement différente. La plupart des applications mobiles stockent le fichier wallet.dat – ou son équivalent mobile – sur l'appareil lui-même et le protège avec un code PIN. Bien que ce type de code sécurise beaucoup moins qu'une clé de cryptage, il fournit un niveau de sécurité suffisant pour la majorité des utilisateurs. Cependant, vous pouvez trouver d'autres solutions logicielles en tapant des mots-clés

dans votre moteur de recherche favori : 7Zip, Axcrypt, TrueCrypt, ou lrzip.

## Attention aux malwares



Il faut être conscient qu'aucun système de sécurité, aussi complexe soit-il, n'est invulnérable.



La plupart des utilisateurs de bitcoins disposent d'un logiciel antivirus installé sur leur ordinateur. C'est suffisant pour un usage quotidien d'un ordinateur. En revanche, dès que nous entrons dans le domaine des données financières – donc du bitcoin – vous devez disposer de couches de sécurité supplémentaires.

Les utilisateurs d'ordinateurs doivent se protéger contre toutes sortes de programmes malveillants. Par conséquent, l'installation d'un programme antivirus est insuffisante, surtout dans le domaine des portefeuilles de bitcoins. Vous avez également besoin d'un programme antispyware et antimalware comme Bitdefender, Kaspersky, Malwarebytes, et Norton Antivirus. Sachez que ces produits antivirus disposent d'une grande quantité de fonctions destinées à vous protéger contre les failles de sécurité d'Internet.



Le malware est le fléau majeur pour les portefeuilles bitcoin. Il s'agit d'une forme très particulière d'infection car, lorsque l'utilisateur en remarque la

présence, il est trop tard. Il existe différentes formes de malwares, chacune ayant pour objectif de vous faire perdre vos bitcoins si vous ne vous protégez pas avec des logiciels appropriés. Les malwares peuvent s'infiltrer selon votre activité Internet. Il suffit de visiter des sites au contenu malicieux (généralement des sites pour adulte), de cliquer sur de mauvais liens, d'ouvrir des pièces jointes suspectes, ou de télécharger du contenu illégal. Chacune de ces actions peut entraîner de sérieux dégâts sur votre ordinateur, mais aussi sur votre portefeuille de bitcoins.

Tous les mails que vous recevez ne contiennent pas des fichiers malveillants. Donc, ne devenez pas paranoïaque à la réception du moindre courrier électronique. En revanche, adoptez un comportement avisé. Ainsi, lorsque vous recevez des e-mails provenant d'un inconnu, n'ouvrez jamais ses pièces jointes. Il est plus difficile d'identifier des liens Internet suspects, notamment sur des réseaux sociaux comme Facebook et Twitter.

Le spyware est souvent comparé à un virus informatique, alors qu'il existe une grande différence entre les deux. Le spyware consigne des informations dans des journaux, comme les sites Web que vous visitez, des détails de connexion, les logiciels installés sur votre ordinateur, et le type d'e-mail que vous

envoyez et recevez. C'est très embêtant pour les personnes qui utilisent des services bitcoin en ligne, car le spyware peut obtenir des informations sur vos connexions, dont quelqu'un pourrait profiter à vos dépens.

Un logiciel antimalware et antispyware est généralement payant après une période d'essai gratuite. La sécurité de vos bitcoins est une priorité, et l'argent dépensé pour ce type de solution n'est rien à côté des pertes que vous pourriez subir si vous la négligez.

## Stockage physique des bitcoins

Plutôt que de stocker vos bitcoins sur un ordinateur ou un périphérique mobile, une troisième option est plus répandue parmi les utilisateurs de monnaie électronique : les bitcoins physiques – eh oui ! cela existe – ne sont pas que des pièces de collection. Ils permettent de stocker votre argent électronique.



Il existe divers types de bitcoins physiques qui, comme les devises que nous connaissons, sont composés de pièces de différentes valeurs. L'encadré « Les Casascius Series de bitcoins physiques » évoque des bitcoins physiques très populaires.

Chaque pièce de monnaie a sa propre valeur. Les bitcoins physiques les plus répandus ont été frappés en argent. Toutefois, il en existe aussi en bronze et en or. Toutes les pièces nécessitent un investissement initial et peuvent être envisagées aussi bien comme des objets de collection que comme un coffre à bitcoins.

## LES CASASCIUS SERIES DE BITCOINS PHYSIQUES

Les bitcoins physiques les plus connus sont ceux de la série Casascius créée par Mike Caldwell. Plusieurs générations de ces bitcoins ont été créées au fil des ans, toutes financées par les acheteurs qui utilisent eux-mêmes des bitcoins. Par exemple, une pièce de 0,5 BTC est financée par 0,5 bitcoin.

Les pièces Casascius sont populaires du fait de leur nombre limité, et aussi parce que toutes les pièces non commémoratives sont faites en argent ou en or. Ajoutez à cela que plusieurs pièces Casascius contiennent des « erreurs », ce qui en fait des objets de collection recherchés.

Pour plus d'informations sur les pièces Casascius, consultez [https://en.bitcoin.it/wiki/Casascius\\_physical\\_bitcoin](https://en.bitcoin.it/wiki/Casascius_physical_bitcoin) ou [https://fr.bitcoin.it/wiki/Portefeuille\\_Papier](https://fr.bitcoin.it/wiki/Portefeuille_Papier).

La plupart des bitcoins physiques permettent aux utilisateurs de stocker l'adresse de leur portefeuille et sa clé privée au dos des pièces. Ainsi, vous « financez » officiellement cette pièce en envoyant

une même quantité de BTC à l'adresse indiquée. Toutes les pièces comportent des instructions de financement.



N'oubliez pas que vous devez générer cette adresse et la clé privée qui lui est associée. Par conséquent, veuillez à être le seul à avoir accès à ces détails.

Une fois que vous avez créé l'adresse de votre portefeuille et la clé privée, vous recevez un petit morceau de papier qui confirme ces éléments. Ce document est généralement accompagné de la pièce elle-même, qui inclut un hologramme. Celui-ci est situé à l'arrière de la pièce, assurant ainsi que les informations du portefeuille ne sont pas falsifiées.

De nombreuses personnes utilisent les pièces physiques pour stocker des bitcoins de rechange dans l'espoir de voir le prix en BTC augmenter dans le futur. Ces pièces ne peuvent pas être dépensées sans briser l'hologramme qui révèle alors la clé privée.



Financer un bitcoin physique est le meilleur moyen de contrôler vos dépenses.

## Acheter des bitcoins en personne

Acheter des bitcoins de visu est une des meilleures manières de s'aventurer dans le monde de la monnaie électronique. Effectuer ce genre d'achat vous

familiarisera avec le transfert peer-to-peer, mais aussi vous permettra de rencontrer des personnes qui partagent le même intérêt que vous pour les bitcoins.



L'échange de bitcoins dans la réalité peut attirer des personnes mal intentionnées. Les malfrats savent que le bitcoin existe également en liquide. De facto, une personne qui transporte beaucoup de bitcoins sur elle devient une cible privilégiée pour ces voleurs.

Avant de pouvoir réaliser votre transaction peer-to-peer, vous devez préparer des éléments essentiels. Sans doute que l'aspect le plus important de cette opération est la création initiale d'une adresse de portefeuille. Après tout, sans adresse de portefeuille valide, il n'y a aucun moyen de stocker vos BTC.

## Votre adresse de portefeuille

Votre portefeuille de bitcoins est une longue chaîne aléatoire de chiffres et de lettres majuscules et minuscules. Vous ne pouvez pas l'apprendre par cœur, car elle a été conçue pour représenter un haut niveau de sécurité. Si quelqu'un était capable de la mémoriser, il pourrait accéder à la chaîne de blocs et surveiller l'activité de vos bitcoins en temps réel sur <https://blockchain.info/> (par exemple).





Vous pouvez créer une adresse de portefeuille de plusieurs manières. Cependant, si vous envisagez d'utiliser le peer-to-peer, des solutions mobiles peuvent s'avérer être un choix intéressant. En installant une application mobile de portefeuille de bitcoins, la procédure de création de l'adresse vous protège au maximum. Gardez à l'esprit que vous devez vous enregistrer avant d'utiliser une appli. Par conséquent, effectuez cette action avant toute autre chose.

Une adresse de portefeuille bitcoin sera automatiquement générée pour vous lors de l'installation du logiciel idoine sur votre ordinateur ou votre appareil mobile.



Une fois que tout semble bien configuré, il reste une dernière chose à faire. Pendant vos transactions peer-to-peer, vous devez présenter votre adresse de portefeuille d'une manière claire à la personne qui vous vend l'argent. Plutôt que de noter l'adresse sur un papier avec les risques d'erreur que cela comporte du fait de sa complexité, il est préférable d'utiliser un code QR. Vous en avez déjà probablement vu sur des emballages ou à la TV. Il s'agit d'un carré blanc avec un motif noir incompréhensible. Votre banque en utilise peut-être pour authentifier les paiements mobiles. Les codes QR représentent une méthode de partage des

informations de paiement avec d'autres utilisateurs.

En créant un code QR, vous pouvez facilement partager votre adresse de portefeuille de bitcoins. Les autres parties à la transaction n'ont qu'à utiliser l'appareil photo de leur smartphone pour scanner le code QR avec l'application de portefeuille installée sur leur mobile. Tous les détails pour réaliser la transaction de leur côté sont remplis automatiquement.

L'utilisation des codes QR facilite les transferts, en accélère la procédure, et améliore l'expérience globale des utilisateurs. Après tout, qui a toujours un ordinateur portable sous la main ?



Un autre avantage de l'utilisation des codes QR tient au fait que le vendeur peut vous prouver que la transaction a bien été envoyée sur son périphérique. En même temps, vous pouvez vérifier, sur votre appareil, que l'argent est bien là. Gardez à l'esprit que chaque transaction demande généralement six confirmations réseau avant que l'argent puisse être dépensé.

Les transactions bitcoin doivent être confirmées sur le réseau avant que les fonds ne soient disponibles pour le destinataire. Chaque fois qu'un nouveau bloc est trouvé sur le réseau – approximativement toutes les dix minutes – une transaction gagne une confirmation

supplémentaire. Dans certains cas, la disponibilité de la transaction peut prendre jusqu'à une heure.



En fonction du logiciel de portefeuille que vous utilisez, les transactions peuvent être plus rapides. Ainsi, sur les périphériques mobiles, vos fonds sont accessibles plus vite que sur un ordinateur. Tout dépend du portefeuille, et cela même si la « norme » est d'avoir six confirmations réseau pour une transaction avant que les fonds puissent être de nouveau utilisés. Le [Chapitre 6](#) vous en dira davantage à ce sujet.

## Rencontre dans un lieu public

Le commerce peer-to-peer du bitcoin se déroule dans un espace public. Cela protège les deux parties contre un potentiel préjudice. De plus, il est facile de se rendre dans un lieu public, même si vous le faites pour la première fois.



Choisissez un lieu où vous vous sentez à l'aise. Préférez donc un endroit neutre. N'invitez personne chez vous, à votre travail, ou dans un endroit que vous fréquentez souvent. La majorité des traders n'ont aucune volonté de vous nuire, mais il est préférable de se garantir contre toute mauvaise surprise.



Une autre raison pour laquelle un lieu public s'avère être un excellent choix est que les deux utilisateurs ont

besoin d'accéder à Internet. Des endroits comme les cafés proposent des connexions Wi-Fi gratuites.

Bien entendu, il est impératif que la connexion se fasse de manière ininterrompue pour ne pas porter atteinte à la validité de la transaction. Encore une fois, cela plaide en faveur des lieux publics plutôt que d'endroits isolés où les connexions cellulaires peuvent poser problème.



Conduire un échange bitcoin peer-to-peer présente un petit risque. Vous pouvez tomber sur un bandit qui vous menacera afin de vous voler vos bitcoins. Essayez alors d'être clairvoyant sans devenir paranoïaque, car ce genre de circonstance est excessivement rare.

## Payer un prix majoré

Acheter de visu à un autre utilisateur peut présenter un inconvénient majeur : vous risquez de payer une majoration par bitcoin ainsi échangé. Cela signifie que le prix payé sera sensiblement plus élevé que le cours actuel.



Tous les traders connaissent précisément le cours du bitcoin sur les plateformes de change les plus réputées. Nous vous conseillons alors de vérifier ce cours avant d'accepter la transaction peer-to-peer. Ainsi, vous obtiendrez la valeur maximale pour vos bitcoins.

Le taux de change du bitcoin fonctionne de deux manières : aucune loi n'interdit au vendeur d'appliquer une majoration. C'est une des facettes d'un marché financier libre basé sur le principe de l'offre et de la demande – chacun peut faire son prix. Les acheteurs cherchent à acheter au cours le plus bas. Toutefois, si le prix du vendeur semble être tout à fait convenable, les acheteurs ne rechigneront pas à payer un petit supplément.

Le montant de cette majoration dépend entièrement du vendeur. À l'instar du fonctionnement des distributeurs automatiques de bitcoins (voir l'encadré suivant), une majoration de 5 % est souvent appliquée. Mais le taux de cette majoration est variable. N'oubliez pas que nous sommes sur un marché libre. Donc, attendez-vous à payer un prix légèrement supérieur au taux de change. C'est le prix à payer pour effectuer une transaction plus rapide que si vous passiez par la lente procédure de vérification habituelle.

## Choisir un moyen de paiement

Effectuer un achat peer-to-peer de bitcoins signifie que vous disposez d'un large éventail de moyens de paiement. Cependant, il y a de fortes chances pour que le vendeur impose le moyen qu'il préfère qui, dans la majorité des cas, est un paiement en espèces.

Et cela pose des problèmes de sécurité, surtout si le montant de la transaction est à quatre chiffres. En cas d'agression, vous risquez de perdre gros. Par conséquent, ne payez jamais un échange de visu en espèces lorsque la somme représente des milliers de dollars, d'euros, ou de livres.

## LES DISTRIBUTEURS DE BITCOINS

Un distributeur de bitcoins fonctionne comme un distributeur de billets standard. Vous achetez des bitcoins avec des espèces. Certains effectuent l'opération inverse. Bien entendu, des frais sont appliqués de l'ordre de 0 à 12 %.

Pour en savoir davantage sur la localisation des distributeurs, consultez le site <http://achat-bitcoins.com/carte-monde-distributeurs-bitcoins/>.

Certains revendeurs de bitcoins locaux peuvent accepter un transfert de banque dont les détails vous seront fournis. Cependant, ce moyen de paiement est rarement utilisé. En effet, un transfert de banque s'effectue sans rencontre préalable.



Utiliser un moyen de paiement comme PayPal ou une carte de crédit ne constitue pas une option valable lorsque vous traitez d'homme à d'homme. En effet, ces deux méthodes de paiement peuvent être utilisées pour rembourser des fonds alors que les transactions de

bitcoins ne le permettent pas. Il en résulte que, en théorie, vous pouvez acheter des bitcoins avec PayPal ou une carte de crédit, recevoir l'argent, puis demander à être remboursé soit par la banque, soit par PayPal. Dans la plupart des cas, vous souhaitez également récupérer l'argent.

## Hot wallets et stockage à froid

---

Deux termes reviennent régulièrement lorsque nous parlons des plateformes de change de bitcoins : stockage à froid et hot wallets.



Ces deux notions recouvrent des mesures de sécurité mises en place par des plateformes de change dans le but de garantir les fonds des utilisateurs contre tout type d'incident :

- » **Le stockage à froid se réfère à la gestion de bitcoins hors ligne.** Vous pouvez comparer ce principe à des fonds protégés dans un coffre plutôt qu'à la caisse de la banque. Dans le cas du stockage à froid, d'autres couches de sécurité sont mises en place. Nous pouvons citer comme exemple le stockage sur clé USB ou un portefeuille matériel dédié.

Comme vous le savez, la majorité des portefeuilles sont stockés sur des serveurs connectés à Internet. Avec le stockage à froid, les portefeuilles sont gérés

hors ligne, ce qui les protège des hackers qui entreraient dans une plateforme par infraction.

Les plateformes de change peuvent protéger la plupart des utilisateurs contre des incidents. Cependant, il existe suffisamment de mouvements de fonds au sein d'une plateforme pour qu'il y ait toujours des utilisateurs qui souhaitent effectuer des retraits. Et nous savons qu'un échange de bitcoins par retrait se fait immédiatement et non pas au bout de plusieurs heures.

» **Hot wallets** identifie une méthode par laquelle chaque échange de bitcoins conserve une certaine liquidité au cas où il y aurait un flux massif de retraits. Vous pouvez envisager cela comme la réserve de *cash* dont une banque doit disposer pour faire face aux demandes de retrait de leurs clients. Le hot wallets fournit constamment des liquidités dans une monnaie électronique. Contrairement au stockage à froid, un hot wallet est un portefeuille bitcoin connecté à internet H24 et 7/7.

Une bonne pratique commerciale en matière d'échange de bitcoins consiste à ne pas trop stocker de fonds dans ce type de portefeuille... un peu chaud en effet. 1 % de la quantité totale des bitcoins circule sur les plateformes de change, ce qui représente plusieurs centaines, voire milliers, de BTC. Si une



plateforme est attaquée par des pirates, la perte de fonds peut être cataclysmique.

Pour éviter cela, les plateformes n'effectuent pas d'importants retraits sur des *hot wallets*, préférant transférer les fonds depuis un stockage à froid vers le destinataire désigné. Chaque plateforme dispose de ses propres limites internes pour effectuer ces opérations. Il est donc difficile de quantifier la somme à partir de laquelle la transaction est refusée dans ces conditions particulières. Retenez simplement que, lorsque vous débutez, il est déconseillé de stocker un trop grand nombre de BTC sur un portefeuille géré par une plateforme de change.

## Sécuriser les fonds

Protéger les fonds des utilisateurs est la priorité de toutes les plateformes de change de bitcoins. Il suffirait qu'une plateforme ait mauvaise presse dans ce domaine pour que sa réputation soit à jamais ternie. En effet, les mauvaises nouvelles se répandent toujours plus vite que les bonnes.

Pour protéger les fonds des clients, les plateformes de change mettent en place des contre-mesures parallèlement au stockage à froid et aux hot wallets (voir la précédente section), bien que ces deux méthodes soient les plus répandues. Sachez qu'il y a de

quoi travailler sur l'amélioration de la sécurité de tous ces dispositifs. Alors, de brillants cerveaux se sont réunis pour créer un Bitcoin Exchange Security Standard, c'est-à-dire une standardisation de la sécurité des échanges.

Ce standard a pour but d'améliorer la sécurité générale autour du bitcoin et des fournisseurs de portefeuilles. Tout cela se faisant dans un cadre technique facile à mettre en œuvre, afin d'obtenir l'adhésion de toutes les plateformes. Dans le passé, aucune plateforme de change ne s'est suffisamment penchée sur les problèmes de sécurité. De facto, elles durent essuyer de nombreuses attaques de hackers, avec une perte de fonds assez élevée.



Il existe une dizaine d'approches sur la création des clés privées ainsi que sur la gestion du stockage à froid et des hot wallets. L'accent est également mis sur les audits de sécurité, les preuves de disponibilité, et d'autres concepts qui n'ont pas encore été dévoilés.

Plutôt que de laisser chaque plateforme développer son propre système de sécurité, un standard unifié pourrait asseoir la légalité de toutes les plateformes. Cette approche a connu quelques succès ces dernières années, montrant ainsi le sérieux de cet écosystème.

De plus, un tel système représente une aide indéniable et incontournable pour les régulateurs. Le bitcoin est sous l'étroite surveillance de régulateurs dans le monde entier. Il serait donc de leur intérêt de définir un standard de sécurité. Les régulateurs ont pour tâche de développer des cadres d'activités financières du bitcoin. La mise en place d'un standard sur les plateformes de change serait un réel bénéfice pour tous les acteurs du bitcoin.

## Prévenir le piratage des échanges

Les plateformes de change du bitcoin sont souvent la cible des hackers qui tentent de dérober des BTC. Force est de constater que de grosses sommes d'argent sont tombées dans des mains malveillantes du fait de grosses failles de sécurité.

Mt. Gox (à Tokyo) fut l'une des plus importantes plateformes de change à avoir subi des attaques. Un des comptes du site fut atteint avec une perte brute d'environ 32\$ US par bitcoin. Cependant, les hackers se heurtèrent à la limite de 1 000 \$ par retrait mise en place par Mt. Gox, rendant alors leur tentative beaucoup moins fructueuse.

Bitcoinica fut pendant longtemps l'une des plateformes les plus populaires jusqu'à cette attaque de 2012 qui lui fit perdre des milliers de bitcoins appartenant à des clients. Bitcoinica promit de les rembourser sur ses fonds propres. Mais, une seconde attaque suivit rapidement la première avec une perte encore plus importante. Ce scénario catastrophe n'apporta au final aucune réponse aux clients de Bitcoinica. Et le lien qui existait entre cette société et Mt. Gox ne lui fut d'aucune aide.

Septembre 2012 marqua la disparition de la plateforme BitFloor sur laquelle furent dérobés 24 000 BTC. Le hacker avait réussi à pénétrer dans une sauvegarde non protégée par des clés. Les clients ainsi lésés furent remboursés en dollars US et non pas en bitcoins.

Février 2013 fut la période la plus sombre de l'histoire du bitcoin, lorsqu'intervint la deuxième attaque de Mt. Gox, et où la plateforme subit une chute dont elle ne se releva pas. Bien que cette structure ne détînt que 2000 BTC, sa facture s'éleva à 750 000 BTC pour l'ensemble de ses clients. Les investigations sur les BTC volés ou manquants sont toujours en cours au moment où vous lisez ces lignes.

La liste ne s'arrête pas là. D'autres attaques eurent lieu en 2015. La mise en œuvre d'un système de sécurité approprié et efficace demande du temps. Donc, en

attendant, il est préférable d'effectuer vos transferts de fonds en dehors des plateformes de change aussitôt que vous en avez la possibilité.

## Chapitre 3

# Bitcoin : les pour et les contre

---

### DANS CE CHAPITRE

- » Analyser les possibilités du bitcoin
  - » Maintenir la sécurité
  - » Faire confiance aux systèmes et à la technologie
- 

Pour ou contre est un principe applicable à chaque chose qui nous atteint. C'est d'ailleurs la seule manière de distinguer le meilleur du pire. Ce chapitre aborde ces deux aspects du bitcoin.

## Les pour du bitcoin

---

Une fois n'est pas coutume, commençons par les bonnes nouvelles du bitcoin.



Il s'agit de mon appréciation personnelle des aspects positifs du bitcoin. Vous vous ferez votre propre opinion en utilisant cette monnaie. Mais comme je suis une personne relativement standard, sachez simplement que ce chapitre regroupe des opinions assez communément admises.

## Liberté financière

Le bitcoin offre de nombreux avantages, dont le plus important est sans doute son niveau de liberté. Et cette liberté s'exerce de différentes manières : liberté de ne pas être obligé de s'en remettre à une infrastructure existante, mais aussi liberté psychologique en devenant le propre contrôleur de votre argent et de la technologie qui permet de le gérer.

Si tout le monde adoptait le bitcoin pour régler ses achats quotidiens, l'argent liquide et les cartes bancaires disparaîtraient, libérant les utilisateurs du diktat des banques. De plus, chacun disposerait à tout moment d'un contrôle total sur ses fonds. Personne ne vous imposerait de stocker vos bitcoins dans un endroit précis, de les dépenser d'une certaine manière, ou bien encore ce qu'il est conseillé ou non de faire avec. Les seules limites de cette liberté sont celles que vous édicterez.

## Vers une liberté financière

Les banques et les institutions financières ont lentement tissé une toile « bienfaitrice » autour de nous qui impose des comportements financiers que nous estimons légitimes. Personne ne cherche d'alternative au compte en banque. D'ailleurs, la

majorité des gens trouvent ou ont fini par trouver que ce système fonctionnait parfaitement bien. Pourquoi pas ! Tant qu'un système ne montre pas ses limites et ses dangers, il ne semble y avoir aucune raison de le contester. Pourtant, le bitcoin est une alternative viable. Mais dans l'optique d'aboutir à une réelle liberté financière, nous devons convaincre le grand public de sa puissance et de sa légitimité.



Dès qu'une masse critique adoptera le bitcoin comme monnaie principale, le système actuel sera ébranlé. Il s'adaptera ou mourra. Pour cela, chaque personne doit savoir ce en quoi consiste le bitcoin pour qu'elle décide d'en faire un élément de sa vie quotidienne. En fonction de chaque individu, cette perception sera d'ordre technique, financier, et peut-être, pour ne pas dire surtout, idéologique. Malgré le développement constant du bitcoin, force est de constater qu'il reste une « niche », donc limité à une portion congrue de la population.

## **ACHETER UN BITCOIN AIDE À L'ÉVOLUTION DES MENTALITÉS**

Il y a plusieurs manières d'envisager le bitcoin et sa technologie de chaîne de blocs comme un meilleur écosystème financier. Si les zones géographiques du monde non soumises à une autorité bancaire pouvaient payer et être payées en bitcoins, elles



gagneraient en liberté et en puissance. Par exemple, si vous travaillez dans les vignobles de l'Afrique subsaharienne et que vous receviez un salaire en bitcoins, vous empêcheriez un exploitant peu scrupuleux de vous rémunérer en litres de vin, rendant ainsi les travailleurs alcooliques et esclaves de leur patron.

La technologie du bloc de chaînes est faite pour accéder à une liberté individuelle, en menant des négociations contractuelles en toute transparence. Elle permettrait, par exemple, d'organiser des élections dont le contrôle « citoyen » empêcherait bien des tentatives de fraudes, limitant de facto toute corruption. Les bénéfices de la chaîne de blocs sont bien réels et peuvent s'appliquer à de multiples activités.

De ce fait, ses applications commerciales semblent illimitées. De plus, les personnes les moins privilégiées de notre monde gagneraient en libertés individuelles, ce qui renforcerait positivement de nombreux aspects de leur vie quotidienne.



La liberté financière attachée au bitcoin ne profite pas uniquement aux commerçants qui acceptent les paiements avec cette monnaie électronique. Le consommateur l'exerce également en pouvant payer ses achats en ligne (ou ailleurs) avec des bitcoins, qu'il s'agisse de marchandises ou de services. Toutefois, pour qu'une liberté puisse s'exprimer pleinement, encore faut-il qu'une grande majorité de personnes s'y rallient en abandonnant les moyens de paiements

traditionnels.

Pour cela, nous devons changer nos habitudes. L'infrastructure financière actuelle a éduqué les consommateurs pour les rendre esclaves de leurs systèmes de paiement. Ils restent basés sur un compte courant sur lequel de l'argent est prélevé en espèces ou via des cartes bancaires. La prochaine étape de ce système est le paiement mobile qui restera, quoi qu'il arrive, lié à un compte en banque. Par conséquent, le moyen de paiement changera sensiblement, mais la source de l'argent restera la même. Seul bénéfice ? Eh bien, plus de porte-monnaie ni de carte bancaire. C'est assez faible comparé à la philosophie du bitcoin.

## Comprendre notre absence de liberté actuelle

Aujourd'hui, le souci est que peu de personnes comprennent à quel point elles sont liées à ce système bancaire « esclavagiste ». Ainsi, il ne leur vient même pas à l'idée que ce système puisse s'effondrer.



### SE PROJETER DANS LES PROBLÈMES

---

Envisageons ce scénario futuriste.

1 million de dollars US circulent dans le monde. Du jour au lendemain, la valeur du dollar tombe de moitié, faisant que chaque dollar ne vaut plus que 50 cents. Pour stabiliser l'économie, la Réserve fédérale décide d'imprimer 1 million de dollars supplémentaire. Cela semble logique puisque nous retrouvons ainsi les 1 million de dollars en circulation. Pourtant, c'est une erreur.

En effet, il y a désormais 2 millions de dollars en circulation pour atteindre une valeur réelle de 1 million.

Doubler la monnaie en circulation ne fait qu'aggraver le problème. En effet, le million de dollars d'origine ne gagne pas en valeur, et si cette valeur devait davantage être dévaluée, la valeur initiale sera alors encore plus faible. À la fin, c'est un effet de dominos qui est créé, et qui empile couche de dette sur couche de dette.

Si un tel cercle infernal se poursuit, un pays connaît une hyperinflation comme l'Allemagne dans les années 1920, ou plus récemment au Zimbabwe au milieu des années 1990 jusqu'en 2009. Mais comme nous pensons que les banques centrales agissent pour le bien de tous, nous n'envisageons jamais un tel scénario.



Si la Réserve fédérale américaine – ou la Banque centrale européenne – décide qu'il faut imprimer davantage de billets « pour relancer l'économie »,

personne ne peut l'en empêcher. Cette intervention ne résout jamais le problème de la chute de la valeur de l'argent en circulation, mais bien au contraire, elle aura pour effet d'augmenter la dette. Et c'est le consommateur qui paiera l'addition et qui, d'une certaine manière, en est responsable en soutenant implicitement ce système.

Faire tourner la planche à billets signifie qu'une plus grande quantité d'argent est en circulation. Mais, pour qu'une monnaie garde sa valeur réelle, il ne faut pas qu'il y ait plus de billets que de valeur, sinon cela conduit à la dévaluation et à l'inflation. C'est un cercle vicieux dans lequel il est impossible que le bitcoin puisse entrer. Lisez l'encadré « Se projeter dans les problèmes » pour comprendre comment un scénario catastrophe peut devenir réalité.

## **La différence entre le bitcoin et une monnaie libre**

Le scénario de l'encadré « Se projeter dans les problèmes » permet de mieux comprendre la différence qui existe entre le bitcoin et le papier-monnaie, plus précisément en termes de liberté financière.

Cet argent que vous avez dans votre portefeuille ou sur votre compte en banque représente une certaine valeur.

Par exemple, un billet de 20 euros vaut 20 euros. Est-ce la vérité ? C'est en tout cas ce que l'on vous raconte. Mais comment vous, pauvre consommateur, pouvez-vous le vérifier ?



Avec le bitcoin, la liberté du marché en fixe le prix, et cela au satoshi près, c'est-à-dire à la plus petite division des bitcoins (0,00000001). Ainsi, ce marché est constitué de tous les bitcoins du monde et aucune autorité supérieure ne peut en fixer le prix. Le bitcoin est l'une des monnaies électroniques les plus transportables et sans frontière. Comme toute monnaie existante, elle peut perdre ou gagner de la valeur en réponse à un marché, et non pas à une décision arbitraire.

Le prix du bitcoin est défini par les monnaies locales. C'est un aspect positif. Bien que le bitcoin soit un moyen de paiement sans frontière, il doit être converti en une monnaie physique dans la majorité des états avant d'être utilisable. Ce niveau de liberté financière permet à chacun d'envoyer de la valeur à d'autres personnes de cette planète. Ces destinataires peuvent alors convertir ces bitcoins en monnaie locale ou les stocker à leur tour en BTC.



Le bitcoin permet de passer outre cet espèce de monopole de services comme MoneyGram et Western Union qui, non seulement prennent d'importantes

commissions, mais exigent des informations très personnelles chaque fois que envoyez ou recevez de l'argent.

## Libérer votre esprit

Psychologiquement, être libéré de tout obstacle est un délicieux moment auquel ne nous ont jamais habitués les infrastructures financières traditionnelles. Mais vous devez l'expérimenter pour le croire. Comment ? Eh bien en payant vos dépenses quotidiennes en bitcoins, et en recevant tout ou partie de votre salaire en bitcoins. Il existe suffisamment d'outils en la matière pour se passer d'intermédiaires – comme les banques ou les établissements assimilés – qui partagent une mentalité commune consistant à vous asservir à leurs services en tout genre.

Nous pouvons dire la même chose de l'idéologie associée au bitcoin. En effet, si vous utilisez quotidiennement cette monnaie électronique, vous favorisez l'extension de ce réseau. Et plus les consommateurs l'utiliseront, plus les commerçants, les institutions, les gouvernements, et les sociétés se tourneront vers le bitcoin et participeront au développement de sa technologie et de son fonctionnement pour aboutir à un protocole bitcoin. Cela ne peut conduire qu'à un monde meilleur pour

tous. Appelez cela l'effet papillon, si vous le souhaitez, tout en gardant à l'esprit que le meilleur moyen de supporter le bitcoin est d'en devenir un membre actif sur le réseau et dans cette communauté en pleine expansion.

## La sécurité

La sécurité du bitcoin fait beaucoup parler d'elle. En effet, les problèmes de sécurité sont justement liés à l'aspect libertaire de cette monnaie. C'est un point délicat qui touche absolument toutes les activités à risques, dont le bitcoin fait partie comme n'importe quel véhicule financier.



Le bitcoin n'est pas soumis aux desiderata des banques centrales qui peuvent dévaluer leur monnaie pour obtenir une économie plus compétitive par exemple. Donc, en termes purement financiers, le bitcoin offre davantage de sécurité dans un système robuste comparé aux institutions financières traditionnelles.

En supposant qu'avec le temps il existe assez de liquidité et un volume d'échanges suffisant dans l'écosystème du bitcoin, le marché s'autorégulera sur le principe de l'offre et de la demande sans aucune intervention externe, comme des traders qui, pour faire

du chiffre, ont besoin d'agir directement sur les marchés.

Des services sont constamment en recherche d'amélioration de la sécurité, et de futures implémentations dans la technologie de la chaîne de blocs augmenteront la sécurité globale du réseau.

La plupart des individus veulent contrôler leurs finances. Les utilisateurs du bitcoin n'échappent pas à cette tendance. Et si l'argent que vous mettez en banque n'est pas sécurisé, personne ne vous remboursera en cas de vol. Dans le cas du bitcoin, la sécurité commence avec les utilisateurs eux-mêmes. L'idée n'est pas, comme toujours avec la philosophie du bitcoin, de s'en remettre à des services spécifiques. Bien entendu, ce type de service existe dans l'univers de la crypto-monnaie, mais il ne doit pas être utilisé de la même manière que dans d'autres institutions financières. N'oubliez pas que le bitcoin est un système décentralisé et que cette notion de décentralisation s'applique aussi à la sécurité. Vous devez en avoir conscience dès que vous commencez votre aventure du bitcoin.

D'un point de vue technologique, la chaîne de blocs (blockchain), que nous traitons au [Chapitre 7](#), et qui alimente le réseau bitcoin, peut s'appliquer dans divers aspects de la vie. Parmi ces aspects, notons



l'implémentation d'un niveau supérieur de sécurité tel que nous l'employons aujourd'hui, sachant que nous découvrons tout juste le potentiel de cette technologie. Un simple exemple de la manière dont la chaîne de blocs peut améliorer la sécurité quotidienne prend la forme d'une connexion sans mot de passe. « Diable ! » hurlez-vous dans votre fauteuil en lisant cela. Be quiet ! Pour accéder à la plupart des services en ligne, comme vos e-mails, vous devez taper un nom d'utilisateur et un mot de passe. La chaîne de blocs peut rendre le principe des identifiants redondants en mettant en place un système de connexion lié à la chaîne de blocs et à l'adresse de votre portefeuille de bitcoins. Ainsi, les utilisateurs n'ont plus à craindre d'oublier les mots de passe !

Au-delà des problèmes de sécurité liés à votre identité, il est important de sécuriser d'autres aspects du bitcoin. Les produits contrefaits sont un gros souci pour les états du monde. Qu'il s'agisse de vêtements, de logiciels, ou de médicaments, tout le monde perd de l'argent à cause de cette activité criminelle. Avec la technologie de la chaîne de blocs, il est possible de suivre le processus de fabrication de chaque article que nous achetons et de vérifier s'il est authentique ou non. Bien que les gouvernements du monde entier soient

séduits par cette idée, peu montrent une réelle volonté de mettre en place le système de la chaîne de blocs.

La technologie sous-jacente du réseau bitcoin permet de découvrir et de mettre en œuvre de nombreuses fonctions de sécurité que nous ne pouvions pas imaginer il y a dix ans. Mais cela demandera du temps avant de devenir d'une efficacité totale, exigeant ainsi que de nombreux développeurs travaillent dans ce domaine. La force de la sécurisation du réseau bitcoin dépend uniquement de celle des utilisateurs et des développeurs qui la soutiennent. Il faudra à tous beaucoup de patience.

## Éviter la fraude

La fraude reste l'un des plus grands fléaux des activités financières.



La fraude prend diverses formes, de la fausse monnaie au vol de cartes de crédit, en passant par le piratage des comptes PayPal et l'intrusion dans les comptes bancaires. Il existe aussi des fraudes du côté du récepteur, et certaines méthodes de paiement ne permettent pas d'être remboursé lorsque vous en êtes victime.

**Ne faire confiance à personne...**

Si vous souhaitez acheter quelque chose en ligne, sur eBay par exemple ou dans une boutique en ligne standard, les options de paiement sont généralement la carte bancaire, PayPal, ou le virement. Choisir le virement peut s'avérer être la pire des options, car en cas de fraude, les fonds ne sont pas récupérables.

Enverriez-vous de l'argent sur le compte bancaire d'une boutique en ligne ? Sans doute, car cela vous paraît être d'une extrême sécurité. Vous pensez qu'une fois les fonds sur le compte, les marchandises vous seront expédiées. Mais, en êtes-vous sûr ? Si les produits ne sont jamais envoyés, votre argent est perdu à tout jamais. En effet, si le virement garantit le paiement de banque à banque, il ne garantit pas l'honnêteté du commerçant qui en profite.

Utiliser PayPal n'est pas une option plus sécurisante. Dans la majorité des cas, PayPal assure la protection des vendeurs. Mais la fraude reste possible. En effet, le vendeur peut tout à fait recevoir l'argent et ne jamais envoyer les marchandises. Idem, l'acheteur peut très bien avoir reçu sa commande et prétendre qu'il n'en est rien, demandant alors un remboursement. Si vous payez pour un objet que vous ne recevez jamais, vous pouvez ouvrir un incident. Mais si le vendeur produit un numéro de suivi – par exemple en envoyant un colis vide – l'acheteur ne peut plus faire grand-chose.

Nous en arrivons au pire des moyens de paiement en ligne et dans la vie quotidienne : la carte bancaire. Il s'agit d'un rectangle en plastique avec un code magnétique qui contient d'importantes données confidentielles, comme le numéro de la carte, sa date d'expiration, le code CVV, et même le code confidentiel de la carte. Bien souvent, la totalité de ces informations est stockée sur la puce de la carte.

Le problème majeur des cartes bancaires est que vous devez physiquement donner la carte ou des détails la concernant pour effectuer un paiement. Même si vous insérez votre carte dans un lecteur, vos données sont vérifiées afin de valider votre paiement. À l'étranger, le système de l'empreinte existe parfois, c'est-à-dire un papier sur lequel les éléments de la carte sont imprimés et que vous devez signer. Aucune méthode n'est sûre, et toutes portent atteinte à la vie privée de l'utilisateur.

### ... à l'exception des bitcoins

Une transaction BTC peut être inversée. Une fois que les fonds ont été envoyés à une adresse différente – même si elle attend une confirmation réseau – vous ne pouvez pas récupérer votre argent. C'est un des revers du contrôle décentralisé de vos finances.



Vérifiez toujours les détails du paiement avant d'effectuer une transaction.

Cela étant dit, l'aspect irréversible du bitcoin est un bienfait pour les commerçants qui resteraient à la merci des institutions financières traditionnelles. Dès qu'un paiement en bitcoins est fait, le commerçant peut le valider sans se soucier d'un potentiel remboursement en cas de fraude. Le bitcoin lui permet de rembourser l'acheteur en cas de produit endommagé puisqu'il connaît l'adresse bitcoin d'où l'argent a été envoyé.

Plutôt que de s'en remettre à une société de cartes de crédit ou à une banque pour rembourser le client, les commerçants l'effectuent eux-mêmes. Enfin, les transactions bitcoin sont créditées et débitées bien plus vite que les méthodes de paiement traditionnelles. C'est un avantage certain pour l'acheteur et le vendeur.



Le bitcoin prévient les commerçants et les clients contre la fraude. Mais si le portefeuille d'un utilisateur est attaqué et que de l'argent y soit volé, il n'y a que peu de moyens d'empêcher le voleur de dépenser les fonds ainsi dérobés. Bien qu'il ne s'agisse pas techniquement d'une fraude, le commerçant pourrait très bien recevoir de l'argent frauduleux, et ainsi accepter et valider une commande. Contrairement à l'argent liquide, il n'existe pas de régulateur central. Par conséquent, l'utilisateur final assume l'entière responsabilité de sa propre sécurité.

# Transparence

Le plus grand avantage du bitcoin – ou pour être plus précis, de la technologie de la chaîne de blocs qui la sous-tend (consulter le [Chapitre 7](#)) – prend la forme d'un système d'échange totalement transparent.

Pour les individus et les affaires commerciales qui souhaitent éviter cette transparence pour des raisons fiscales par exemple, le bitcoin sera inévitablement un inconvénient. Cependant, la chaîne de blocs agit comme une sorte de livre comptable public répertoriant toutes les transactions financières réalisées sur le réseau bitcoin. Elle peut aussi être adaptée pour répondre à d'autres besoins comme le stockage des fichiers, la détention, le commerce d'actifs, ou même la vérification de la procédure de fabrication des médicaments. Les possibilités ne sont limitées que par notre imagination.



L'intérêt majeur du bitcoin et de la technologie de la chaîne de blocs se situe au niveau financier. Bien que le bitcoin autorise l'envoi d'argent à quiconque dans le monde à moindres frais – tout en donnant la possibilité de suivre ce paiement jusqu'à son destinataire – ce principe n'est pas idéal pour tous. C'est pourquoi il est nécessaire de garder à l'esprit que le bitcoin est bien plus qu'un moyen de paiement. Par exemple, vous

pouvez placer la propriété de votre voiture sur la chaîne de blocs qui sera validée par le réseau lorsque le bloc associé à vos données sera confirmé. Si vous vendez cette voiture, vous pourrez transférer numériquement cette propriété en l'envoyant à une autre personne sur la chaîne de blocs bitcoin. Une fois ce transfert réalisé et confirmé sur le réseau, le nouveau propriétaire pourra officiellement se prétendre propriétaire de la voiture. Pas de paperasserie – juste un échange de clés et l'envoi d'un actif numérique qui symbolise le véhicule.



Tous les consommateurs ne veulent pas que leurs données financières soient diffusées publiquement. C'est tout à fait compréhensible. Mais sachez que chacun agit sous un pseudonyme sur le réseau bitcoin. Ainsi, personne ne pourra savoir qui vous êtes réellement si vous ne souhaitez pas que cela soit divulgué. L'adresse de votre portefeuille est liée à la transaction, mais il n'y a aucun nom ou emplacement physique qui lui est attaché.

L'infrastructure financière actuelle n'offre aucune vision sur la manière dont la valeur stockée du bitcoin est utilisée. Les fonds que vous stockez sur un compte sont palpables en ce sens que vous pouvez retirer votre argent. Mais chacun sait que les banques utilisent notre argent pour en créer davantage. En d'autres termes,

nous sommes conscients que les banques jouent avec nos économies. Si elles perdent tout, personne ne sera là pour panser les blessures.

La nature transparente du bitcoin et de la technologie de la chaîne de blocs est un atout pour de nombreuses personnes. Avec de plus en plus de sociétés et de développeurs qui se focalisent sur l'extension de la chaîne de blocs à d'autres secteurs que l'espace financier, personne ne peut savoir ce qui sera concerné dans le futur. Alors, si vous avez des idées, rejoignez-nous ! Commencez par utiliser le bitcoin et laissez-vous emporter !

## Faibles commissions

Les commissions pour le transfert des bitcoins à l'étranger sont bien plus faibles que celles appliquées par les sociétés spécialisées en la matière pour l'argent classique. Hourra ! Des sociétés comme Western Union peuvent appliquer des commissions pouvant atteindre 50 \$ pour des virements internationaux.



Vous pouvez arguer du fait que des métaux précieux peuvent être utilisés comme méthode de transfert de valeurs à travers le monde. Mais l'or et l'argent se voient appliquer des frais supplémentaires bien supérieurs à ceux des méthodes susmentionnées.



C'est dans ce domaine que le bitcoin fait excellente impression, notamment dans les pays où il est difficile d'ouvrir un compte bancaire ou d'utiliser des cartes de crédit. Le bitcoin représente alors une forme alternative de paiement qui peut être convertie en monnaie locale.

Plusieurs sociétés sont déjà sur le marché, ciblant l'Afrique et les Philippines. Ces services connaissent un assez gros succès à une petite échelle, mais il reste fort à parier qu'elles s'étendront dans les années à venir. Il y aura de multiples améliorations à apporter à ce système dans le futur dans la mesure où nous ne faisons que découvrir le potentiel de la chaîne de blocs.

Le même principe des faibles commissions s'applique à ceux qui reçoivent des bitcoins, puisque tout frais de transaction associé au transfert est payé par l'expéditeur. Cela offre de nombreux moyens aux sociétés pour réduire les frais généraux chaque fois qu'ils paient leurs employés, plus spécialement pour les travailleurs détachés dans différents pays. Enfin, cela réduit les délais de paiement qui, en fonction du moyen utilisé, peuvent être de plusieurs semaines.

## **Les inconvénients du bitcoin**

---

Le bitcoin est génial ! OK... ça nous le savons depuis le début du livre. Mais cessons un instant notre

prosélytisme pour mettre en évidence les potentiels inconvénients de cette crypto-monnaie.

## Conscience et compréhension

Si vous parlez du bitcoin à un français moyen, vous observerez probablement les deux attitudes suivantes :

- » Il a entendu parlé du bitcoin, car les journaux ont relaté des escroqueries dont Silk Road, Mt. Gox (et d'autres) ont été victimes.
- » Il n'a jamais entendu parlé du bitcoin ou bien en pointillé, et ne connaît en rien l'idéologie qui soutend cette monnaie. Le manque d'exposition du bitcoin est à l'origine de la faible adhésion du grand public.

## Plaider en faveur du bitcoin

Pour l'individu moyen, le bitcoin est avant tout affaire de technique. Il ne peut pas connaître les tenants et les aboutissants de l'utilisation du bitcoin au quotidien. Pour créer un portefeuille de bitcoins, vous devez installer un logiciel sur un ordinateur, ou une application sur un mobile. C'est tout ! (Vous en doutez ? Alors, consultez le [Chapitre 2](#).)

Il y existe une multitude de personnes qui n'ont jamais entendu prononcer le mot « bitcoin ». Et parmi celles

qui en connaissent le nom, très peu ont cherché à savoir ce qu'il cachait. De facto, nous observons un vrai problème d'information sur le bitcoin. Les analystes parlent ainsi d'une technologie qui est « en avance sur son temps ». Les personnes enthousiasmées par le bitcoin cherchent à convaincre les autres de les rejoindre dans l'univers de la crypto-monnaie. En effet, plus la masse d'utilisateurs augmentera, plus les informations sur le bitcoin circuleront.

L'aspect technologique est assez bien expliqué aujourd'hui auprès des sociétés commerciales. L'heure est donc venue d'en faire autant auprès des particuliers afin qu'ils envisagent concrètement les bénéfices qu'ils peuvent tirer du bitcoin. C'est pour cela que ce livre est entre vos mains. N'hésitez pas à faire part de son existence !

## Rencontrer des possesseurs de bitcoins

Si vous parvenez à convaincre quelqu'un d'utiliser des bitcoins, vous provoquerez un effet boule de neige. Chacun partagera son expérience avec des néophytes qui, une fois convaincus, partageront la leur à leur tour. La masse d'utilisateurs ne cessera d'augmenter.



Malheureusement, les conversations autour du bitcoin sont assez rares en société. Il existe quelques

conférences sur le sujet. Toutefois, comme l'entrée est généralement payante, elles ne sont constituées que d'un public restreint. La plupart de ces interventions sont ensuite postées sur YouTube. Surveillez les communautés en ligne pour accéder à des informations sans cesse actualisées.



Heureusement, il existe des groupes de rencontres locaux partout dans le monde. Ce type de réunion est l'un des meilleurs moyens de partager sa passion du bitcoin. L'avantage de ces rencontres est d'être gratuit. Vous trouverez votre groupe local et les dates de réunion sur <https://bitcoin.fr>. Dans le champ de recherche situé en haut à droite, tapez **meetup bitcoin**. Vous obtiendrez une liste de rencontres organisées autour de cette monnaie. Bien entendu, n'hésitez pas à organiser vos propres événements. Cela ne coûte rien, et la majorité des gens préfèrent que ce type de réunion se déroule dans un espace public comme un bar ou un restaurant, chacun payant ses consommations.

L'intérêt de ces rencontres est d'accueillir des personnes qui n'ont aucune connaissance sur le bitcoin. L'instant le plus sensationnel de ces réunions survient lorsque vous informez des néophytes sur les bienfaits de la monnaie électronique et de la technologie de la chaîne de blocs. Sachez alors ne pas entrer dans des explications trop techniques.

Le bitcoin peut fédérer des gens très différents. Mais une fois qu'un socle commun est trouvé, il devient facile d'engager une conversation. Dès lors que vous vous sentirez en confiance, il sera facile d'expliquer les tenants et les aboutissants de l'argent électronique en général et du bitcoin en particulier.

Les opportunités de devenir un orateur sur ce sujet ne manqueront pas. Les rencontres autour du bitcoin réunissent entre 5 à 150 personnes, tandis qu'une conférence en regroupe de 300 à 500.



Présenter c'est bien, mais convaincre de l'utilité du bitcoin, c'est encore mieux. Privilégiez alors l'interaction à l'ennuyeux exposé magistral.

Une fois que l'auditoire s'intéresse au concept du bitcoin, il cherche à en savoir davantage sur ses implications et sur sa technologie. Vous parlerez de tous ces aspects en évitant des mots aussi abstraits que « chaîne de blocs ». Contentez-vous de décrire ce qu'est le bitcoin, plutôt que d'expliquer ce qu'il cherche à faire.

## Confiance

La confiance est l'élément clé de tout moyen de paiement. Si vous n'avez pas confiance dans votre banque, vous n'ouvrirez jamais un compte courant, et

n'utiliserez pas une carte de crédit. Vous cacherez votre argent liquide dans le tiroir de votre table de nuit. Il en va de même pour les bitcoins : si vous ne leur accordez pas votre confiance, vous resterez attaché à une infrastructure financière classique. Consultez l'encadré « Faire confiance aux technologies modernes », plus loin dans ce chapitre pour changer de point de vue sur la modernité.



Eu égard à tous les gros titres sur les bitcoins et ses fraudes, le piratage, les services illégaux, et j'en passe, cette monnaie connaît un gros problème de confiance qu'il faut absolument résoudre. Pour cela, ne regardez pas le bitcoin comme une valeur économique solitaire, mais accordez votre confiance au réseau bitcoin dans sa globalité. Cela inclut des services associés, des sociétés, des coopératives de mineurs (ou coopératives minières), les utilisateurs actuels et ceux qui les rejoindront dans le futur.

Le bitcoin n'en est qu'à ses débuts. Au moment où nous écrivons ces lignes, il n'a que six ans d'existence. Comme tout moyen de paiement, son adoption est lente et doit faire face à beaucoup d'adversité. Une chose que le public oublie souvent est que le bitcoin n'a pas vocation à remplacer les moyens de paiement actuels. Il est fait pour attirer l'attention sur une manière plus transparente de procéder.



Posez-vous la question suivante : « Ai-je suffisamment confiance dans les infrastructures de paiement actuelles pour penser qu'elles peuvent sauvegarder éternellement mes données en toute sécurité, qu'elles ne les transmettent pas à des tiers, et qu'elles me protègent contre tout incident financier ? ». Si vous ne répondez pas de manière absolument affirmative, alors jetez un œil sur le bitcoin.

Pourtant, le consommateur continue à faire aveuglément confiance aux institutions financières alors qu'elles ont montré leurs limites et provoqué bien des dégâts dans les finances des ménages. En voici la principale raison : il est pratique d'utiliser un compte bancaire auquel est associée une carte. De plus, les banques ont installé un véritable monopole sur l'argent en proposant des services financiers et des rémunérations sans véritable alternative pour le client.

Aujourd'hui, il semble y avoir un éveil des consciences sur la dictature des institutions financières et sur la manière dont nous pouvons dépenser notre argent et, plus important encore, sur le volume de ces dépenses. Dans la plupart des pays, les banques limitent la quantité maximale d'argent que vous pouvez retirer par jour dans un distributeur. Idem pour les achats

effectués par carte bancaire. Il existe une limite sur 28 jours glissants.

Certes, en Occident, les consommateurs disposent d'autres options de paiement des marchandises et des services. Les cartes bancaires, les cartes de crédit, et même les virements sont très fréquemment utilisés, rendant les paiements en espèces quasiment obsolètes. Mais qu'arrivera-t-il quand les banques décideront de limiter les fonds que vous pouvez dépenser avec ces moyens de paiement ?



Les institutions financières traditionnelles veulent conserver les dépôts le plus longtemps possible. En effet, ça leur permet de prêter l'argent à d'autres fournisseurs de services et de se rémunérer sur les intérêts. C'est une des raisons pour lesquelles les virements prennent plusieurs jours. D'autres raisons tiennent à la lenteur inhérente des plateformes bancaires, comme le réseau SWIFT. Bien que le SEPA (Single Euro Payments Area) ait accéléré les virements dans les pays d'Europe, les performances et les fonctionnalités réelles se basent toujours sur la manière dont le système a été mis en œuvre dans chaque banque individuellement.

Bien qu'il n'y ait rien de mauvais dans ce système, les clients sont les premières victimes de ces retards. En effet, plus les délais sont longs, plus il y a de frais à



payer. Il existe des méthodes pour accélérer ces procédures, mais les infrastructures financières sont conservatrices.

Ou pour être plus précis, il y a une manière de modifier ce système en s'unissant et en demandant des changements. Aimeriez-vous que votre argent soit stocké sur un livre public que vous pouvez consulter à loisir, et envoyer de l'argent à n'importe qui dans le monde sans délais ni frais de transaction ? Si votre réponse est affirmative, alors penchez-vous sur le bitcoin.

Personne ne dit que vous devez placer toute votre confiance dans le bitcoin dès le départ. Mais si vous ouvrez votre esprit sur ce qu'est le bitcoin et ses objectifs, vous pourrez prendre une décision sagement mûrie sur le crédit à accorder aux monnaies électroniques.

## **FAIRE CONFIANCE AUX TECHNOLOGIES MODERNES**

Le consommateur accorde assez facilement sa confiance à des services qu'il utilise quotidiennement. Des réseaux sociaux comme Facebook, Twitter, et Instagram stockent de nombreuses informations à notre sujet. Et vous savez quoi ? Nous les communiquons avec beaucoup de consentement. Pourquoi ? Parce que nous leur accordons une certaine confiance au

partage de données avec des amis et des membres de notre famille.

Personne ne réalise tout à fait ce que ces sociétés peuvent faire de nos données. Lorsque vous ouvrez un compte sur ces réseaux, vous acceptez les termes et les conditions de leur utilisation. Elles stipulent qu'elles peuvent partager les données avec des tiers pour des raisons publicitaires et autres.

Ainsi, beaucoup font confiance à Google, Apple, Facebook et j'en passe, mais restent réfractaires au bitcoin. C'est la différence majeure qui existe entre des services qui n'impactent pas nos finances et ceux qui, au contraire, veulent perturber le monde de la finance. La nature humaine se méfie de tout ce qui est nouveau et qui modifie ses habitudes.

Maintenant, si toutes les banques avaient une chaîne de blocs – basée sur le système transactionnel, les transferts de fonds sur ce réseau seraient presque immédiats et les fonds disponibles dans les plus brefs délais. Avec un tel système en place, il n'y a aucune raison pour qu'un travailleur nigérien en France ne puisse pas envoyer de l'argent à sa famille en quelques minutes.

## Risques et volatilité

Le bitcoin est un outil financier générateur de risques comme n'importe quel autre moyen de paiement ou

devise. Cependant, ces risques sont sensiblement différents avec le bitcoin. L'un d'eux tient à un prix relativement volatil, mais une fois encore, quelle monnaie normale ne fluctue pas au quotidien ?



Le bitcoin et la technologie de chaîne de blocs réduisent la majorité des risques liés aux méthodes traditionnelles de paiement. Il n'y a pas de rétrofacturation, la fraude est compliquée du fait de la transparence, et les frais de transaction sont faibles comparés à ceux des cartes bancaires, des virements, et/ ou des services de paiement.



Cela ne signifie pas qu'il n'y a aucun risque avec le bitcoin. Il s'agit d'une nouvelle technologie avec une partie idéologique et une partie moyen de paiement. La technologie est encore en développement au moment où vous lisez ces lignes, et nous découvrons encore le potentiel de la chaîne de blocs. Donc, même si vous envisagez d'investir dans le bitcoin pour « soutenir » son développement technologique, des risques demeurent. Même les meilleures solutions et implémentations peuvent ne pas s'avérer viables au final... si personne ne les adopte.

Mais il existe l'autre versant de cette histoire. Le développement de la technologie de la chaîne de blocs montre, qu'à long terme, il y a de la place pour son expansion et la création d'emplois. Chaque nouvelle

technologie nécessite des personnes qui veulent bien la mettre en œuvre et la faire progresser, si possible d'une manière conviviale.

D'un point de vue technologique, il y a peu de risques à investir dans le bitcoin. Investir dans une entreprise qui travaille sur cette nouvelle technologie n'est pas plus risqué que d'investir dans n'importe quel autre type de société.



L'histoire n'est plus la même lorsque vous voulez spéculer sur le cours du bitcoin. Dans ce cas, les risques sont bien réels. Ce n'est jamais une très bonne idée de spéculer sur un cours volatil, comme celui du bitcoin qui varie constamment.

Les économistes et les investisseurs ont regardé de près le prix du bitcoin. Ce qui apparut d'abord comme jeton numérique inutile se transforma rapidement en une chose prenant de la valeur le jour où la la valeur des 1 dollar US fut atteinte. Et son prix continua de monter pour atteindre les 1 100 \$ en 2013. Beaucoup de personnes voyaient encore dans le bitcoin une fausse monnaie Internet.

Le bitcoin est toujours vu comme une sorte de fausse monnaie virtuelle. Pourtant, cet argent a fait pas mal de vague dans le monde de la finance. Les investisseurs de tout bord ont acheté des bitcoins sentant dans le

BTC une méthode sûre pour stocker et transférer des valeurs comparée aux métaux précieux ou aux méthodes traditionnelles de paiement.

## Usage limité (pour le moment)

Le bitcoin ne peut pas être utilisé dans tous les aspects de notre vie quotidienne, même si de nombreuses choses peuvent être payées en bitcoins sur Internet ou dans des boutiques. Il est toutefois possible de payer des factures en bitcoins en recourant aux services d'un tiers. Cependant, cela est contradictoire avec la philosophie du bitcoin qui cherche justement à éliminer les intermédiaires.

Il faudra encore quelques années avant que les commerçants commencent à proposer le prix de leurs marchandises ou de leurs services en bitcoins. Pour cela, il faut que le consommateur adopte le bitcoin comme moyen de paiement. Cette adoption n'interviendra pas tant que des efforts d'informations ne seront pas faits dans tous les pays du monde. Malheureusement, ces efforts sont surtout faits aux USA, et commencent seulement à se développer en Europe.



Il ne faut pas négliger les marchés émergents comme l'Afrique, l'Asie, voire l'Australie. Mais l'Asie et

l'Afrique sont des choix objectifs du fait de leur marché des transferts potentiel, le faible nombre de comptes en banque, et les prouesses technologiques.

Malgré tout cela, le bitcoin est une méthode de paiement qui peut être utilisée pour tout. Les cartes de débit en bitcoin en sont le plus bel exemple puisqu'elles permettent de payer en BTC quasiment partout où la carte bancaire est acceptée. Cependant, cela ne poussera pas les commerçants à accepter le bitcoin du jour au lendemain.

Il est également possible de payer ses factures en bitcoins, même si ces services sont limités aux zones du SEPA. Mais là encore, cela n'encourage pas les entreprises à accepter soudainement le bitcoin comme elles acceptent depuis toujours les virements bancaires.

La zone SEPA est constituée de pays européens où le protocole SEPA est appliqué par des banques et des institutions financières. Le SEPA permet aux citoyens d'effectuer, en un minimum de temps (généralement un ou deux jours ouvrables), des transferts en euros vers les autres pays utilisant cette monnaie. SEPA apparaît comme précurseur du bitcoin par cette modification importante apportée à un système financier tel que nous le connaissons. Bien que la technologie de la chaîne de blocs doive encore s'affiner, le bitcoin peut facilement être converti en différentes

devises et utilisé pour payer des marchandises et des services.

Avec le développement des paiements mobiles, le bitcoin va devenir un gros concurrent du système actuel. En réalité, les portefeuilles bitcoin mobiles furent développés bien avant que les institutions financières lancent leurs propres applications mobiles. Et la majorité de ces portefeuilles ont été améliorés ces dernières années, rendant ainsi le transfert de bitcoins bien plus simple à réaliser grâce à des codes QR scannés avec la caméra des téléphones.



Quoi qu'il advienne dans le futur, il y a fort à parier que le bitcoin, ou tout au moins sa technologie de la chaîne de blocs, y jouera un rôle majeur. Si les choses se déroulent comme prévu, la chaîne de blocs et le bitcoin deviendront les méthodes de transferts d'argent les plus utilisées avec des frais proches de zéro. Pour conclure, nous pouvons dire que le bitcoin est la meilleure forme d'argent jamais inventée.

# Chapitre 4

## Créer de l'argent avec le bitcoin

---

### DANS CE CHAPITRE

- » Présentation du minage de bitcoins
  - » Financer avec le bitcoin
  - » Échanger des bitcoins
  - » Acquérir des bitcoins
- 

Ce chapitre explique les différentes méthodes permettant de créer de l'argent avec le bitcoin. À vous d'utiliser celle qui correspond à vos besoins.

## Le minage des bitcoins

---

Le minage de bitcoins est une dénomination trompeuse. En effet, nous ne sommes pas dans Minecraft. Ce n'est pas à coups de pioche que vous extrairez de la pierre afin de découvrir des bitcoins. En d'autres termes, il n'existe pas de mines de bitcoins comme il existe des mines d'or. Le minage identifie l'introduction d'une plus grande quantité de bitcoins dans l'écosystème de la monnaie électronique.





En 2140, il y aura 21 millions de bitcoins en circulation. Au moment où nous écrivons ces lignes, le volume des bitcoins est de 15 millions.

## Fonctionnement du minage

Comment de nouveaux bitcoins naissent-ils ? Tout nouveau bitcoin est généré par un processus informatique appelé minage. Il s'agit d'un calcul mathématique très complexe qui peut être effectué à n'importe quel moment de la journée par votre ordinateur. De facto, vous faites partie intégrante du réseau bitcoin, non seulement dans la sécurisation du réseau via votre matériel dédié à cette tâche, mais aussi en générant de l'argent qui va être mis en circulation.

Il existe certaines similarités avec le minage d'autres ressources, comme l'or : l'offre disponible augmente lentement au rythme des extractions minières. Eh bien, en matière de bitcoins, l'extraction se fait en résolvant des équations mathématiques complexes qui exigent davantage de ressources au fil du temps.



Pour s'assurer qu'aucune monnaie autre que celle prévue ne soit générée quotidiennement, la procédure de minage est liée à ce que l'on appelle une difficulté cible. Cette difficulté augmente lorsque davantage de puissance de calcul s'ajoute au réseau, et elle diminue

quand un nombre plus restreint de mineurs participent au calcul.

## Une brève histoire du minage de bitcoins

Au fil des ans, le minage de bitcoins a connu une importante évolution en termes d'exigence matérielle. Ainsi, en 2009, très peu de matériel informatique était exigé, car un nombre réduit de gens trouvait un réel intérêt à ce projet. Mais, au fur et à mesure que le nombre de personnes s'intéressant au bitcoin augmenta, la puissance de calcul informatique nécessaire suivit de manière exponentielle. Le paramètre de difficulté (qui détermine la puissance nécessaire à la résolution des équations mathématiques) s'ajusta lui aussi pour assurer un intervalle de dix minutes entre chaque nouveau bloc. En d'autres termes, une équation est résolue toutes les dix minutes. Cet intervalle permet en effet de collecter autant de transactions possibles en un bloc et de les valider simultanément.

En 2009, les premières versions de client bitcoin disposaient d'un processus intégré permettant à chacun d'exécuter le logiciel de minage via leur CPU (processeur de leur ordinateur). Comme chaque ordinateur a un CPU, et qu'une poignée de personnes

effectuait ce minage en même temps, il y avait assez peu d'émulation. En fait, la majorité des bitcoins furent minés les premiers mois par Satoshi Nakamoto. Il distribua d'ailleurs des bitcoins à d'autres personnes afin de tester le réseau.

Il ne fallut pas beaucoup de temps pour s'apercevoir que le minage pouvait tirer profit des processeurs graphiques (GPU), et non pas juste des CPU. En effet, le GPU qui équipe une carte graphique étant spécialement conçu pour résoudre des calculs mathématiques complexes, il s'avéra bien plus efficace que le CPU dans cette tâche.

Toutefois, cette performance du GPU consomme beaucoup plus d'électricité que le CPU. Ce changement fut le premier chapitre de la course aux armements du minage de bitcoins.

Les développeurs et les ingénieurs commencèrent à plancher sur l'idée de créer un nouveau hardware capable de miner encore plus rapidement et plus efficacement qu'un GPU et un CPU. Les FPGA (Field Programmable Gate Arrays) virent le jour quelques années plus tard. Ils surpassèrent les CPU dans l'opération de minage. Par ailleurs, les FPGA pouvaient miner aussi vite qu'un GPU en consommant moins d'électricité.

Aujourd'hui, le minage repose sur l'ASIC (application-specific integrated circuit), un circuit intégré propre à une application spécialement conçue pour le minage de bitcoins. Le premier fut exploité début 2013, et surpassa tellement les GPU et les FPGA en performances que les mineurs jetèrent leur dévolu sur ces brillantes machines. Mais l'ASIC présente un inconvénient majeur : c'est un gouffre énergétique, bruyant, et dégageant une chaleur extrême. En revanche, un mineur ASIC de bitcoins est supérieur à n'importe quel type de matériel existant, et demeure très coûteux.

Plus l'utilisation de ces nouveaux périphériques se développa, plus les besoins électriques augmentèrent de manière exponentielle. De facto, le minage de bitcoins ne fut pas rentable dans de nombreuses régions du monde. Dans la majorité des cas, le coût de l'équipement combiné à la consommation électrique ne permettait pas de faire un quelconque bénéfice sur le minage réalisé chez soi. Mais il y avait une solution à ce problème : le cloud mining, une technique qui permet de miner en achetant de la puissance de minage sur des machines réparties partout dans le monde.

Le cloud mining est devenu très populaire ces dernières années. Il permet de miner sans investir dans un équipement puissant. La plupart des fournisseurs de ce minage en nuage informatique sont dédommagés

quotidiennement ou mensuellement pour leur surcoût d'électricité. Cette technologie permet à un utilisateur de gagner directement de l'argent plutôt qu'attendre le bon vouloir de machines fantaisistes. Le [Chapitre 11](#) donne davantage de détails sur le cloud mining.

Dans le futur, nous pouvons imaginer que les microprocesseurs seront plus petits, plus rapides, et plus économes en énergie. Les ingénieurs tentent de réduire l'alimentation électrique de ces puces. En rendant le minage plus efficace énergétiquement, il pourra devenir bénéfique dans un nombre plus important de pays.

## Échanger des bitcoins

L'échange de bitcoins est l'une des manières les plus lucratives d'utiliser cette crypto-monnaie. La valeur du bitcoin est volatile. Cela signifie que son cours varie régulièrement à la hausse et à la baisse. Des traders expérimentés sont capables de prédire ces variations.



Savoir acheter et vendre au bon moment permet de faire de bonnes plus-values. Toutefois, dans un marché de l'offre et de la demande, il faut aussi accepter de perdre de l'argent. Donc, effectuez ce type d'opération à vos risques et périls. On vous aura prévenu.

## Day trading contre monnaie fiduciaire

Le day trading (spéculation en séance) consiste à vendre et à acheter des instruments financiers – comme des bitcoins – pendant la même séance spéculative. La monnaie fiduciaire, quant à elle, se réfère au cours légal de la monnaie dans chaque pays.

Utiliser le bitcoin permet d'échanger de plusieurs manières. La méthode la plus objective consiste à échanger des bitcoins de et vers les devises locales. Dans la majorité des cas, les gens décident de s'en remettre aux marchés monétaires connus, car ils génèrent un plus gros volume d'échanges que des devises plus petites. Par conséquent, le plus gros marché est la Chine où le BTC est échangé contre des yuan chinois (CNY). En fonction de votre pays, vous pourrez ou non accéder facilement au CNY à des fins commerciales. Mais, un rapide coup de fil ou déplacement à votre banque peut vous permettre de collecter des informations utiles sur la manière d'obtenir des yuan chinois et sur le taux de change en supposant, bien entendu, que votre objectif est ensuite d'investir le marché chinois du bitcoin.

D'autres devises majeures peuvent facilement être converties de et vers des bitcoins. Au moment où nous

écrivons ces lignes il s'agit de :

- » la livre anglaise ;
- » le dollar canadien ;
- » l'euro ;
- » le rouble russe ;
- » le dollar US.



Si vous possédez des bitcoins, inutile d'obtenir au préalable des monnaies fiduciaires pour commencer votre expérience du day trading. Il suffit de choisir votre devise d'échange. Le bitcoin est réputé pour sa nature volatile. Il y a donc des risques de pertes et des chances de gains lorsque vous « boursicotez » ainsi tous les jours. Parfois, ces gains et ces pertes peuvent être considérables, parfois pas. C'est la cruelle incertitude des spéculations.



La spéculation peut également se faire autrement que par la vente et l'achat de bitcoins. Plusieurs plateformes permettent de spéculer sur la hausse ou la baisse du prix du bitcoin par rapport à un certain marché – même s'il n'accepte pas le bitcoin comme moyen de paiement. Cela inclut :

- » Vauloro (<https://vauloro.com>), un échange bitcoin/ or

- » Kraken échange de bitcoins contre des devises (<http://kraken.com>)
- » Plus500 ([www.plus500.fr](http://www.plus500.fr))
- » Avatrade ([www.avatrade.fr](http://www.avatrade.fr))
- » Etoro ([www.etoro.com/fr](http://www.etoro.com/fr))



Même si quelques commerçants acceptent d'être payés en bitcoins, presque tous les fonds sont convertis directement dans une monnaie légale. Pourquoi ? Eh bien pour protéger les commerçants de la volatilité du bitcoin, volatilité qui reste une des raisons majeures qui les poussent à traîner des pieds face à la monnaie électronique.

En revanche, ces conversions ont un effet indésirable : les processeurs de paiement doivent liquider ces paiements en bitcoins le plus rapidement possible pour régler au commerçant la somme exacte. Il en résulte un nombre d'ordres de vente colossal qui offre l'opportunité d'acquérir des bitcoins à bas prix.



Ne spéculiez pas si vous avez un cœur fragile ! De nombreux facteurs peuvent faire varier le cours du bitcoin. Un piratage ou bien des décisions prises pour ou contre le bitcoin affecteront sa valeur. Sachez qu'il n'y a pas toujours une raison bien définie pour justifier la variation du cours du bitcoin.



## Day trading contre altcoins

Si vous ignorez tout du day trading, consultez la précédente section. Maintenant, laissez-moi vous présenter les altcoins – également connus comme des monnaies alternatives. Il s'agit de clones de bitcoins, des concurrents au bitcoin. Il en existe plus de 4000 différentes.

Si vous n'aimez pas échanger ou spéculer avec les marchés de la monnaie fiduciaire, vous pouvez le faire avec les monnaies alternatives. Les altcoins cherchent à améliorer l'idée du bitcoin. Certaines personnes souhaitent davantage d'anonymat, tandis que d'autres développeurs veulent explorer les limites de la technologie de la chaîne de blocs. Plutôt que de soumettre leurs idées aux développeurs du bitcoin, ils utilisent le code bitcoin, en changeant le nom, apportent des améliorations mineures, et lancent alors une nouvelle monnaie électronique.



Au fil des ans, seule une dizaine d'altcoins ont réussi à s'imposer, et cela grâce à une importante communauté et à l'intégration de fonctions uniques qui n'ont pas encore été implémentées dans le bitcoin. Néanmoins, aucune de ces communautés alternatives n'est aussi développée et soutenues que celle du bitcoin. Mais cela ne signifie pas qu'aucune spéculation n'est faite sur la

scène des altcoins. Beaucoup de traders préfèrent spéculer sur les marchés des altcoins, car il y a de la place pour de rapides profits, mais aussi pertes.

La plupart des altcoins sont créés par des groupes pump-and-dump. Il s'agit de développeurs qui font beaucoup de battage autour de leur monnaie et qui promettent des fonctions uniques et très intéressantes. Il suffit que des personnes croient en ces promesses pour qu'elles deviennent désireuses d'acheter à un très bas prix. Cette action a bien évidemment comme effet de faire grimper le cours de l'altcoin. Les quelques monnaies alternatives qui sont les mieux positionnées actuellement ne sont pas « gérées » par des groupes pump-and-dump. Il s'agit de Litecoin, CasinoCoin, et Guldencoin.



Plutôt que de faire monter le prix en vendant, certains développeurs d'altcoins encouragent les membres de la communauté à placer beaucoup d'argent pour faire monter le cours de l'altcoin. Une fois ce cours suffisamment haut, ces développeurs retirent leurs fonds, prennent leur argent, et créent une nouvelle monnaie la semaine suivante.



Il y a beaucoup d'altcoins à découvrir. Cependant, la plupart d'entre eux ne servent à rien. Mais, si vous parvenez à vous procurer cette monnaie à bas prix, il y a probablement un beau profit à réaliser. Toutefois, ne

devenez pas trop cupide, car le cours peut baisser beaucoup plus vite qu'il ne monte.

## Bitcoin et financement participatif

---

Le financement participatif ou crowdfunding permet de lancer un projet via des plateformes Internet afin d'obtenir de l'argent auprès de contributeurs, en général privés, pour financer un projet culturel, humanitaire, associatif, etc. En acceptant le bitcoin comme moyen de paiement de votre crowdfunding, vous décentralisez davantage ce financement et pouvez toucher un nombre encore plus important de personnes.

Le bitcoin apparaît donc comme un outil puissant pour soulever des fonds dans l'optique de financer un projet à venir ou existant. Dans la mesure où le bitcoin n'est pas taxé dans la majorité des pays, de nombreuses personnes voient en lui une sorte de « paradis fiscal » pour financer des projets.



Lorsque vous convertissez en monnaie locale les fonds ainsi obtenus, une taxe peut s'appliquer en fonction du volume d'argent que vous recevez.



Ne lancez jamais un financement participatif pour un faux projet ou pour obtenir de l'argent qui ne servira

pas le but pour lequel les gens vous ont accordé leur confiance. Cela s'appelle de l'escroquerie et vous devrez en répondre devant la justice.

Mais rassurez-vous. La proportion de faux projets dans ce domaine est infime. En fonction du type de projet que vous présentez, il vous faudra parfois attendre un peu plus longtemps que vous le souhaitez pour réunir les fonds, notamment si cela nécessite la mise en œuvre d'une chaîne de blocs.

Mais tous les projets ne s'en remettent pas à des plateformes de crowdfunding pour de bonnes raisons. Certaines personnes voient dans le financement participatif une manière de réunir rapidement des fonds, sans être obligé de rembourser les contributeurs si le projet capote. Bien que la majorité des plateformes mettent en place un système de sécurité pour identifier une utilisation suspecte de leur outil, force est de constater que les projets tiennent généralement leur promesse.

Mais toutes ces considérations sur le crowdfunding n'ont rien à voir avec le bitcoin lui-même qui, au final, n'est qu'un moyen supplémentaire mis au service des contributeurs. Consultez des statistiques sur les contributions et les projets menés à terme à l'adresse [www.kickstarter.com/help/stats](http://www.kickstarter.com/help/stats).



Lorsque vous contribuez à un financement participatif en bitcoin, vérifiez si des contreparties sont prévues. Le crowdfunding diffère de l'achat de parts dans une société ou d'un produit à un tarif plus intéressant. Contribuer à un crowdfunding consiste à dépenser de l'argent pour aider quelqu'un à réaliser son rêve avec ou sans contrepartie pour vous à la clef. Donc, philosophiquement, vous n'aidez pas quelqu'un pour obtenir quelque chose en retour. C'est l'idée du financement participatif.

## Comprendre ICO et IPO

Initial coin offering (ICO) ou levée de fonds, et Initial public offering (IPO) ou introduction en bourse ne sont pas des droïdes Star Wars. Ce sont des termes financiers :

- » **ICO** : Les investisseurs potentiels peuvent acheter une partie des altcoins disponibles avant que ne commence la procédure de minage. La plupart des investisseurs le font dans l'espoir de voir le prix de la monnaie augmenter dans un futur proche.
- » **IPO** : Une IPO identifie ici une levée de fonds en crypto-monnaie. Des investisseurs reçoivent des dividendes d'une société et réalisent des intérêts.

Les deux termes ont une connotation légèrement négative dans le monde du financement participatif par bitcoins. En effet, de fausses promesses et des projets frauduleux ont souvent été associés à l'ICO et à l'IPO. Bien entendu, ils sont aussi utilisés de manière tout à fait honnête.

Par exemple, chaque fois que vous envisagez de créer une nouvelle utilisation de la technologie de la chaîne de blocs qui met en œuvre son propre jeton, vous déterminez en fait une ICO. Pour un certain volume d'investissement, l'utilisateur recevra X jetons en retour qu'il utilisera sur la nouvelle plateforme une fois qu'elle sera lancée. Vous offrez ainsi une contrepartie tangible à vos « bailleurs », et cela même si elle ne prend pas une forme physique. Le succès de votre projet déterminera ou non le gain de valeur de ces jetons numériques. Parallèlement, vous incitez les « donateurs » à propager dans le monde l'existence de votre crowdfunding, ce qui contribuera grandement au succès de la plateforme.

Vous n'avez pas à distribuer des jetons numériques à ceux qui veulent récupérer votre projet. Toutefois, les investisseurs – gros ou petits – ne souhaitent obtenir rien d'autre qu'un retour sur investissement, et cela le plus tôt possible. L'utilisation d'une ICO/IPO peut vous

y aider selon l'ampleur de votre projet et ce qu'il va impliquer.



Vous vous ajouterez un facteur de stress chaque fois que vous créerez (ou investirez) dans un projet mettant en œuvre une ICO ou une IPO. En tant qu'investisseur, vous devrez suivre la progression et vérifier le rendement. En tant que développeur ou créateur du projet, vous devez assumer vos responsabilités, notamment dans la distribution des actifs numériques aux bonnes personnes.

Créer une campagne de crowdfunding avec une IPO/ICO génère à la fois excitation et attentes. Bien que les gens puissent apprécier la valeur intrinsèque de votre projet, ils porteront aussi un regard attentif sur l'aspect spéculatif de leur participation. Et s'il y a une chose que nous pouvons affirmer sur les personnes qui vous témoignent leur confiance en vous donnant de l'argent, c'est qu'elles ne font pas partie des gens les plus patients au monde.

## Offrir des parts et des dividendes

Plutôt qu'offrir des actifs numériques aux potentiels investisseurs, proposez-leur des parts sociales en échange de leur contribution. Avec cette approche, vous pourrez demander un peu plus ou un peu moins selon

vos désirs, mais toujours en assurant que ces parts ont une valeur réelle.



Ces valeurs de parts peuvent être rémunérées de manière hebdomadaire, mensuelle, ou même sous forme de dividendes trimestriels versés aux actionnaires. Une fois encore, cela incitera les investisseurs à parler de votre projet ou de votre entreprise.

Pour rendre l'offre encore plus attrayante, vous pouvez verser les dividendes en bitcoins. Bien que les montants risquent d'être assez faibles au début, les investisseurs recevront tout de même un premier retour sur investissement. De plus, chacun y verra une indication parlante sur la manière dont la société (ou le projet) est dirigée et sur les améliorations qui seront apportées dans le futur.



Le principe du paiement des dividendes en bitcoins peut également s'appliquer à de potentiels investisseurs qui préfèrent les moyens traditionnels de paiement. Une fois qu'ils vous ont adressé les fonds désignés, vous pourrez leur verser des dividendes en bitcoins pour leur permettre de se familiariser avec cette crypto-monnaie.

## Maintenir les bitcoins pour



# l'avenir

---

Le bitcoin attire de nombreux spéculateurs du monde entier. Sachant que le cours du bitcoin fluctue constamment, vous pouvez gagner beaucoup d'argent en achetant des bitcoins à bas prix dans l'espoir de réaliser une bonne affaire dans un futur proche.



N'oubliez pas qu'en 2140, il y aura 21 millions de bitcoins en circulation. Il semble donc évident que le prix du bitcoin augmentera dans le temps. Nous verrons bien si nos prévisions sont exactes ou pas... enfin, si nous vivons jusque-là.

## Conduire votre véhicule d'investissement vers l'avenir

Le bitcoin est assimilé à un véhicule d'investissement. Aux premiers jours du bitcoin, beaucoup de personnes achetèrent une monnaie bon marché en espérant que le réseau se développerait et que le cours du bitcoin monterait. C'est en gros ce que l'on peut appeler un véhicule d'investissement.

Cecla étant dit, le prix du bitcoin a parcouru du chemin depuis son lancement en 2009. Au début, chaque bitcoin miné fut virtuellement inutile. Cette tendance se poursuivit jusqu'à ce que le réseau commence à se

développer et que de plus en plus de personnes montrèrent leur intérêt pour le bitcoin.

Le prix du marché connut une lente mais stable progression entre 2010 et 2013. 2013 fut d'ailleurs une année très intéressante pour le bitcoin, durant laquelle la valeur augmenta très vite pour atteindre les 1 163 \$ US. Comme nous pouvions nous y attendre, ce prix ne se stabilisa pas, et la valeur commença à baisser lentement.

## DEUX PIZZAS POUR 10 000 BITCOINS ?

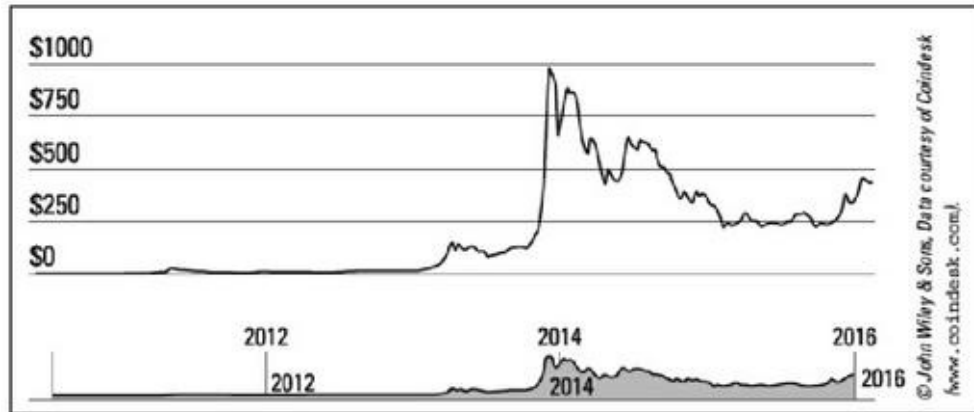
La « valeur du bitcoin » commença à intéresser les médias lorsqu'un utilisateur nommé Laszlo sur BitcoinTalk ([www.bitcointalk.org](http://www.bitcointalk.org)) offrit, sur un forum, 10 000 BTC pour l'achat de deux pizzas. Un autre forum d'utilisateurs de BitcoinTalk proposa de commander deux pizzas chez Dominos et de les livrer chez Laszlo en échange de cette offre.

Ce jour-là marqua la première transaction « officielle » de bitcoins pour un produit et un service enregistré sur la chaîne de blocs. Ainsi, le 22 mai 2010 est connu sous le nom de Laszlo's Pizza Day et a de multiples célébrations à travers le monde. Cette journée fut celle où l'enthousiasme vis-à-vis du bitcoin commença à croître avec des discussions passionnées autour du bitcoin et de sa chaîne de blocs.

Après cette journée, de plus en plus de personnes commencèrent à apprécier la valeur potentielle du bitcoin, et les

investisseurs se procurèrent autant de bitcoins que possible. Des personnes fortunées, comme les jumeaux Winklevoss (qui ont vu Facebook leur passer sous le nez), se fixèrent comme objectif de posséder systématiquement 1 % des bitcoins en circulation. Cela révèle une forte ambition lorsque l'on sait que le nombre total de bitcoins en circulation sera de 21 000 000 en 2140.

Jusqu'à fin 2014 et début 2015, le prix du bitcoin ne cessa de baisser malgré une adoption commerciale de plus en plus marquée et un nombre grandissant de créations de portefeuilles. Certains experts financiers virent là le talon d'Achille du bitcoin, tandis que d'autres considérèrent que cette monnaie électronique perturbatrice entraînait dans une nouvelle ère. En termes purement financiers, il y eut une bulle dans la valeur du bitcoin suivie par un crash qui replaça le prix au niveau où il était avant cette bulle spéculative. Au moment où nous écrivons ces lignes, personne ne peut savoir qui a tort ou raison. Mais une chose est sûre : les rapports annonçant la disparition du bitcoin sont grandement exagérés. La [Figure 4.1](#) montre les variations du cours du bitcoin au fil des ans.



**FIGURE 4.1** : Les fluctuations du bitcoin.

## Rentabiliser votre butin

Beaucoup utilisent le bitcoin comme un moyen de spéculer. De facto, les investisseurs achètent au plus bas prix pour revendre au plus haut, sans acheter quoi que ce soit avec cette crypto-monnaie.



L'avenir du bitcoin pose question lorsqu'il y a autant d'argent qui ne circule pas pendant une période inconnue. Lorsque la valeur semble horizontalement à la dérive sur les graphiques, il apparaît que la demande baisse sensiblement. D'un autre côté, avec autant de personnes qui détiennent une grande quantité de bitcoins, cette monnaie paraît être à l'abri d'une chute spectaculaire qui lui ferait atteindre le cours qui était le sien avant 2013.

Mais il faut s'attendre à ce que certains impatients liquident leurs actifs. Dans ce cas, le bitcoin

n'échappera pas aux conséquences d'une vente massive. Toutefois, le besoin de rentabilité est aussi garant d'une certaine stabilité de cette monnaie. Bref, tout est question de psychologie.

Le bitcoin est l'une des monnaies électroniques dont le volume est prédéfini. Ainsi, au jour d'aujourd'hui, 75 % du volume total est en circulation. Malgré cela, il existe une petite pénurie dès lors que les bitcoins ne sont ni dépensés ni vendus à d'autres investisseurs.

Cela laisse aux parties intéressées une plus petite quantité d'argent à acheter ; achat qui, à son tour, provoquerait une augmentation de la valeur. En fonction de la somme que certaines de ces personnes cupides ont payée, il faudra beaucoup de temps avant que le prix du BTC s'établisse à une valeur les incitant à vendre des actifs.



Thésauriser ainsi peut s'avérer être un problème dans le monde du bitcoin. Mais n'oublions pas que cette monnaie électronique n'est âgée que de six ans. Il lui reste encore beaucoup de temps pour se développer, parvenir à maturité, et être adoptée d'une manière plus globale. Tant que ça ne sera pas le cas, le bitcoin sera vu et adopté uniquement comme un véhicule d'investissement.

Vérifiez le graphique du cours instantané du bitcoin à l'adresse

<https://bitcoinwisdom.com/markets/bitstamp/btcu>

## Acquérir des bitcoins

---

Plutôt que d'acheter des bitcoins sur une plateforme de change comme nous l'expliquons au [Chapitre 2](#), vous pouvez en acquérir d'une autre manière. Pour participer activement au développement de cette crypto-monnaie et en apprécier toutes les implications futures, commencez par vous inscrire sur un forum. Voici d'excellents exemples :

- » BitcoinTalk (<https://bitcointalk.org/>)
- » Bitcoin subReddit ([www.reddit.com/r/Bitcoin/](http://www.reddit.com/r/Bitcoin/))

## Acquérir via des forums

La majorité des discussions se déroulent sur BitcoinTalk à l'adresse [www.bitcointalk.org](http://www.bitcointalk.org), où les possibilités de gagner des bitcoins ont augmenté proportionnellement à la popularité grandissante de son forum. Il s'avère être une place de choix pour des sociétés qui souhaitent faire connaître leur activité.



Les signatures de forum (placées en bas des profils et visibles sous chaque post) permettent aux utilisateurs

de BitcoinTalk de gagner une faible quantité de bitcoins chaque fois qu'ils y abordent positivement le sujet. La personne qui organise cette campagne piste le nombre de vos posts par semaine et vous verse la somme sur laquelle vous vous êtes entendu. Pour entrer dans ce processus, il vous faut lancer des discussions constructives provoquant des réactions elles aussi constructives qui vous rapporteront également des bitcoins.

Les récompenses des campagnes de signatures dépendent de plusieurs facteurs. Tout d'abord entre en ligne de compte le budget de la société qui rémunère. L'argent obtenu dépendra totalement de cette surface financière. Dans certains cas, cette somme est proche de zéro. Dans d'autres, elle s'avère être assez substantielle. Beaucoup de choses reposent sur le produit ou le service que la société cherche à promouvoir, et sur la quantité d'interactions que génère la campagne de signature en général, sur un forum particulier.

Ensuite, certaines campagnes limitent le nombre de posts que vous pouvez publier sur une période donnée. La période de paiement se fait sur un laps de temps défini pendant laquelle l'utilisateur peut créer des posts afin de promouvoir la campagne de signatures. En règle générale, ce paiement s'effectue de manière

hebdomadaire, et la société qui a lancé le projet publicitaire peut décider de limiter le nombre de publications par semaine. Tout post au-delà de cette période ne sera pas rétribué.



Un des facteurs les plus importants pour savoir si le forum est bon dépend de votre statut sur BitcoinTalk. Les membres qui sont très actifs et qui interviennent dans de nombreuses conversations verront leur « classement » monter dans le forum. Plus vous êtes à un niveau élevé, plus le forum sera rentable pour vous.

Des utilisateurs légendaires dont le niveau d'activité est supérieur à 850, et les utilisateurs héro avec un niveau dépassant 500 gagnent généralement pas mal de bitcoins. De plus, ils sont rarement limités dans leur nombre de posts sur une période donnée.



Polluer le forum avec des messages courts et abscons entraînera votre exclusion de la campagne de signatures.



Pour plus d'informations sur les campagnes de BitcoinTalk, consultez la page <https://bitcointalk.org/index.php?board=52.0>.

## Acquérir en travaillant

Plusieurs plateformes proposent du travail payé en bitcoins. Ne voyez pas cela comme une possibilité de



changer de carrière. Il s'agit davantage d'un complément de revenus qui vous permettra d'asseoir une réputation et de gagner parallèlement un peu d'argent.

Malheureusement, un nombre limité de ces tâches rétribuent suffisamment. De facto, voyez cela comme la possibilité de mettre un pied dans une activité qui pourrait se développer dans le futur.



Lorsque vous acceptez d'effectuer un travail en échange de bitcoins, veillez à intervenir pour des personnes et des entreprises légales. En effet, cela garantit le sérieux de l'activité, donc celle du paiement de votre travail.

Comme pour n'importe quelle activité rémunérée, vous devez d'abord effectuer votre tâche avant de revendiquer un salaire. Comme il n'y a généralement aucun contrat de signé entre les deux parties, ne sautez pas aveuglément sur la première opportunité venue.

Il existe aussi des travaux plus rémunérateurs. C'est le cas pour les programmeurs en PHP, SQL, JavaScript, ou C#.

Le bitcoin est une branche économique encore très jeune, et de nombreuses sociétés pensent qu'elles ont tout ce qu'il faut pour jouer un rôle dans ce secteur prometteur. Il résulte de cette perspective d'avenir un développement des opportunités économiques qui ne

cesseront de se présenter dans les prochaines années. Les intervenants seront rémunérés en BTC, ainsi que les actions et leurs dividendes. Le télétravail sera également de mise, même si de nombreux jobs nécessiteront une présence physique dans l'entreprise.



En fonction de votre lieu d'habitation, tout revenu perçu en bitcoins pourra être taxé. Vérifiez auprès de votre administration fiscale pour savoir si le bitcoin fait l'objet d'une déclaration dans votre pays.

## Acquérir via des robinets (faucets)

Une des méthodes les plus faciles pour acquérir des bitcoins s'appelle les robinets (faucets). Un robinet est un site Web où des utilisateurs peuvent demander une petite quantité de bitcoins pendant un certain laps de temps allant de quelques minutes à plusieurs jours.



Ne comptez pas devenir riche en une nuit ! Les robinets ne coulent pas à flots. Ils « déversent » en réalité très peu de bitcoins. En revanche, vous n'avez absolument rien à faire pour les gagner.

Les robinets à bitcoins fonctionnent sur un principe très simple : ils distribuent des bitcoins tant que des entreprises payent pour afficher leur bannière publicitaire. Le fait de cliquer sur de telles bannières

génère un petit revenu pour le site qui l'héberge. Une fraction de ces revenus est redistribuée, et l'origine des fonds est connue. Dans la plupart des cas, les opérateurs de robinets à bitcoins sortent l'argent de leur propre poche les premières semaines voire les premiers mois, jusqu'à ce qu'ils génèrent suffisamment de trafic et de publicité.



Pour les utilisateurs débutants, les robinets à bitcoins permettent d'acquérir cette crypto-monnaie sans effort et sans dépenser d'argent. Toutefois, ces robinets ne vous rapporteront guère plus de 2 à 3 euros, même si vous y passez la journée. La rentabilité horaire n'est pas de mise ici, car il existe d'autres moyens bien plus efficaces pour gagner des bitcoins, comme les campagnes de signatures des forums ou l'exécution de microtâches, comme cela est expliqué dans la précédente section.

Pour plus d'informations sur les robinets à bitcoins, consultez la page Web [www.robinetabitcoin.com/](http://www.robinetabitcoin.com/).

# Gérer des bitcoins

## QUATRE TYPES DE PORTEFEUILLES DE BITCOINS

- » Logiciel portefeuille : Une application installée sur votre ordinateur pour gérer vos bitcoins.
- » Portefeuille matériel : Un périphérique physique où vous stockez vos bitcoins.
- » Portefeuille sur papier (ou porte-monnaie papier) : Pas vraiment du papier, mais une méthode de stockage très sécurisée des bitcoins qui n'est pas connecté à la chaîne de blocs. Également connu sous le nom de stockage à froid.
- » Portefeuille en ligne : Une société tierce partie qui agit comme intermédiaire, gérant vos bitcoins et administrant votre compte.

## DANS CETTE PARTIE...

- » Conserver vos bitcoins dans différents types de portefeuilles.

- » Tout savoir sur les transactions, les confirmations réseau, et les frais.
- » Mettre les mains dans le moteur de la chaîne de blocs et comprendre en quoi elle peut vous être utile.

# Chapitre 5

## Votre portefeuille de bitcoins

---

### DANS CE CHAPITRE

- » Comprendre le fonctionnement des portefeuilles
  - » Examiner les différents types de portefeuilles
  - » Assurez la sécurité de votre portefeuille
- 

Si vous avez lu d'autres chapitres précédant celui-ci, vous savez grosso modo à quoi correspond un portefeuille (ou porte-monnaie) de bitcoins. Sinon, vous vous demanderez certainement de quoi il retourne. Mais sachez que, dans tous les cas, ce chapitre va entrer les détails de cet élément important de l'univers du bitcoin.

Comme son nom l'indique, un portefeuille de bitcoins est un emplacement de stockage des informations directement liées aux bitcoins que vous possédez. Ainsi, ce portefeuille stocke vos fonds – comme un compte bancaire – tout en permettant d'envoyer et de recevoir des bitcoins.



Il n'est pas exagéré de dire qu'un portefeuille de bitcoins est la seule chose la plus importante à protéger.

Une fois le portefeuille logiciel installé sur votre ordinateur ou votre appareil mobile (comme expliqué au [Chapitre 2](#)), une adresse de portefeuille de bitcoins vous sera proposée. Il s'agit d'un numéro d'identification qui vous reconnaît comme membre du réseau bitcoin. Il fonctionne comme un numéro de compte pour envoyer, recevoir, et stocker des bitcoins.

## Déverrouiller les clés publiques et privées

---

Un portefeuille n'est pas qu'une simple adresse. Il contient également la clé publique et privée de chacune de vos adresses bitcoin. Votre clé privée est une chaîne aléatoire de chiffres et de lettres qui permet de dépenser votre crypto-monnaie. Cette clé est mathématiquement liée à l'adresse de votre portefeuille. Grâce à un code de cryptage très puissant, aucune décompilation n'est possible.



Si vous ne sauvegardez pas votre clé privée et que vous la perdiez, il deviendra impossible d'accéder à votre portefeuille.



Vous en saurez davantage sur les clés privées à l'adresse <https://bitcoin.fr/qu-est-ce-qu-une-cle-privee/>.

Il existe aussi une clé publique. Cette clé est confondue, à tort, avec l'adresse du portefeuille. En fait, un portefeuille de bitcoins est une version cryptée de votre clé publique.



La clé publique est une chaîne de 256 bits de long – et la hash finale (c'est-à-dire l'adresse du portefeuille) est de 160 bits. La clé publique est donc utilisée pour confirmer que vous êtes bien le propriétaire d'une adresse qui peut recevoir des fonds. Elle est mathématiquement dérivée de votre clé privée, mais inversée ; se lancer dans des calculs pour trouver la clé privée accaparerait le plus puissant des superordinateurs pour plusieurs trillions d'années.

Parallèlement à ces deux clés et à une adresse de portefeuille, votre portefeuille de bitcoins stocke un registre de toutes vos transactions entrantes et sortantes. Chaque transaction liée à votre adresse sera stockée dans le portefeuille afin de permettre aux autres utilisateurs de contrôler leurs habitudes d'achat et de vente.

Enfin et surtout, un portefeuille de bitcoins stocke aussi vos préférences d'utilisateur. Cependant, ces



préférences dépendent du type de portefeuille que vous utilisez et de la plateforme où vous l'avez créé. Le client Bitcoin Core, par exemple, ne propose que très peu de préférences, évitant ainsi bien des confusions dans l'esprit des débutants.

## DANS L'INTIMITÉ DE VOTRE CLÉ PRIVÉE

La clé privée de votre portefeuille de bitcoins est l'information la plus importante à sauvegarder et à sécuriser constamment. Ce « chiffre secret » permet de dépenser les bitcoins de votre portefeuille, puisqu'il est utilisé pour vérifier que vous êtes bien le « propriétaire » légitime de la monnaie associée à votre adresse.

Un portefeuille de bitcoins, qu'il soit installé sur un ordinateur ou un périphérique mobile, peut contenir plusieurs clés privées, chacune sauvegardée dans le fichier wallet.dat.

Les clés privées des portefeuilles de bitcoins sont des nombres de 256 bits qui peuvent être représentés de plusieurs manières. La clé suivante est au format hexadécimal qui se compose de 32 octets ou 64 caractères de long. Chacun d'eux est compris entre 0 et 9 ou entre A et F :

```
E9 87 3D 79 C6 D8 7D C0 FB 6A 57 78 63 33 89 F4 45 32 13 30 3D  
A6 1F 20 BD 67 FC 23 3A A3 32 62
```

Ainsi, sans clé privée, les fonds stockés dans une adresse de portefeuille de bitcoins ne pourront pas être utilisés. Or, il est virtuellement impossible de déceler le déchiffrement d'une clé

privée à partir de la clé publique et/ou de l'adresse du portefeuille lui-même. Cela fait du bitcoin l'un des protocoles de cryptage les plus complexes à craquer.

En revanche, afficher la valeur d'une clé publique (qui correspond à l'adresse bitcoin) ne nécessite pas de connaître la clé privée. La clé publique associée à l'adresse du portefeuille permet de recevoir des bitcoins, et également d'en afficher le solde. Mais sans clé privée, il n'y a aucune manière de dépenser les bitcoins associés à l'adresse de votre portefeuille de bitcoins.

Le meilleur moyen de sécuriser vos bitcoins consiste à les dépenser depuis une autre adresse de portefeuille. Les bitcoins ne peuvent être dépensés qu'une seule fois. Ainsi, dès que le contenu d'une adresse a été utilisé, la clé privée devient inutile.



Votre portefeuille génère un fichier « maître » qui contient l'ensemble de vos informations. Pour les utilisateurs d'ordinateur, ce fichier est appelé wallet.dat. Il est enregistré sur une machine Windows dans le dossier C:/User/Votrenom/Documents/AppData/Roaming/Bitcoin/. Créez toujours plusieurs sauvegardes du fichier wallet.dat sur d'autres périphériques de stockage, tels qu'une clé USB ou une carte mémoire. Le logiciel vous permettra d'importer le fichier wallet.dat au cas où sa version d'origine se trouverait perdue ou endommagée, de restaurer vos paramètres précédents, et d'inclure tous les fonds associés à l'adresse de votre portefeuille de bitcoins.

Pour plus d'infos sur l'importation des clés privées et des fichiers wallet.dat, consultez <https://bitcoin.fr/comment-importer-une-cle-privee/> ainsi que l'encadré « Dans l'intimité de votre clé privée ».

## **Garder la main sur un portefeuille de bitcoins**

---

Lorsque vous retirez des billets à un distributeur, vous les mettez généralement dans votre portefeuille ou dans votre sac à main. Surprise, surprise : les bitcoins doivent eux aussi être entreposés quelque part afin que vous puissiez les retrouver lorsque vous en avez besoin. Il existe pour cela plusieurs types de portefeuilles de bitcoins : les portefeuilles logiciels, matériels, sur papier, et en ligne (ou Web). Vous pouvez envisager votre portefeuille de bitcoins comme celui dans lequel vous rangez vos billets de banque. La seule différence est que, dans un portefeuille de bitcoins, vous ne pouvez pas ranger des photos de vos enfants.

Tous les bitcoins sont stockés dans une immense base de données (sorte de registre public) appelée chaîne de blocs. Le bitcoin utilise un logiciel qui interagit avec la chaîne de blocs, vous permettant de voir votre solde à tout moment. Vous en saurez plus sur la chaîne de

blocs au [Chapitre 7](#), mais sachez qu'il est important d'apprécier le moment où vous devez consulter votre portefeuille, car la chaîne de blocs est vraiment le squelette du bitcoin sans qui cette crypto-monnaie s'effondrerait : chaque portefeuille de bitcoins lit la chaîne de blocs pour confirmer votre solde.

Un portefeuille de bitcoins peut également contenir plusieurs adresses et les regrouper pour vous.

## Les logiciels portefeuilles

Un logiciel portefeuille est une application bitcoin installée sur votre ordinateur. Il vous donne un contrôle total et assure la sécurité, car chacun de vos bitcoins n'est accessible que sur votre ordinateur. Ce logiciel, appelé Bitcoin Core, a été développé et soutenu par la Bitcoin Foundation.

Lorsque votre logiciel est installé, il crée le fichier wallet.dat qui contient les données relatives à votre portefeuille personnel.



Pour savoir où trouver un logiciel portefeuille, visitez <https://bitcoin.org/fr/>, et placez le pointeur de la souris sur Introduction. Dans le menu local qui s'affiche, cliquez sur Débuter.

Le logiciel portefeuille est open source. Cela signifie que son code source est accessible à tous ceux qui le

souhaitent. Il permet ainsi de s'assurer que le code ne contient aucun malware ou tout autre code suspicieux qui pourrait endommager votre ordinateur et compromettre votre sécurité. L'open source signifie aussi que vous êtes un petit prodige si vous parvenez à compiler des applications comme un portefeuille de bitcoins. Rassurez-vous, nous ne présumons pas que vous êtes capable d'une telle prouesse.

## Synchroniser votre portefeuille

Pour être certain que vous disposez toujours des dernières informations sur votre compte, vous devez synchroniser régulièrement votre portefeuille. Les ordinateurs et les tablettes exécutent cette synchronisation eux-mêmes. Par conséquent, veillez à paramétrer cette action.



Lorsque vous téléchargez et installez le logiciel client Bitcoin Core pour la première fois, l'opération risque de durer plusieurs jours, car le programme doit télécharger l'historique de chaque transaction effectuée depuis 2009 jusqu'à la toute dernière réalisée.



Chaque fois que vous fermez le portefeuille soit en éteignant votre ordinateur, soit en fermant l'application, n'oubliez pas de le synchroniser au prochain redémarrage.

## Sécuriser votre portefeuille

Le client Bitcoin Core permet de crypter un mot de passe – ce que nous vous conseillons de faire, car si quelqu'un réussit à entrer dans votre ordinateur, il cherchera à connaître le mot de passe d'accès à votre portefeuille. Avec un mot de passe bien crypté, vos bitcoins seront en sécurité.

Chaque fois que vous envoyez des bitcoins depuis votre portefeuille, vous devez fournir ce fameux mot de passe. Par conséquent, mémorisez-le bien !

## Sauvegarder votre portefeuille

Lorsque vous créez votre portefeuille de bitcoins, effectuez-en une sauvegarde avec le logiciel. Vous pouvez placer le fichier de sauvegarde sur une clé USB ou un disque dur externe. Ce fichier encrypté sera difficile à craquer, et surtout, il permettra d'accéder de nouveau à vos bitcoins s'il arrive malheur à votre ordinateur.

## Adresses multiples

Lorsque vous installez le portefeuille de bitcoins, vous pouvez créer plusieurs adresses pour que chacune d'elles soit réservée à une personne en particulier.

## Portefeuilles matériels

Certaines sociétés développent des versions de portefeuille qui autorisent le stockage de vos bitcoins sur un support bien physique. Lorsque vous avez ce périphérique avec vous, il suffira de vous connecter à Internet pour dépenser vos bitcoins (ou plus sérieusement pour assurer le transfert des bitcoins).

## Portefeuille sur papier

Posséder un portefeuille sur papier signifie que l'adresse qui gère vos bitcoins n'a pas encore été connectée à la chaîne de blocs. De facto, elle n'est pas « active ». Tant que le portefeuille n'est pas connecté à la chaîne de blocs, on le considère comme étant un stockage à froid (jargon du bitcoin pour parler d'un compte hors ligne).

Vous pouvez toujours vérifier le solde de n'importe quelle adresse de bitcoins en cherchant la chaîne de blocs. Toutefois, pour dépenser votre argent, vous devrez associer l'adresse sur papier au portefeuille en ligne.



Les portefeuilles sur papier sont réputés pour être la méthode de stockage des bitcoins la plus sûre lorsque vous n'avez pas l'intention de les dépenser.

Lorsque vous envoyez des bitcoins à une adresse, ils sont stockés dans la chaîne de blocs. Mais pour être utilisés, vous aurez besoin de connaître la clé privée. Comme nous l'avons dit, cette clé est une longue chaîne de caractères alphanumériques qui, quand elle est liée à un portefeuille de bitcoins, permet d'accéder à vos bitcoins par le biais du portefeuille correspondant. Donc, un portefeuille est une méthode sécurisée de stockage de vos bitcoins dont vous devez connaître la clé privée.



Lorsque vous créez un portefeuille sur papier, vérifiez que vous n'êtes pas connecté à Internet. Si vous l'êtes, un malware risque d'intercepter vos données, de décrypter votre clé privée, et d'accéder alors à vos bitcoins.



Consultez la prochaine section consacrée à la création pas à pas d'un portefeuille sur papier.

Voici un rapide tutoriel sur la création d'un portefeuille sur papier. Le service que nous avons utilisé pour cet exemple est [BitAdress.org](http://bitaddress.org), la plateforme où la mise en place de ce type de portefeuille est vraiment très simple :

1. Visitez <http://bitaddress.org> avec votre navigateur Web préféré.



2. Vous arriverez à la version française du site illustrée à la [Figure 5.1](#). De nouvelles adresses de bitcoins y sont continuellement générées avec les clés privées adéquates. Bougez le pointeur de la souris ou tapez un texte dans le champ de saisie afin d'augmenter l'aléa de vos adresses et de vos clés jusqu'à ce que le pourcentage affiché arrive à 100.
3. Ne sauvegardez pas la clé privée et les codes QR qui vous sont présentés. Au lieu de cela, cliquez sur Portemonnaie papier.
4. Sélectionnez le nombre d'adresses que vous souhaitez créer, et cliquez sur le bouton Générer.
5. Cochez la case Enlever l'image si vous ne souhaitez pas voir l'élément graphique, puis cliquez sur le bouton Générer. La création est ultra rapide.



**FIGURE 5.1** : Générer de nouvelles adresses de bitcoins.

- 6. Pour sauvegarder les portefeuilles sur papier (ou porte-monnaie papier) ou pour les imprimer, cliquez sur le bouton Imprimer.**
- 7. Vous pouvez alors les imprimer sur feuille ou les enregistrer sur votre ordinateur au format PDF. Cette dernière possibilité est déconseillée. Il est préférable de les imprimer sur papier.**
- 8. Avec votre smartphone ou votre tablette, flashez le code QR situé à gauche de chaque adresse, ou bien tapez la clé publique dans le logiciel client installé sur votre ordinateur. En faisant cela, vous pouvez commencer à transférer des bitcoins sur votre porte-monnaie papier. Vous pouvez scanner le code QR de la clé privée (situé à droite) qui permet de vérifier la propriété du compte afin d'en communiquer le solde.**

## **CARTES CRYPTO WALLET**

---

Prypto propose un produit appelé Crypto wallet qui consiste en deux cartes : L'une intéresse votre adresse bitcoin, et l'autre votre clé privée. Elles sont protégées par une bande à gratter. Tant que cette bande n'est pas grattée, exactement comme les cartes à gratter de la Française des jeux, personne ne sait de quoi il s'agit. Cela ajoute une étape supplémentaire de sécurité.

Pour plus d'informations, rendez-vous sur <http://cryptowalletcards.com/>.

## Les portefeuilles en ligne

Certaines sociétés offrent des services de portemonnaie. Elles agissent donc comme des intermédiaires dans le stockage de vos bitcoins, et permettent de les dépenser et d'en déposer à volonté. En contrepartie, elles assurent l'administration et la sécurité de votre compte. Mais cela signifie également que ces sociétés exigeront des informations très personnelles à votre sujet. Adieu l'anonymat si cher à beaucoup d'utilisateurs.



Si vous envisagez de recourir à un portefeuille tiers, vérifiez la réputation de la société avec laquelle vous souhaitez travailler. Dans le passé, de nombreuses sociétés gérant des bitcoins pour des particuliers ont mis la clé sous la porte, ont été piratées, ou bien encore ont fait faillite. Par exemple, en février 2014, la plus grande plateforme de change, Mt. Gox, cessa soudainement son activité. De nombreuses personnes y perdirent leurs bitcoins. Par conséquent, faites votre choix de manière avisée. Le pays dans lequel est enregistrée cette société aura ses propres exigences, exactement comme pour n'importe quel autre type

d'entreprise. Comme la réglementation autour du bitcoin est en plein développement, portez votre dévolu sur un pays disposant d'une grande expérience des services financiers, tel que les USA, le Royaume-Uni, la France, ou l'Île de Man. Mais malgré vos précautions, évitez de stocker dans ces sociétés plus que ce que vous pouvez vous permettre de perdre, pour éviter la faillite !

Voici quelques exemples de solutions de portefeuilles en ligne :



- » **Les plateformes de change de bitcoins :** Certaines personnes préfèrent confier tout ou partie de leurs bitcoins à des plateformes de change afin d'y accéder aisément dans le but d'échanger la crypto-monnaie contre des euros, des dollars, des livres sterling, ou pourquoi pas une autre monnaie électronique. Bien que cela paraisse séduisant, nous déconseillons cette pratique pour les raisons évoquées précédemment.
- » **Services de portefeuille dédiés :** Il existe des services de porte-monnaie en ligne sans aucune connexion avec des plateformes de change.
- » **Portefeuilles mobiles :** Comme avec la majorité des logiciels, certaines sociétés offrent des solutions Web pour périphériques mobiles.

## Paramétrer une adresse bitcoin

Une adresse bitcoin fonctionne comme une adresse e-mail en ce sens qu'elle permet d'envoyer et de recevoir des données – en l'occurrence des bitcoins. Cela étant dit, il existe une distinction majeure entre les adresses bitcoin et les adresses mail. En effet, il est possible d'avoir plusieurs adresses bitcoin que vous pouvez utiliser pour effectuer vos transactions. En réalité, il est judicieux d'utiliser une nouvelle adresse pour chaque nouvelle transaction. Certes, cela peut être compliqué à gérer par un quidam comme vous et moi quand le nombre de transactions quotidiennes est important. Contrairement à la croyance populaire, la génération d'une nouvelle adresse bitcoin n'exige pas une connexion Internet active.



Une adresse bitcoin est un identificateur qui représente la destination possible – ou la source – d'une transaction. Chaque adresse est composée de 26 à 35 caractères alphanumériques, et commence par un 1 ou un 3. Créer de nouvelles adresses peut s'effectuer sans surcoût via votre logiciel de bitcoins. Vous pouvez aussi obtenir une nouvelle adresse de votre plateforme de change ou d'un fournisseur de porte-monnaie en ligne.



Un des aspects les plus importants d'une adresse bitcoin est sa sensibilité à la casse. Ainsi, une adresse comme celle-ci contient à la fois des lettres majuscules

et minuscules :

1L5wSMgerhHg8GZGcsNmAx5EXMRXSKR3He

Changer une lettre majuscule pour une minuscule et inversement entraînera l'invalidité de l'adresse, et donc une absence de transfert de fonds.



La probabilité pour qu'une adresse invalide soit acceptée et de l'ordre de 1 sur 4,29 milliards de transactions.



Nous conseillons d'utiliser une adresse bitcoin par transaction. Gardez à l'esprit que vous pouvez tout à fait utiliser la même adresse encore et encore. Toutefois, l'utilisation d'une nouvelle adresse pour chaque transaction ajoute une couche de protection à votre vie privée.



Chaque adresse bitcoin est une « facture » de paiement. Une fois que ce paiement a été reçu à votre adresse, il n'y a aucune raison pour que l'expéditeur conserve cette donnée. Cependant, dans l'éventualité d'une perte de l'adresse du portefeuille ou de sa corruption, tout paiement futur à cette même adresse serait invalide et perdu à tout jamais. C'est la raison pour laquelle il est conseillé d'utiliser une adresse par transaction.

## La sécurité de votre portefeuille

Vous devez sécuriser votre portefeuille de bitcoins exactement comme vous rangez précieusement votre porte-monnaie dans votre sac ou votre poche, ou que vous gardez secret le code de votre carte bancaire. Cette section vous donne des conseils et des astuces pour sécuriser votre porte-monnaie virtuel.

## Sécuriser des portefeuilles mobiles

Un portefeuille (ou porte-monnaie si vous préférez ce terme) mobile est très pratique, car il s'installe aussi facilement sur une tablette que sur un smartphone. Ces deux types d'appareils sont constamment à portée de mains de leurs utilisateurs et ils ne nécessitent aucun équipement supplémentaire dès lors que vous disposez d'un accès à Internet. Cette connexion est de type Wi-Fi ou données mobiles permettant ainsi d'effectuer des transactions.

De ce fait, les portefeuilles mobiles sont beaucoup plus polyvalents que leurs homologues de bureau. En matière de sécurité, il n'y a pas de grande différence entre les deux. La clé privée – qui permet d'envoyer des bitcoins depuis votre porte-monnaie – est stockée directement sur le périphérique mobile. Cela réduit les risques de voir tomber votre clé dans des mains malintentionnées.

Cependant, les technologies des tablettes et des smartphones évoluent à un rythme infernal, poussant le consommateur à changer régulièrement son appareil actuel contre un modèle dernier cri. De ce fait, il semble impératif de sauvegarder votre clé privée dès que votre portefeuille de bitcoins mobile est installé sur votre appareil.

Cette sauvegarde dépend des fonctionnalités en la matière de votre périphérique. Parfois, un logiciel par défaut l'effectue automatiquement. Une copie de votre sauvegarde peut être exportée vers des clouds comme Dropbox ou Google Drive, voire par simple e-mail.

Pour cette sauvegarde, vous pourrez utiliser n'importe quelle application dédiée de votre appareil.



L'authentification est une mesure de sécurité essentielle dans la protection contre le vol ou l'utilisation frauduleuse de votre porte-monnaie. La majorité des portefeuilles mobiles utilisent un système de code PIN exigeant de l'utilisateur la saisie de 4 à 6 chiffres pour accéder à ses bitcoins.

Si vous n'entrez pas le bon code au bout d'un certain nombre d'essais, le portefeuille sera automatiquement bloqué. Son propriétaire en sera notifié par SMS ou par e-mail. Le message indiquera comment déverrouiller ce portefeuille mobile.



Au final, les portefeuilles mobiles représentent le meilleur compromis entre sécurité et pratique. Ensuite, tout dépend du comportement de son utilisateur. S'il est négligent ou s'il oublie de sauvegarder sa clé privée, il ne disposera d'aucune solution pour restaurer son porte-monnaie de bitcoins. Le bitcoin permet aux utilisateurs de prendre le contrôle de leur fonds, ce qui implique une grande responsabilisation de leur part, comme sauvegarder impérativement leur portefeuille mobile.

## Sécuriser ou non les portefeuilles en ligne

Vous pouvez facilement faire un parallèle entre les fournisseurs de portefeuille en ligne et les institutions financières telles que les banques. Ces deux services gèrent vos fonds personnels et permettent de vérifier le solde de votre compte à tout instant et d'effectuer tout type de transactions. Bien entendu, vous avez confiance dans les moyens de sécurité de votre banque pour assurer la pérennité de votre argent. En matière de bitcoins, cette confiance a priori est plus sensible. Nous pensons que la vision de Satoshi Nakamoto reposait sur l'idée que le bitcoin évoluerait dans une société où chaque interaction serait réalisée par les utilisateurs, sans passer par des tiers.



Un service de porte-monnaie de bitcoins en ligne est très pratique, mais aussi très risqué. En effet, un des avantages de ce système est de pouvoir accéder à tout moment à votre portefeuille via un navigateur Web. Cela suppose une confiance absolue dans le fournisseur de ce service.



Cependant, n'oubliez pas que ces services reposent sur des intermédiaires qui contrôlent vos fonds à votre place. Le plus gros risque est, même si vous connaissez l'adresse de votre portefeuille en ligne, de ne plus pouvoir accéder à votre clé privée. Dans l'hypothèse où le service de portefeuille en ligne s'arrêterait ou serait l'objet d'un piratage, vous n'aurez plus aucun contrôle sur vos fonds stockés dans ce portefeuille.

Vous êtes en plus responsable de la protection de votre compte. La majorité des plateformes de portefeuille en ligne fournissent une authentification à deux niveaux (voir le [Chapitre 2](#)). Cependant, force est de constater que ce système n'est pas totalement parfait. En effet, il ne protège pas contre le vol de vos fonds en cas de piratage du service.



Si vous êtes indépendant et souhaitez donc contrôler vos fonds, il n'y a aucune raison d'opter pour un service en ligne. Car aussi pratiques qu'ils soient, vos fonds restent exposés à des risques. Les portefeuilles en ligne sont loin de la philosophie de Satoshi Nakamoto,

le créateur de cette crypto-monnaie.

## Sécuriser les porte-monnaie papier

Un portefeuille sur papier est assimilable à un document contenant toutes les données nécessaires à la création des clés privées. Toutefois, son rôle ne se limite pas à cette tâche. En effet, ce type de porte-monnaie permet de stocker des bitcoins avec un assez haut niveau de sécurité. Dans ce cas, le papier inclut des clés publiques et des codes QR.

Les codes permettent d'utiliser les fonds associés aux bitcoins d'une adresse de portefeuille. Attention, car les portefeuilles sur papier ne peuvent être utilisés qu'une seule fois et pour la totalité de la somme qu'ils représentent. De facto, si vous n'utilisez pas toute cette valeur, la différence sera perdue.

Les portefeuilles sur papier peuvent servir à de nombreuses fins. Utilisez-les pour faire des cadeaux et ainsi mettre le pied de vos amis à l'étrier du bitcoin. Ou bien, vous pouvez donner un porte-monnaie papier à une personne pour la récompenser d'une action. Bien entendu, le destinataire de ce portefeuille doit installer un porte-monnaie de bitcoins sur son ordinateur ou

son périphérique mobile. Il pourra alors importer la clé privée associée à cette adresse.



Quelle que soit votre appréciation de ce système, les portefeuilles sur papier sont très sécurisés. En effet, ils ne sont pas connectés à Internet, ne peuvent pas être piratés, et ils ne dépendent pas d'un tiers. Toutefois, il s'agit de morceaux de papier qui peuvent être volés, perdus, ou encaissés par un tiers. Il est donc conseillé de stocker ces papiers dans un coffre ou un coffret de dépôt ce qui, avouons-le, n'est pas pratique pour certains utilisateurs.

# Chapitre 6

## Les transactions bitcoin

---

### DANS CE CHAPITRE

- » Comprendre les transactions
  - » L'importance des confirmations réseau
  - » Les frais appliqués au bitcoin
- 

Le concept des transactions bitcoin est simple à expliquer. Il s'agit d'un transfert de propriété électronique d'une certaine quantité de BTC effectué sur le réseau bitcoin. Par exemple, si vous possédez 5 bitcoins et que vous en envoyiez 2 à un utilisateur lambda, vous transférez la propriété électronique de ces 2 bitcoins vers le portefeuille de cette personne. Les 3 autres BTC restent dans votre porte-monnaie, puisque vous en demeurez le propriétaire.

Ce chapitre explique les bases des transactions et répond à un certain nombre de questions légitimes que vous pouvez vous poser sur l'échange des BTC.

# Les principes des transactions

Dans sa perception la plus directe, une transaction consiste à donner, à une personne désignée, des BTC qui vous appartiennent.



Pour qu'une transaction soit considérée comme « valide », il doit y avoir au moins une entrée, même si plusieurs entrées sont tout à fait légitimes. Une entrée fait référence à une sortie d'une précédente transaction. Notez que chaque entrée d'une transaction bitcoin doit être signée électroniquement. La signature s'effectue via la clé privée associée à l'adresse bitcoin qui initie le transfert de BTC.

Si plusieurs entrées sont associées à une transaction bitcoin, cela signifie que le montant qui sera envoyé provient de plusieurs adresses de porte-monnaie. Comme mentionné au [Chapitre 5](#), tout utilisateur de bitcoin peut générer un nombre infini d'adresses, chacune stockant une certaine quantité de BTC.

Voici un exemple : si vous envoyez 2 BTC à ce bon vieux « Robert », 1 BTC pourra provenir de l'adresse #2, 0,33 BTC de l'adresse #7, et le reste de l'adresse #8. Dans cet exemple, les adresses de portefeuilles #1, #3, #4, #5 et #6 n'ont pas de solde, ce qui les rend impropres à la transaction.

Toutefois, une transaction bitcoin peut se limiter à une seule entrée, mais avoir plusieurs sorties. Comme vous pouvez l'imaginer, des sorties multiples indiquent qu'une transaction bitcoin a été envoyée et répartie sur plusieurs adresses. Par exemple : votre solde de 5 BTC pourra être ainsi réparti : 2 BTC pour Robert, 1 BTC pour Marie, et les 2 BTC restants pour un autre portefeuille de bitcoins que vous contrôlez. Sur la chaîne de blocs, il y aura donc une transaction qui présentera trois entrées différentes, une pour Robert, une pour Marie, et la troisième pour votre autre adresse de porte-monnaie.



Envoyer un paiement en bitcoins peut être libellé en satoshi, c'est-à-dire la plus petite unité des transactions bitcoin (8 décimaux après la virgule). Du fait de cette divisibilité, la valeur de 1 satoshi peut varier grandement. Bien que 1 Satoshi ne vaille pas grand-chose aujourd'hui, rien ne dit qu'il n'atteindra pas la somme d'une poignée de centimes voire d'euros dans le futur, notamment si le bitcoin se développe auprès du plus grand nombre. (Attention, car tout ce que nous disons ici n'est que pure spéculation traitée au [Chapitre 4](#).)



En termes de transaction, les paiements en bitcoins ne sont pas très différents des paiements en espèces. La quantité de bitcoins associée à toutes les entrées peut

être supérieure à la quantité d'argent dépensée, ce qui crée de la « monnaie ». C'est ce qu'il se passe avec l'argent liquide. Si vous donnez un billet de 5 euros pour régler une dépense de 4,30 euros, on vous rendra 70 centimes de monnaie. Avec les bitcoins, la monnaie prend la forme d'une propriété électronique de BTC associée à l'adresse de votre portefeuille. Si le montant des entrées est supérieur à la valeur associée aux sorties, une sortie supplémentaire sera créée à l'adresse initiale afin de recevoir cette « monnaie ».

Il existe plusieurs méthodes de transactions entre utilisateurs de bitcoins. Tout d'abord, vous pouvez demander l'adresse du destinataire et envoyer l'argent via le logiciel bitcoin installé sur votre ordinateur ou votre appareil mobile. Pour les utilisateurs de mobiles, une alternative consiste à flasher le code QR généré par le destinataire. Chaque type de logiciel bitcoin permet aux utilisateurs de créer des codes QR qui peuvent comporter l'adresse du portefeuille où envoyer les fonds, ainsi que le montant total du paiement.

Un exemple : votre adresse de portefeuille bitcoin a reçu un total de 5 BTC sur une période donnée, alors que vous en avez envoyé 2 à Robert. La transaction aura une entrée et créera deux autres sorties lorsque vous enverrez l'argent à Robert. La première sortie intéresse alors la transaction effectuée pour Robert, c'est-à-



dire 2 BTC. La seconde sortie intéresse la transaction de la « monnaie » qui « renvoie », vers l'adresse de votre portefeuille, les 3 BTC inutilisés.

Pour plus d'informations sur les codes QR, rendez-vous [https://fr.wikipedia.org/wiki/Code\\_QR](https://fr.wikipedia.org/wiki/Code_QR).

## Recevoir des confirmations

Les confirmations bitcoin sont envoyées chaque fois qu'une transaction a été validée par les mineurs. (Pour plus d'informations sur le minage, reportez-vous au [Chapitre 4](#). Aucun canari ou lampe torche n'est requis.) Chaque bloc trouvé sur le réseau inclut une certaine quantité de transactions bitcoin qui y ont pris place antérieurement. Elles ont été diffusées sur tous les nœuds bitcoin dans le but d'en établir la validité.



Chaque bloc localisé sur le réseau bitcoin après qu'une transaction a été annoncée fournira une confirmation réseau. Comme indiqué, au moins six confirmations réseau sont nécessaires pour consacrer la validité de la transaction (voir la prochaine section).

### QUE FAIRE SI JE REÇOIS DES BITCOINS ALORS QUE MON ORDINATEUR EST ÉTEINT ?

Le bitcoin est souvent considéré comme l'argent d'Internet, car Internet est nécessaire à son utilisation, mais aussi parce que

vous devez disposer d'une connexion active pour utiliser correctement le logiciel. Mais sachez qu'il n'est pas nécessaire d'être connecté 24h/24 et 7j/7, même pour participer à une transaction.

Une fois votre adresse de portefeuille générée, elle reste active sur la chaîne de blocs pour... l'éternité – ou tout au moins tant que durera la chaîne de blocs. Si vous disposez d'un logiciel client synchronisé – sur ordinateur ou mobile – il n'interférera pas avec la manière dont vous recevrez des bitcoins sur votre adresse.

Bien entendu, la connexion sera nécessaire pour diffuser la transaction sur le réseau. Cette connexion pourra s'effectuer en Wi-Fi ou en données mobiles. Peu importe la rapidité de cette connexion puisque vous devez être en ligne simplement pour envoyer la transaction sur les nœuds bitcoin du réseau. La procédure entière ne prendra pas plus d'une seconde.

Imaginez que vous receviez une transaction sans être connecté au moment précis où elle est réalisée. Dans ce cas, les fonds seront tout de même transférés de l'expéditeur à votre adresse de portefeuille bitcoin puisqu'elle est « valide » sur la chaîne de blocs. En revanche, vous en aurez la notification qu'au moment où vous vous connecterez via votre logiciel. Après cela, la transaction sera visible sur votre portefeuille avec le nombre de confirmations réseau.

Chaque transaction bitcoin est suivie sur le réseau, et diffusée via divers nœuds dans le but de vérifier si elle est ou non valide. Que vous soyez ou non connecté, cette transaction est enregistrée

sur la chaîne de blocs. Les fonds seront visibles dans votre porte-monnaie dès que vous vous connecterez de nouveau.

Le principe de la réception hors ligne peut être comparé à celui des e-mails lorsque vous n'êtes pas devant votre ordinateur, ou que celui-ci est éteint. Tant que vous n'êtes pas connecté, impossible de savoir si vous avez ou non reçu des messages électroniques. En revanche, dès que vous lancez votre logiciel de messagerie client, tous les nouveaux courriels stockés sur le serveur sont importés dans votre ordinateur via ce programme. C'est exactement ce qu'il se passe avec le client bitcoin. Une synchronisation s'opère avec le serveur, ou la chaîne de blocs, et toute nouvelle information sera portée à votre connaissance en quelques minutes.



Une confirmation dans le monde du bitcoin signifie qu'une transaction a bel et bien été validée sur le réseau. Sans confirmation, une transaction reste « entre » utilisateurs. Tant qu'il n'y a aucune forme de vérification sur la chaîne de blocs, cette transaction présentera des risques de sécurité entre les parties. La confirmation des transactions peut prendre du temps. N'y voyez pas un désagrément, mais une mesure de sécurité.

La plupart des portefeuilles de bitcoins montreront une transaction comme étant « effectuée » sans se soucier du nombre de ses confirmations. Les utilisateurs de PC peuvent voir un état de type « n/unconfirmed », où n

indique le nombre de confirmations reçues. L'obtention de six confirmations peut prendre jusqu'à une heure.

Il n'y a aucun moyen pour un client bitcoin de « forcer » l'affichage des confirmations. Tout repose sur le réseau lui-même. Et avec ce fameux délai de dix minutes qui s'applique aux blocs bitcoin, il n'y a aucun moyen d'influer sur la vitesse de confirmation entre les blocs. Cela étant dit, il peut y avoir un facteur décisif sur la manière dont la transaction est captée par un bloc du réseau.

En supposant que la transaction bitcoin ait été diffusée sur le réseau juste avant que ne soit découvert un nouveau bloc, votre première confirmation peut s'effectuer assez rapidement. Mais si la transaction est captée par le prochain bloc – ce qui est possible dans la mesure où le processus est aléatoire – il faudra plus de temps pour que cette première confirmation soit accréditée.



Voici la règle générale sur les transactions : une transaction bitcoin qui ne présente aucune confirmation risque une double dépense. Cela signifie que l'utilisateur peut utiliser deux fois la même quantité de bitcoins depuis l'adresse de son portefeuille. Vous en saurez davantage à ce sujet au [Chapitre 10](#). En réalité, toute transaction qui a moins de six confirmations est exposée au même risque.

Cependant, les processeurs commerciaux et de paiement sont libres de mettre en place leur propre nombre de confirmations. Cette mesure ne s'applique pas aux possesseurs de bitcoins qui utilisent un logiciel installé sur leur ordinateur, et dont les fonds restent « non confirmés » tant que les fameuses six confirmations réseau ne sont pas atteintes. Les utilisateurs de mobile, en fonction de leur porte-monnaie, peuvent utiliser plus rapidement les fonds entrants.

## Les six confirmations

En comprenant bien que chaque confirmation d'une transaction survient quand un nouveau bloc est découvert sur le réseau bitcoin – environ toutes les dix minutes – il faut sensiblement une heure pour obtenir six confirmations. Une fois fait, l'argent peut être utilisé par le destinataire.

Ce délai peut apparaître à la fois comme une bénédiction et comme une calamité. L'avantage d'attendre six (ou plus) confirmations est la validité de l'opération, en étant assuré de ne pas être victime d'une double dépense. N'oubliez pas que les transactions bitcoin ne sont pas « remboursables » et que, sans ce principe des confirmations multiples, vous pouvez courir vers un désastre financier total.

Certains rapportent que six confirmations ont demandé plusieurs heures. Certes, cela peut arriver. Cependant, le délai d'obtention des confirmations se réduit de plus en plus. Il dépend aussi du taux de hachage utilisé sur le réseau pour résoudre les blocs.

Même lorsque la transaction est « confirmée » par le logiciel bitcoin suite aux six confirmations réseau, le protocole bitcoin ne considère pas encore la transaction comme « valide ». Au moment de la création du bitcoin, un morceau de code fut écrit dans le protocole de cette monnaie pour que la génération de nouvelles « pièces » (minage de bloc) ne soit validée qu'après 100 confirmations. En réalité, la plupart des coopératives minières (comme mentionné au [Chapitre 4](#)) ne valident qu'après 120 confirmations réseau.

## Double dépense

Bien que le réseau bitcoin soit sécurisé, il existe toujours un risque de double dépense. Il s'agit d'un acte par lequel l'utilisateur dépense deux fois le même bitcoin. Pour éviter cela, le réseau bitcoin vérifie chaque transaction individuellement via une procédure de confirmations.



En général, le plus gros risque de survenance d'une attaque de type double dépense est encouru quand des commerçants ou des traders agissent dès qu'une transaction est visible sur le réseau. Ces transactions non confirmées – également connues sous le nom de transactions à zéro confirmation – représentent un risque majeur en termes de double dépense. Il en résulte que tous les utilisateurs de bitcoins savent qu'ils doivent attendre au moins six confirmations avant de pouvoir déplacer de nouveau des fonds. Plus une transaction spécifique présente de confirmations, et plus il y a des chances qu'elle soit légitime, et qu'il ne s'agisse pas d'une double dépense.



Les risques d'être victime d'une double dépense sont minces. Mais aucun système n'étant parfait, ils n'en restent pas moins bien réels. Cela étant précisé, il existe cinq formes d'attaques potentielles associées à la double dépense, et que nous détaillons dans les prochaines sections.

## Race attaque

Les traders et les commerçants acceptent un paiement immédiatement sans confirmation s'exposant ainsi à la double dépense si une personne malintentionnée parvient à dépenser les mêmes bitcoins auprès de deux utilisateurs différents.

## Attaque de Finney

L'attaque de Finney implique la participation d'un mineur une fois qu'un bloc a été miné. Il est impossible d'éliminer les risques d'une attaque de Finney, malgré les précautions du commerçant. Cette attaque n'est possible que si un mineur y participe et si une séquence spécifique d'événements survient. Donc, cette attaque n'est ni triviale, ni gratuite et n'intéressera un fraudeur que si le gain qui en résulte est significatif.

## Attaque Vector76

On l'appelle l'attaque à une confirmation, car elle combine une Race attaque et une attaque de Finney permettant ainsi à une transaction ayant obtenue une confirmation de faire l'objet d'une double dépense. La même action de protection contre la Race attaque (pas de connexion entrante, une connexion sortante explicite sur un nœud bien connecté) réduit significativement le risque d'une telle attaque.

## Attaque force brutale

L'attaquant soumet une transaction au commerçant/réseau afin de payer un produit ou un service tout en minant privativement une chaîne de blocs dans laquelle est incluse la transaction de double



dépense. Après avoir attendu les  $n$  confirmations, le commerçant envoie le produit. Si l'attaquant parvient à trouver plus que  $n$  blocs à cet instant précis, il réalise son embranchement (fork) et récupère son argent ; sinon, il peut tenter d'étendre son fork en espérant pouvoir le récupérer via le réseau.

## Attaque des 51 %

Si l'attaquant contrôle plus de la moitié du taux de hachage du réseau, les chances de succès de ses attaques sont de 100 %. En effet, cette personne malveillante génère des blocs plus vite que le reste du réseau. La chaîne de l'attaquant peut alors remplacer celle constituée par le réseau légal. Pour plus de détails à ce sujet, consultez la page <https://dossiers.cryptofr.com/quest-ce-quune-attaque-des-51/>.

## Zéro confirmation

Une tendance a vu le jour dans le monde du bitcoin par laquelle des commerçants n'attendent pas les six confirmations pour considérer que le paiement est valide. Ce comportement augmente les risques d'être victime d'une double dépense.

Néanmoins, le commerçant et les processeurs de paiement peuvent déterminer le nombre de confirmations nécessaires à la validité d'une transaction bitcoin. Alors que la plupart des services fixent ce nombre entre 3 et 6, d'autres valident l'opération dès qu'elle est diffusée sur le réseau dans un état « non confirmé ». Évidemment, l'achat effectué en ligne est réalisé plus vite, accélérant ainsi la procédure de commande.



Les commerçants qui valident une transaction à un état de confirmation zéro vendent généralement des produits numériques ou bon marché. Par exemple, la grande majorité des bars et des restaurants considèrent que la transaction est valide à zéro confirmation, car ils sont protégés par le processeur de paiement en cas de double dépense. Des processeurs comme BitPay, BitKassa, et Coinbase fournissent aux commerçants une protection contre ce type d'attaque, même quand le nombre de confirmations de la transaction est fixé sur 0.

Les transactions bitcoin à zéro confirmation sont idéales pour les entreprises et les particuliers dans le but d'accepter rapidement, et en toute sécurité, des paiements avec cette crypto-monnaie, en dépit des risques associés à cette pratique. Avec ce genre de dispositif, il n'y a aucune raison de se passer d'une

absence de confirmation réseau pour valider un paiement.

## Calculer les frais

---

Le bitcoin est souvent présenté comme un réseau de paiement n'incluant aucun frais sur les transactions. C'est vrai jusqu'à un certain point. Certes, aucun frais n'est appliqué au destinataire d'une transaction bitcoin provenant d'un autre utilisateur du réseau. Mais parfois des frais, même minimes, sont réclamés.

Des frais sur les transactions réalisées en bitcoins sont inclus dans chacune de ces opérations. En réalité, la plupart des portefeuilles de bitcoins permettent à l'utilisateur d'inclure des frais dans le but d'accélérer la procédure. En effet, lorsque de tels frais sont appliqués, la transaction est prioritaire sur les autres.



Il existe des exceptions à ce principe d'accélération. Dans le client Bitcoin Core, si votre transaction est inférieure à 1 000 octets, ne présente que des sorties de 0,001 BTC minimum, et dispose d'un haut niveau de priorité, des frais ne sont pas exigés. Toutes ces conditions doivent être réunies pour que cette exception puisse s'appliquer. Dans le cas contraire, des frais de 0,0001 BTC par milliers d'octets seront ajoutés. Les utilisateurs du client Bitcoin Core noteront qu'à

chaque fois que des frais sont inclus, le client sera amené à demander à l'utilisateur d'accepter ou de rejeter les frais associés à la transaction. Le fait de les rejeter ralentira la transaction par abaissement de son niveau de priorité.



La taille moyenne des transactions se situe entre 500 et 600 octets. Les frais inhérents à ces transactions sont de l'ordre de 0,0001 BTC. L'ajout d'une transaction dans un bloc du réseau est totalement aléatoire, mais reste affecté par les frais (s'ils sont exigés). Chaque bloc libère un espace de 50 000 octets pour les transactions à un haut niveau de priorité – indépendamment des frais (TX) – à ajouter (approximativement 100 transactions par bloc). Après cela, les transactions soumises à des frais de 0,00001 BTC/kilooctet sont ajoutés au bloc, en incluant d'abord les frais de transaction par kilooctet les plus élevés. Cette procédure se répète jusqu'à ce que la taille du bloc atteigne 750 000 octets.

## Examiner la vitesse des transactions

---

La priorité d'une transaction est définie par une formule mathématique relativement complexe. Le calcul est le suivant : nombre de bitcoins à dépenser

multiplié par l'âge de la transaction et divisé par la taille des données d'entrées regroupées pour être dépensées.

Comme vous pouvez l'imaginer, il y a souvent plus de transactions qui attendent d'être diffusées que de blocs disponibles. Ces transactions en attente restent dans un memory pool du mineur (un groupe de transactions qui n'ont pas encore été vérifiées par le réseau bitcoin), et qui seront incluses dans de futurs blocs et dont la priorité sera définie par les frais appliqués (s'il y en a).



Le relais des transactions peut être sujet à des taxes. Le relais ignore toutes les sorties d'au moins 0,01 BTC, et vérifie si la transaction est dite avec ou sans frais. S'il y a des frais, 0,00001 BTC est ajouté au total de la transaction. Sinon, la transaction est considérée comme « gratuite » et placée au plus bas niveau dans la liste des priorités.

Pour plus d'informations sur le relais des transactions, consultez

[https://en.bitcoin.it/wiki/Transaction\\_fees#Rel](https://en.bitcoin.it/wiki/Transaction_fees#Rel)

Pour davantage de détails, consultez  
[https://en.bitcoin.it/wiki/Transaction\\_fees#Tec](https://en.bitcoin.it/wiki/Transaction_fees#Tec)  
et

[https://fr.wikipedia.org/wiki/Bitcoin#Les trans](https://fr.wikipedia.org/wiki/Bitcoin#Les_trans)

# Comprendre les frais de minage

Les transactions bitcoin sont intégrées dans des blocs par les mineurs (voir le [Chapitre 4](#)). Par conséquent, inclure des frais dans chaque transaction encourage les mineurs à inclure vos transactions dans le bloc suivant.



Chaque frais de transaction peut être vu comme une petite récompense pour tous les mineurs qui ont résolu le bloc contenant votre ou vos transactions.



La procédure de minage s'arrêtera quand tous les bitcoins auront été minés, ce qui devrait survenir en 2140. Pour cela, on suppose que les mineurs continueront à résoudre des blocs incluant des transactions en échange des frais présents dans chaque transaction individuelle. Il existe tout un débat autour des frais et de leur pouvoir incitatif à résoudre des blocs. Il faudra bien des années avant qu'un consensus soit trouvé. En conséquence, ne vous préoccupez pas trop de cette question aujourd'hui.



Sans frais de minage, pourquoi les mineurs mineraient-ils pour valider vos transactions ? De plus, personne n'est obligé d'inclure des frais, sauf s'il en a été convenu autrement par votre porte-monnaie de bitcoins. Toutefois, il est bon d'inclure des frais, aussi minimes soient-ils, dans le but d'aider le réseau bitcoin et les mineurs individuels.

# Gérer les transactions multisignatures

---

Nous savons que l'idée du bitcoin est de donner le contrôle sur ses fonds à l'utilisateur final, et cela à tout moment. Alors que laisser le contrôle d'un portefeuille à un utilisateur pour un usage individuel ne pose pas de problème, les choses sont sensiblement différentes pour des entreprises, des familles, ou même des amis partageant un projet. La confiance peut très vite s'effriter.

Un portefeuille de bitcoins standard fonctionne de la manière suivante : un utilisateur dispose d'une clé privée et possède un contrôle total sur l'adresse de ce porte-monnaie. Si plusieurs personnes participent à un même projet, une seule option est alors possible : faire confiance aux utilisateurs qui connaissent la clé privée d'une adresse de portefeuille commune. Mais, s'il vient à l'idée à cette personne de retirer tous les fonds, les autres membres ne pourront rien faire contre, puisqu'elles ne disposent d'aucun contrôle.

Cela va sans dire qu'une meilleure solution consiste à donner le contrôle à plusieurs utilisateurs sur le même portefeuille. Ainsi, un système à plusieurs signatures a été développé sous le nom de compte multisignature ou multisig.



Contrairement à un porte-monnaie de bitcoins standard, des adresses multisignatures exigent de fournir plusieurs clés privées avant que les fonds ne soient utilisables. Ce système fonctionne quasiment comme celui d'un portefeuille normal. Ainsi, pour recevoir des fonds, aucune clé privée n'est exigée. En revanche, chaque envoi de fonds est numériquement signé par le logiciel bitcoin sur votre périphérique, et cela en utilisant une clé privée liée à votre adresse de portefeuille.

Les adresses multisignatures exigent « m – de – n » clés privées pour rendre disponibles les fonds associés à une adresse de bitcoins particulière. Par exemple, une adresse à trois signatures exigera au moins 2 des 3 clés privées pour valider un envoi. Ici,  $m = 3$  (nombre total de clés) et  $n = 2$  (nombre de clés requises).



L'impossibilité de fournir deux des trois clés bloque la transaction. Les adresses bitcoin multisignatures ajoutent une couche de sécurité pour les entreprises et les groupes de personnes qui partagent une adresse de portefeuille. Cette idée est sans doute la meilleure pour tous ceux qui prennent la sécurité du bitcoin au sérieux, et cela même pour un usage personnel.



Armory, l'un des logiciels client disponibles, fut le premier fournisseur de portefeuilles à intégrer des adresses multisignatures. Il y a plus d'un an, Armory



dévoila sa nouvelle fonction LockBoxes, qui montre comment générer une adresse bitcoin à plusieurs signatures. Regardez une vidéo détaillée sur le sujet à <https://www.bitcoinarmory.com/tutorials/armory-advanced-features/lockbox/create-lockbox/>.

## EXEMPLE DE MULTISIGNATURE

---

Dans un groupe de trois personnes – Jean, Robert, et Josiane – trois combinaisons de 2 clés sur les 3 clés détenues sont possibles :

- » Jean et Robert signent la transaction avec leurs clés privées respectives
- » Jean et Solange signent la transaction avec leurs clés privées respectives.
- » Robert et Solange signent la transaction avec leurs clés privées respectives.

Si cette procédure n'est pas scrupuleusement suivie, les transactions ne peuvent pas être traitées.

# Chapitre 7

## La chaîne de blocs

---

### DANS CE CHAPITRE

- » Décomposer les blocs et la chaîne de blocs
  - » Découvrir le potentiel de la chaîne de blocs
  - » Projeter cette technologie dans l'avenir
- 

La chaîne de blocs bitcoin est une prouesse technologique dont ce chapitre présente différents aspects. Vous apprendrez ici tout ce que vous avez toujours voulu savoir sur la chaîne de blocs, sans jamais oser le demander.

Commençons tout d'abord avec les bases : Qu'est-ce que la chaîne de blocs ? Pour faire simple, disons que la chaîne de blocs est une sorte de registre ou livre d'opérations public offrant une transparence sans précédent sur l'écosystème du bitcoin. Elle liste toutes les transactions effectuées en bitcoins depuis son lancement en 2009. Ainsi, chaque transaction est répertoriée sur la chaîne de blocs. Mais cette technologie est capable de beaucoup plus.



La chaîne de blocs est une avancée technologique majeure. Sa nature décentralisée signifie qu'il n'existe aucun point d'échec central susceptible de la mettre à mal.

Vous pouvez regarder une vidéo très sympathique expliquant ce qu'est la chaîne de blocs à l'adresse <https://webtv.univ-rouen.fr/permalink/v12562048104cgem0jpbq/iframe/>

## Enregistrer des transactions

Une des questions les plus souvent posées est la suivante : Pourquoi appelle-t-on cela une chaîne de blocs ? Pour bien le comprendre, vous devez d'abord saisir la notion de bloc. Si nous envisageons la chaîne de blocs comme un livre d'opérations, le bloc d'origine en serait la première page. Chaque nouveau bloc apparaissant par la suite sur le réseau bitcoin contient une somme de contrôle (ou hash) provenant du bloc précédent. Ainsi, depuis l'apparition du premier bloc en 2009 – appelé Bloc genesis – il existe une chaîne d'opérations, toutes incluses dans différents blocs. Donc, à travers ces blocs, il est possible de suivre la traçabilité des transactions. Si nous reprenons l'analogie avec le livre d'opération (ou registre) chaque nouvelle page contient un résumé de la ou des pages précédentes. Il se passe exactement la même chose avec

la chaîne de blocs au fur et à mesure que des données supplémentaires y sont stockées.

La chaîne de blocs bitcoin est plus largement connue comme étant un livre ouvert contenant les enregistrements passés, présents, et futurs des transactions en bitcoins. La chaîne de blocs apparaît comme un outil comptable, mais aussi comme un écosystème financier totalement transparent. C'est ce niveau de transparence qui effraie les institutions financières traditionnelles. Elles n'aiment pas divulguer leurs chiffres et leurs statistiques, alors que la chaîne de blocs est totalement transparente à ce sujet. Cependant, il existe un niveau de pseudonymité attaché à la chaîne de blocs bitcoin. Ainsi, les utilisateurs individuels ou les sociétés sont représentés par une adresse de portefeuille bitcoin, plutôt que par un nom ou une adresse postale.



D'un point de vue financier, envisagez la chaîne de blocs comme une base de données partagée des transactions. Chaque nœud bitcoin (un ordinateur qui exécute constamment un logiciel portefeuille pour détecter et valider de nouvelles opérations) du réseau détient une copie de l'historique des transactions depuis le début (2009) jusqu'au jour de l'opération en cours. Dans le futur, de plus en plus de transactions s'ajouteront à la chaîne de blocs existante, créant ainsi

une sorte de ligne de temps sur l'évolution du bitcoin.

Chaque nouveau bloc est généré chronologiquement puisqu'il contient le hash du bloc qui le précède. Sans cet ordre chronologique, cette somme de contrôle resterait inconnue, et le bloc serait rejeté du réseau. Mieux encore, les anciens blocs du réseau ne peuvent pas être modifiés, car cela imposerait de les générer de nouveau.

Cette technique consistant à mémoriser toutes les transactions précédentes entraîne une croissance constante de la taille de la chaîne de blocs. Au moment où vous lirez ce livre, la taille de la chaîne de blocs sera d'environ 50 Go.

## Comprendre l'analyse de la chaîne de blocs

---

En 2014, une nouvelle tendance a commencé à émerger dans l'univers du bitcoin et de la technologie de la chaîne de blocs. Il s'agit d'un nouveau marché au sein même de l'écosystème du bitcoin. Il a été rendu possible grâce à la transparence de la chaîne de blocs. Mais, cet outil divise les opinions.

Une des choses qui font prospérer le bitcoin comme moyen de paiement est le retour que nous avons sur la manière dont les gens dépensent leurs bitcoins, non

seulement du point de vue des produits et/ou services achetés, mais par rapport au temps pendant lequel cette crypto-monnaie reste dans les portefeuilles avant d'être dépensée. Comme les espèces, le bitcoin est un moyen de paiement que vous pouvez utiliser n'importe où et n'importe quand. Disposer d'une analyse détaillée sur la durée de stockage des bitcoins pourrait inciter à adopter cette crypto-monnaie. C'est ce que cherche à faire, entre autres, l'analyse de la chaîne de blocs.

Les aspects positifs de l'analyse de la chaîne de blocs sont assez faciles à dégager. Le bitcoin est un système financier encore jeune, donc immature. De ce fait, une analyse permet de dégager des études pouvant jouer en faveur de l'adoption des bitcoins :

- » Combien de bitcoins sont dépensés ?
- » D'où proviennent les portefeuilles les plus récents ?
- » Est-ce que le problème de thésaurisation est résolu, ou au contraire va-t-il continuer à se développer ?

Toutes ces questions méritent une réponse ciblée que l'analyse de la chaîne de blocs se propose de donner.

Ce n'est pas un secret de révéler que les bitcoins les « plus anciens » enregistrés sur le réseau n'ont pas été échangés pendant des années. Certains disent même qu'ils appartiennent à Satoshi Nakamoto, le créateur de cette monnaie électronique. D'autres

arguent qu'il s'agit des premiers utilisateurs du bitcoin qui, une fois leur achat effectué, ont oublié qu'ils possédaient des bitcoins et ne sont jamais revenus les utiliser sur le réseau. Enfin, une hypothèse explique que des clés privées ont été perdues à la suite d'une panne d'un disque dur, bloquant ainsi l'utilisation des bitcoins associés au portefeuille concerné.

Rendre le bitcoin plus convivial est un autre obstacle que l'analyse de la chaîne de blocs peut aider à surmonter. Par exemple, la plupart des utilisateurs trouveraient sympa de recevoir un SMS chaque fois qu'ils envoient ou reçoivent des bitcoins. Certains fournisseurs de porte-monnaie proposent cette fonctionnalité. Recevoir un SMS permet à l'utilisateur débutant de surveiller ses dépenses et le solde de son compte.

## **Au-delà des transactions**

---

La chaîne de blocs peut être appliquée à tous les domaines : le suivi de colis en temps réel dans le monde entier, la lutte contre le piratage en ligne, et la lutte contre la contrefaçon. Ce ne sont que quelques applications possibles de la chaîne de blocs. Vous comprenez que le concept de chaîne de blocs peut s'étendre bien au-delà de son pur aspect financier en matière de bitcoins.

Au-delà de l'aspect financier, la chaîne de blocs nous permet bien plus que de consigner des transactions dans un registre d'opérations. Un certain nombre de projets sont en cours de développement pour la rédaction de contrats, le transfert électronique de propriété, et même des droits d'auteur. En voici deux d'entre eux :

- » **Factom** : Une couche supérieure de la chaîne de blocs du bitcoin centrée sur la tenue de livres et l'enregistrement des données (par exemple des dossiers médicaux).
- » **Storj** : Encourager les utilisateurs avec des jetons Storj à stocker une partie de la chaîne de blocs sur leur ordinateur. Ces jetons pouvant être ensuite utilisés par les utilisateurs pour stocker certaines de leurs données personnelles sur cette même chaîne.



Du fait de sa transparence, les possibilités de la technologie de la chaîne de blocs sont infinies, et les développeurs ne font qu'apprécier la partie visible de cet iceberg.

## Travailler avec des applications de la chaîne de blocs

---

En termes de développement, la majorité des applications de la chaîne de blocs se focalisent sur des



services financiers. Cela est tout à fait normal puisque le bitcoin est avant tout une monnaie utilisée partout dans le monde, même dans des pays où le système bancaire n'est pas bien développé. De plus, la chaîne de blocs est bien connue pour être une sorte de livre d'opérations ouvert.

Le potentiel du développement d'applications de la chaîne de blocs est si immense qu'il est bien difficile aujourd'hui de dire ce qu'il nous attend dans ce domaine. Retenez simplement que ces applications couvriront des domaines financiers ou non. Leur but sera toujours d'améliorer notre vie quotidienne. Toutefois, jusqu'à ce que ces applications soient correctement codées, nous ne pouvons faire que des suppositions.

L'idée qui se cache derrière les applications de la chaîne de blocs est identique à celle du bitcoin : redonner le pouvoir aux utilisateurs sans passer par des services centralisés ou des sociétés. Comme la chaîne de blocs est décentralisée et transparente par nature, ses applications présenteront des avantages technologiques sans précédent. Pour en savoir plus sur la centralisation et la décentralisation, consultez le prochain encadré.

La puissance technologique de la chaîne de blocs vient d'une courbe d'apprentissage rapide. En effet, ce type de développement n'est pas une mince affaire. Il faut

du temps, même aux programmeurs, pour se familiariser avec les paramètres et l'appel de l'API associés à la chaîne de blocs du bitcoin.

L'objectif principal du développement d'applications de la chaîne de blocs est d'améliorer notre vie quotidienne en donnant de la transparence et de la responsabilité à l'infrastructure existante, et plus spécialement dans le domaine financier qui en a grandement besoin. Mais il y a de nombreux autres secteurs qui peuvent adopter la technologie de la chaîne de blocs. Les années qui viennent nous donneront bien des indications sur ce que l'avenir nous réserve en la matière.



Développer une chaîne de blocs nécessite l'écriture d'une grande quantité de code et l'appréciation d'éventuelles conséquences. En premier lieu, il faut dégager des fonds pour que les développeurs acceptent d'écrire une application à partir de rien.

La chaîne de blocs cherche à créer des communautés et à donner, à des utilisateurs individuels, des choix qu'on ne leur propose pas habituellement. C'est un peu comme partager une idée sur la manière d'améliorer quelque chose dont chacun pourra profiter. Un exemple concret est celui des crypto-monnaies alternatives, plus connues sous le nom d'altcoins. Il en résulte que le développement de la chaîne de blocs n'est pas lié à un seul langage de programmation. La diversification est

l'une des plus grandes souplesses que cette technologie peut apporter aux développeurs. Il reste à voir si cet esprit communautaire va s'étendre au développement d'applications. Nous pouvons tout de même effectuer une comparaison entre l'état actuel du développement de la chaîne de blocs et les premiers jours de l'Internet.

N'importe quel type d'application de la chaîne de blocs peut être développée en utilisant une grande variété de langages de programmation, y compris JavaScript, Ruby, Perl, et PHP. Il faut aussi prendre en compte le système d'exploitation puisque ces applications doivent être compatibles avec Android, iOS, Windows Phone, et BlackBerry.

## CENTRALISÉ VS DÉCENTRALISÉ

---

Il existe une différence majeure entre les systèmes centralisés et les systèmes décentralisés. Les systèmes centralisés suivent un chemin très balisé en matière d'opérations quotidiennes et de considération des clients. Les systèmes décentralisés se focalisent sur la communauté et demandent donc à ce que chacun participe à l'effort collectif :

- » Des sociétés ou des services centralisés ne permettent qu'à un nombre limité de personnes de fournir des services ou des produits au client.
- » Des sociétés ou des services décentralisés donnent potentiellement à chacun la possibilité de fournir ces

mêmes services ou produits à qui que ce soit dans le monde, à n'importe quel moment, et n'importe où. Par le peuple, pour le peuple, et avec le peuple est le leitmotiv des systèmes décentralisés.

## En route pour le Bitcoin 2.0

---

Le bitcoin est perçu comme une monnaie servant plusieurs buts. Pourtant, de nombreuses personnes cantonnent le bitcoin à un moyen de paiement.

Bitcoin 2.0 représente la prochaine génération des applications et des plateformes bitcoin, dont la majorité d'entre elles ne se focaliseront pas sur le secteur financier. Les plateformes et les applications Bitcoin 2.0 utiliseront la technologie de la chaîne de blocs pour impacter d'autres domaines de notre vie quotidienne.



Le bitcoin et la technologie de la chaîne de blocs peuvent faire beaucoup plus qu'être asservis à des objectifs financiers. Toutefois, n'oublions pas que ces deux éléments vont permettre d'évoluer davantage vers cet écosystème financier, tout en améliorant son fonctionnement.

La technologie du bitcoin et de la chaîne de blocs peuvent s'appliquer à de nombreux domaines. Ainsi, il est possible d'utiliser des chaînes de blocs pour

identifier des personnes afin de remplacer des méthodes peu sécurisées utilisées par des services comme Facebook ou encore Twitter.

Le potentiel du Bitcoin 2.0 et de la technologie de la chaîne de blocs ne pourra pas passer inaperçu. Diverses institutions financières essaient de voir comment implémenter la chaîne de blocs dans leur infrastructure existante. Même si ces institutions financières ne croient pas en l'avenir de la crypto-monnaie, elles pensent en revanche que la chaîne de blocs contient en elle bien des solutions futures.

Qu'est-ce qui rend l'écosystème Bitcoin 2.0 aussi attractif ? Eh bien, les blocs de données diffusés et découverts sur le réseau. En effet, ces blocs peuvent transférer n'importe quel type de données entre des utilisateurs, et cela d'une manière totalement transparente. La consignation d'engagements, des ressources de médias numériques, et même des assurances électroniques est une idée sur laquelle les développeurs pourraient se pencher.

Bitcoin 2.0 sera capable d'améliorer le modèle d'échange traditionnel du bitcoin. Aujourd'hui, les plateformes de change de bitcoins permettent aux utilisateurs de stocker, d'utiliser, et de recevoir de la monnaie électronique sans autre bénéfice. Bitcoin 2.0 pourra proposer des fonctions comme le prêt peer-

to-peer, des comptes portant intérêts, et même la possibilité de réaliser des transactions financières sans recourir à un courtier ou à une banque.

En poussant la réflexion encore plus loin, les applications Bitcoin 2.0 et les plateformes pourront se passer d'un intermédiaire pour acheter et vendre des marchandises. La propriété des marchandises sera, en théorie, liée à des jetons numériques qui pourront être transférés à un autre utilisateur de la chaîne de blocs, avec paiement simultané de ce transfert. Cela représente un très gros potentiel pour une grande partie de l'e-commerce qui trouvera un intérêt certain dans la chaîne de blocs.

Et pourquoi ne pas utiliser la technologie du Bitcoin 2.0 pour mettre en œuvre une carte d'identité virtuelle permettant de terminer les processus de vérification aussi bien dans l'univers du bitcoin qu'ailleurs ? Plutôt que de soumettre des documents sensibles à des tiers qui vont les stocker sur des serveurs centralisés, une carte d'identité virtuelle pourra être vérifiée directement par la chaîne de blocs elle-même. Le propriétaire de la carte d'identité virtuelle gardera le contrôle total de ses données, le vendeur ne recevant aucune copie enregistrable de ces informations.

Utiliser la technologie Bitcoin 2.0 pour créer une nouvelle race de marchés décentralisés n'est qu'une innovation parmi d'autres. Il serait tout à fait possible d'échanger des métaux précieux contre des espèces ou de la monnaie électronique via la chaîne de blocs. Mais d'autres aspects de la vie, comme des médias numériques, peuvent aussi bénéficier de ces marchés décentralisés. Comme il n'y a aucun intermédiaire, les coûts pour les artistes s'en trouveront considérablement réduits.

Enfin, la technologie de la chaîne de blocs s'appuie sur une communauté pour soutenir cette nouvelle vague d'innovation. Il est également tout à fait possible d'envisager une autorité locale voulant montrer ses prévisions budgétaires à ses contribuables. Ici, une application Bitcoin 2.0 pourra présenter ces prévisions, le budget, les options potentielles, et les solutions. Chacun pourra alors voter via cette technologie, dans un système ouvert et démocratique. L'ensemble de la procédure étant totalement transparent. De facto, le vote résultant serait alors lui aussi entièrement transparent, sans qu'aucune information personnelle sur les votants ne soit divulguée.



Créer de nouvelles applications et services décentralisés sera l'objectif principal de la technologie Bitcoin 2.0. Cette vague d'innovation incitera chaque individu à

devenir son propre patron et à créer son propre secteur d'activité. Ainsi, nous avons vu que peu de personnes ont la patience d'attendre un taxi ! Quel rapport me direz-vous ? le rapport c'est Uber, un exemple typique de service décentralisé. Croyez-nous, les applications potentielles du Bitcoin 2.0 seront immenses et risquent de changer à tout jamais notre appréciation de la communauté des utilisateurs.



# Bitcoins et activités commerciales

## QUATRE INCONVÉNIENTS DU *CLOUD MINING*

- » Manque de contrôle : Vous empruntez du matériel informatique et un serveur appartenant à quelqu'un d'autre, vous retirant ainsi tout contrôle sur ces machines.
- » Asservissement à l'honnêteté d'un tiers : Pourquoi payer plus que vous ne le devriez ?
- » Prise en charge des frais de maintenance et d'électricité : La société de cloud mining vous facture une partie de ses frais d'entretien et de fonctionnement.
- » Sociétés illégales ou fragiles : Certaines sociétés de cloud mining peuvent sembler légales alors qu'elles ne le sont pas. Elles sont vulnérables aux attaques.

**DANS CETTE PARTIE...**

- » Tout savoir sur les activités commerciales avec le bitcoin, les processeurs de paiement, et l'acceptation des bitcoins dans votre boutique.
- » Tout connaître sur les taxes, la réglementation, et les licences.
- » Sécuriser vos investissements et comprendre les dangers de la double dépense et des différents types d'attaque.
- » Tout sur le minage de bitcoins et son fonctionnement, et sur son utilité à votre niveau.

# Chapitre 8

## Utilisation commerciale du bitcoin

---

### DANS CE CHAPITRE

- » Vendre avec le bitcoin
  - » Examiner les processeurs de paiement en bitcoins
  - » Accepter le bitcoin dans votre boutique
- 

La lecture des précédents chapitres vous a permis de comprendre ce qu'est le bitcoin et comment en acquérir. Maintenant, vous vous posez probablement la question de savoir comment les choses se déroulent dans la vie quotidienne.

Ce chapitre traite des meilleurs moyens d'utiliser votre crypto-monnaie en tant qu'outil commercial afin de le substituer à la monnaie traditionnelle, et d'accepter les paiements en ligne.

## Vendre des marchandises contre des bitcoins

---

Si vous vendez des marchandises, vous devez convaincre vos amis et votre famille de vous payer en BTC. Mais qu'en est-il lorsque votre activité dépasse le cercle assez restreint de ces personnes ? Cette section va donc s'intéresser aux diverses plateformes existantes qui facilitent la vente de produits en échange de bitcoins : les sites de ventes aux enchères, les boutiques en ligne, et les profits que vous pouvez tirer des forums en ligne.

## Vendre aux enchères

Vendre des marchandises contre des bitcoins est une pratique aussi vieille que la monnaie électronique elle-même. Toutefois, il a fallu du temps avant que des structures ne commencent à commercer en bitcoins. Ainsi, les sites et les salles de vente aux enchères, comme eBay, sont des lieux privilégiés pour le bitcoin.



Très peu de sites de vente aux enchères acceptent les paiements en bitcoins au moment où nous écrivons ces lignes. Cependant, plus les développeurs exploreront la possibilité de créer de tels sites décentralisés, plus leur nombre augmentera dans les années à venir. Vous trouverez une liste de ces sites à l'adresse [https://en.bitcoin.it/wiki/Trade#Auction\\_sites](https://en.bitcoin.it/wiki/Trade#Auction_sites).



Au fil des ans, divers marchés ont accepté les paiements en bitcoins. Mais, beaucoup d'entre eux, comme Silk Road et Silk Road 2.0 furent connus pour leurs marchandises illégales et leurs services douteux. Cette expérience démontra à l'univers du bitcoin que les choses devaient changer si l'on voulait que la crypto-monnaie ne soit pas assimilée aux activités suspectes.

Il y a environ deux ans, le premier site de vente aux enchères commença à expérimenter les paiements en bitcoins. Contrairement à eBay, ce site Web ne se contente pas de mettre en rapport des acheteurs et des vendeurs du monde entier. En effet, pour décourager toute activité illégale, les sites de ventes aux enchères mettent en place des systèmes permettant d'asseoir leur notoriété et d'obtenir des avis des utilisateurs.

Plutôt que d'utiliser un système de paiement centralisé comme eBay le fait avec PayPal, ces autres sites de ventes aux enchères utilisent des BTC comme moyen de paiement. Comme les paiements en bitcoins ne sont pas remboursables, il a fallu mettre en place un autre type de protection pour les acheteurs et les vendeurs.



La détention de fonds de la part d'une tierce personne durant la vérification nécessaire à la validation de la transaction, permet de protéger l'acheteur et le vendeur. Lors d'un achat, l'acheteur envoie les BTC à

une adresse de dépôt. Le vendeur est ainsi assuré de recevoir la totalité de la somme, et non pas de faire a priori confiance à l'acheteur sur sa capacité à assumer sa dépense. De leur côté, les acheteurs sont protégés par les règles liées à ce type de dépôt. En effet, les fonds ne seront « débloqués » que si l'acheteur confirme la réception des produits achetés sur le site de vente aux enchères. Une fois que tout a été vérifié et que la transaction paraît correcte, l'acheteur indique à ce service qu'il peut délivrer les fonds au vendeur. Lorsque la transaction est terminée avec succès ou non, les deux parties peuvent laisser un avis sur leur partenaire dans la transaction.

## Créer votre propre boutique en ligne

Une autre manière d'utiliser le bitcoin commercialement consiste à créer votre propre boutique en ligne qui accepte les paiements en bitcoins.

Créer une boutique virtuelle et accepter les bitcoins n'est pas une opération insurmontable à réaliser, car les plateformes les plus communément utilisées pour cela proposent des modules de paiement en bitcoins prêts à l'emploi.



Une des techniques les plus simples pour vous mettre le pied à l'étrier consiste à créer un site Web sur WordPress à l'adresse

<https://fr.wordpress.com/create/>. WordPress

couvre de nombreux besoins, du blog à la boutique en ligne en passant par tout autre type de sites Web. Pour le commerce en ligne, des plugins comme WooCommerce, WP eCommerce, et GoUrl MarketPress permettent d'accepter très facilement le bitcoin. Vous trouverez une liste de plugins pour WordPress à <http://bloginfos.com/plugin-bitcoin/> ou <https://fr.wordpress.org/plugins/search/bitcoin>

Parallèlement à WordPress, d'autres processeurs de paiement en bitcoins, y compris Bitpay et Coinbase (voir plus loin dans ce chapitre), proposent des solutions d'e-commerce intégrées à leurs services qui peuvent se mettre en place dans des solutions de panier en ligne comme XCart et ZenCart, pour ne citer qu'eux.



Vous devez décider d'effectuer ou non chacune des transactions en BTC. Il existe un risque associé à la conservation des fonds en bitcoins, car la valeur de cette monnaie est très volatile puisque des variations sont observées quotidiennement. De ce fait, conserver des fonds en bitcoins signifie une fluctuation de la valeur possédée. En fonction des produits que vous vendez et des fournisseurs à payer, il peut s'avérer

judicieux de convertir immédiatement les BTC en monnaie locale.

## Vendre sur les forums BitcoinTalk

Voici sans doute la meilleure méthode : vendre des marchandises en échange de bitcoins en postant vos produits sur des forums BitcoinTalk. Pour en savoir plus à ce sujet, consultez le site [www.bitcointalk.org](http://www.bitcointalk.org). Il propose une section dédiée à l'achat et à la vente de produits sous forme physique et numérique. Cependant, il existe des inconvénients à passer par un forum plutôt qu'un site de vente aux enchères, ou de monter sa propre boutique.



La vente de produits en BTC sur des forums BitcoinTalk repose sur un système de confiance validé par le succès des ventes antérieures. En supposant que votre compte n'a aucun avis favorable, quel acheteur vous ferait a priori confiance dans un système de paiement sans remboursement possible ? Résoudre ce problème est plus simple qu'il n'y paraît. En effet, de nombreuses personnes acceptent de servir d'intermédiaire en conservant les fonds jusqu'à ce que les deux parties à la transaction soient d'accord pour la valider (voir plus haut dans ce chapitre). Les mêmes règles que sur un site de vente aux enchères s'appliquent alors :



l'acheteur envoie les fonds sur le « compte séquestre », le vendeur expédie l'objet, et une fois que l'acheteur a vérifié son colis, les fonds sont remis au vendeur.

En théorie, les deux parties sont protégées. Pourtant, il y a un inconvénient. Un peu comme avec eBay, l'intermédiaire chez qui la somme est consignée devra prendre une décision en son âme et conscience dès qu'un litige surviendra. Imaginez un scénario où vous expédiez le produit, et où l'acheteur prétend avoir reçu un colis vide. L'acheteur a photographié le colis fermé, puis le colis ouvert avec rien à l'intérieur.



Si le vendeur n'a pas photographié ce même paquet avec l'article à l'intérieur, voire fait une vidéo montrant la procédure d'emballage, il y a matière à litige. Disposer d'un numéro de suivi du colis peut permettre au dépositaire des fonds de savoir où en est la livraison. C'est alors à cet intermédiaire, détenteur provisoire des fonds, de décider, en son âme et conscience, qui a raison et qui a tort entre l'acheteur et le vendeur. Mais, tout être humain est faillible.

Un site de vente aux enchères ou votre propre boutique en ligne est sans doute le meilleur moyen de vendre des produits payés en bitcoins. En revanche, les forums BitcoinTalk créent des transactions peer-to-peer où, généralement, aucun intermédiaire n'est requis, sauf

peut-être un dépositaire temporaire des fonds. L'objectif final est de satisfaire le client et d'être payé. Par conséquent, choisissez la méthode la plus appropriée à vos besoins.

Consultez ces deux sections du site :  
<https://bitcointalk.org/index.php?board=49.0> et  
<https://bitcointalk.org/index.php?board=51.0>.

## Les solutions de paiement en bitcoins

---

Comme nous l'avons déjà expliqué, contrairement aux paiements effectués par carte bancaire, les paiements en bitcoins sont l'objet de frais minimum, mais aucun remboursement n'est possible. Cela signifie qu'une fois que quelqu'un envoie des fonds depuis son portefeuille à un destinataire, cette transaction devient irréversible, et les fonds payent ainsi la marchandise.

Bien entendu, le destinataire pourrait redonner l'argent reçu si nécessaire. Ce qu'il faut simplement comprendre c'est qu'un paiement en bitcoins ne peut être ni annulé ni remboursé, contrairement aux paiements réalisés avec une carte de crédit. La raison en est simple : les cartes bancaires sont délivrées par une institution financière centrale qui peut rembourser des fonds versés. Avec le bitcoin, aucune autorité

centrale n'est capable de reverser de l'argent électronique, et les utilisateurs sont seuls responsables du stockage et de l'envoi des fonds en BTC.



Rien ne justifierait le remboursement d'une transaction effectuée en bitcoins. En effet, chaque transaction est diffusée sur la chaîne de blocs, un livre public qui répertorie tous les transferts en BTC passés, présents, et futurs (voir le [Chapitre 7](#) pour plus d'informations sur la chaîne de blocs). La chaîne de blocs montre clairement, à tout un chacun, où se trouvent les fonds provenant de « l'adresse A » et quelle en est la quantité.

Cela nous amène à un autre aspect des bitcoins et du remboursement des sommes qu'il est important de garder à l'esprit. Chaque fois qu'un client paye en bitcoins directement ou via une plateforme de change, il est essentiel qu'il sache que cette méthode de paiement est irréversible. Par exemple, si vous vendez à Jean des produits facturés en bitcoins, la transaction échouera pour une raison très simple : les méthodes de paiement traditionnelles comme PayPal ([www.paypal.fr](http://www.paypal.fr)), Skrill ([www.skrill.com](http://www.skrill.com)), et les transactions par carte bancaire sont sujettes à des fraudes et à des remboursements.

PayPal est une plateforme particulièrement sensible pour les paiements en bitcoins. Tout d'abord, PayPal

n'offre pas de protection suffisante au vendeur sur des produits numériques. Ensuite, au moment de la rédaction de ce livre, le bitcoin est encore assimilé à un produit numérique dans les conditions d'utilisation du service. Si l'acheteur demande un remboursement à PayPal, même après avoir reçu les bitcoins, l'argent lui sera reversé sans qu'aucune question ne lui soit posée. Ce principe est également appliqué par Skrill. Il suffit que l'acheteur ouvre un incident pour qu'on lui reverse ses fonds.

Quel que soit le scénario, le vendeur perd ses bitcoins, car la méthode de paiement est irréversible.



La gestion des bitcoins tombe sous la seule responsabilité de l'utilisateur final. Disposer d'un contrôle absolu sur vos finances personnelles donne une extrême sensation de puissance et fait peser sur vous une grande responsabilité.

Les commerçants qui acceptent le bitcoin perçoivent l'avantage que procure un moyen de paiement qui ne peut pas effectuer de remboursement. La fraude sur les paiements en ligne est l'un des plus gros soucis pour les revendeurs du monde entier. Le bitcoin peut régler ce problème. En plus, en acceptant le bitcoin, le commerçant ouvre son activité à un nombre de clients bien plus élevé.



Accepter les paiements en ligne ou hors ligne en bitcoins est devenu incroyablement facile et convivial aujourd'hui. Une grande variété de services sont à votre disposition pour intégrer, dans votre site Web, des boutons qui renvoient vers un paiement en bitcoins. Certains proposent de générer des codes QR pour les paiements en magasin. La suite de cette section présente quelques-unes de ces options de paiement.

## BitPay

Probablement l'une des sociétés de paiements les plus célèbres ([www.bitpay.com](http://www.bitpay.com)). Elle fut l'une des premières à travailler avec le bitcoin et reste aujourd'hui l'un des leaders des processeurs de paiement dans cette monnaie.



BitPay présente de nombreux avantages pour les clients et les commerçants souhaitant payer en bitcoins. Pour les clients, plusieurs options permettent d'effectuer une transaction via BitPay : ils peuvent flasher un code QR, copier manuellement l'adresse de destination, ou bien cliquer sur un lien afin de payer directement avec le logiciel bitcoin installé sur leur ordinateur.

De leur côté, les commerçants n'ont pas à se soucier de la configuration de BitPay. Ainsi, pour les propriétaires d'un site Web, quelques lignes de codes suffiront pour

ajouter BitPay au système de paiement du panier. BitPay se charge de convertir les prix en monnaie locale, mettant ainsi en place un système simple pour les commerçants.



Autre avantage : BitPay – à l’instar d’autres processeurs de paiement mentionnés dans ce chapitre – offre un service de conversion en monnaie fiduciaire et à la volée des transactions effectuées en bitcoin. Dans la mesure où le bitcoin est une crypto-monnaie volatile, c’est une bonne idée de convertir ces fonds aussi vite que possible.

Contrairement aux opérations réalisées avec des cartes bancaires qui nécessitent environ une semaine avant d’être créditées sur le compte du commerçant, les paiements en bitcoins sont versés le premier jour ouvrable suivant la transaction.

C’est donc un système idéal qui permet aux commerçants de disposer de liquidité plus rapidement et d’éliminer ainsi les points de friction éventuels avec leurs fournisseurs.

BitPay inclut gratuitement ce système de conversion dans son kit de démarrage. De facto, le bitcoin apparaît comme la solution de paiement la moins chère si nous la comparons aux autres moyens utilisés aujourd’hui. De plus, l’intégration de BitPay comme système de

vérification des paiements ne nécessite aucune infrastructure particulière ni investissement.

Mais il y a plus. BitPay autorise les commerçants à accepter les paiements par périphériques mobiles. Des factures peuvent ainsi être établies avec l'application pour mobile de BitPay. Elle consiste habituellement en un code QR qui contient l'adresse et le montant du paiement. Le client doit simplement flasher le code QR avec son application bitcoin, cliquer ou toucher un bouton Send (ou Envoyer), et la transaction est opérée.

Si vous avez besoin de fonctionnalités supplémentaires, envisagez de mettre à jour BitPay en intégrant, par exemple, QuickBooks POS ou un accès VPN. Les offres Business et Entreprise ajoutent des fonctionnalités à l'offre initiale gratuite. Cette dernière est largement suffisante pour couvrir les besoins de la majorité des vendeurs. Pour plus d'informations, consultez la page <https://bitpay.com/pricing>.

## Coinbase

Coinbase est un autre processeur de paiement très populaire. Similaire à BitPay (voir la précédente section), Coinbase offre davantage de fonctionnalités aux commerçants qui souhaitent découvrir l'univers des paiements en bitcoins. Coinbase est disponible à

l'international suivant ainsi le chemin tracé par BitPay au fil des ans.



Coinbase agit différemment de ses concurrents. Aucun frais n'est prélevé sur le premier million de dollars. Au-delà, des frais à hauteur de 1 % sont appliqués. Pour de nombreux commerçants, il faudra pas mal de temps avant de dépasser cette limite de 1 million et se voir ensuite appliquer 1 % de frais sur toutes les transactions.



La conversion de bitcoins en monnaie courante via Coinbase se fait entre un et trois jours ouvrables selon la localisation du commerçant. Les paiements sont initiés quotidiennement, ce qui est bien plus rapide que les cartes bancaires ou les virements.

L'API de Coinbase permet au commerçant de rembourser le client. C'est une fonction spectaculaire dans la mesure où, comme nous l'avons maintes fois répété, les paiements en bitcoins ne le permettent pas techniquement. Cependant, rien n'empêche le destinataire des fonds de renvoyer manuellement l'argent à son expéditeur. Eh bien, c'est ce principe qui est appliqué ici. En quelques clics, le commerçant peut rembourser le client si cela s'avère nécessaire.



Pour plus d'informations sur le remboursement via Coinbase, visitez la page



<https://www.coinbase.com/merchants?locale=fr>.

## Accepter les bitcoins dans votre boutique

---

Il ne faut pas beaucoup de temps à un commerçant ou à un revendeur pour accepter les paiements en bitcoins, et cela sans coût supplémentaire au niveau de son infrastructure.



À la différence de bien des méthodes de paiements traditionnelles, ceux qui sont effectués en bitcoins s'avèrent très simples, aussi bien pour le commerçant que pour le client. De plus, les frais associés aux transactions sont ridicules. Enfin, vous n'avez aucune inquiétude à avoir quant à un afflux massif d'espèces puisque le bitcoin n'est pas un paiement physique.

### Les boutiques en ligne

Les revendeurs en ligne peuvent facilement intégrer les paiements en bitcoins sur leurs boutiques en ligne. Quelques lignes de code suffisent. Une fois que cette intégration est faite, vous pouvez accepter les paiements en bitcoins sans problème et ainsi intéresser davantage de clients à travers le monde.

La plupart des processeurs de paiement en bitcoins offrent des solutions d'e-commerce ainsi qu'une assistance à leur intégration. De plus, la majorité des solutions d'e-commerce prennent déjà en charge l'intégration du bitcoin. La raison en est simple : aucun coût supplémentaire n'est appliqué pour utiliser le bitcoin, tout en ouvrant la porte de votre boutique à une clientèle bien plus large. Quel commerçant refuserait pareille opportunité ?

Si un revendeur possède déjà un site Web et un nom de domaine, aucune infrastructure supplémentaire ne sera nécessaire. En effet, il existe des solutions personnalisées disponibles auprès des processeurs de paiement en bitcoins (voir la précédente section).

Un des aspects les plus séduisants des transactions en bitcoins est que la plupart des processeurs de paiement n'appliquent pas de frais pour convertir ces paiements en monnaie locale. Chaque processeur propose à ses clients l'option de convertir en argent normal, et à la volée, chaque transaction effectuée en bitcoins afin de les protéger contre la volatilité de cette crypto-monnaie. Les fonds convertis sont ensuite déposés sur le compte bancaire du client sous 48 heures (deux jours ouvrables).

Une fois que vous avez intégré les paiements en bitcoins dans votre solution d'e-commerce existante, il

reste une étape essentielle à accomplir : Insérer le fameux logo « Nous acceptons les bitcoins » ([voir la Figure 8.1](#)) sur votre page Web. Ce bouton informe les clients, mais peut également inciter d'autres commerçants à accepter les paiements dans cette monnaie électronique.



**FIGURE 8.1** : Les bitcoins sont enfin acceptés... hurra !



La procédure de paiement en ligne est très simple. Tous les prix affichés en monnaie locale sont convertis en bitcoins par le processeur de paiement au moment de la validation de la commande. Sur la page de paiement, les clients voient le code QR qu'ils peuvent flasher avec leur périphérique mobile, ainsi qu'une adresse bitcoin où ils peuvent envoyer manuellement des fonds à partir de leur logiciel bitcoin. Une fois que la transaction a été diffusée sur le réseau bitcoin, la procédure de paiement est terminée.

## Les boutiques en dur

À l'image des boutiques en ligne, les commerces en dur, c'est-à-dire là où vous avez l'habitude de vous rendre physiquement pour acheter des produits, n'ont pas besoin de matériel supplémentaire pour accepter les paiements en bitcoins. Il suffit de disposer d'un ordinateur, d'un smartphone, ou d'une tablette et d'une connexion à Internet. La plupart des lieux disposent de ce genre d'équipements. De facto, il ne faut que quelques minutes pour accepter les paiements en bitcoins.



Choisissez simplement le processeur de paiement. Il vous procurera sûrement une application mobile ou une interface Web permettant de lancer les paiements en bitcoins. Quelques minutes suffiront à vous rendre opérationnel.

Comme les paiements ligne, le règlement des achats en boutique se fait par le flashage de codes QR. Les processeurs de paiement en bitcoins permettent aux marchands de générer ces codes avec leur adresse BTC et le montant associé via l'appli ou l'interface Web.

Une fois que le client a flashé le code QR avec son appareil mobile, le paiement est accepté en quelques secondes.



Comme vous pouvez le constater, accepter les bitcoins n'est qu'une question de volonté, car aucune excuse

technique ne peut être avancée contre ce moyen de paiement, qu'il soit utilisé en ligne ou directement en magasin. Dans ce dernier cas, le commerçant sera toutefois contraint de saisir quelques informations afin de générer le code QR. Ce type d'apprentissage est tout à fait normal puisqu'il s'agit d'une nouvelle technologie. Toutefois, les clients aguerris à cette technique se feront une joie d'aider les commerçants en cas de besoin.

## Chapitre 9

# Rester du bon côté de la loi

---

### DANS CE CHAPITRE

- » Faire face aux taxes
  - » Comprendre le cadre complexe de la réglementation
  - » La question d'un agrément ou non
- 

Tout ce que nous ne comprenons pas nous fait peur. De ce fait, nous souhaitons tout contrôler : les extra-terrestres, le monstre du Loch Ness, nos partenaires, les avocats, et les agents fiscaux. Notre contrôle peut s'exercer sur le bitcoin jusqu'à une certaine limite. Bannir le bitcoin n'aurait aucun sens simplement parce qu'il n'existe pas de méthode permettant de le contrôler correctement. Malgré la transparence de la chaîne de blocs, les adresses des portes-monnaies demeurent anonymes puisqu'aucun nom ou lieu n'y sont attachés.

Pourquoi certains cherchent-ils à interdire le bitcoin ? (Quelques suppositions sont faites dans l'encadré situé à la fin de ce chapitre.)



Certains aspects du bitcoin demandent davantage d'investigations pour définir un cadre réglementaire. Tout d'abord, force est de constater qu'acheter et vendre des produits et des services avec des bitcoins est une activité tout à fait légale. D'autre part, la plupart des banques centrales ont alerté les institutions financières et les particuliers des risques associés au bitcoin, sans pour autant proscrire l'utilisation de cette monnaie électronique.

Ce qui inquiète les autorités policières et les instances gouvernementales est le fait que le bitcoin n'est pas contrôlé par une autorité centrale. Chaque utilisateur de bitcoins en détermine l'avenir sans se plier à la volonté d'une poignée d'individus qui s'accaparent le pouvoir. La décentralisation est une nouvelle race de technologie que nous avons bien du mal à appréhender, et qui ne facilite donc pas l'intégration du bitcoin dans un climat de confiance absolu.

Ce chapitre traite de l'aspect juridique du bitcoin dans divers pays et explique ce que vous pouvez faire pour vous protéger, mais aussi ce que vous devez faire pour ne pas fâcher votre percepteur.

## **Bitcoin et fiscalité**

---

Le célèbre écrivain Daniel Defoe a dit : « La mort et les impôts : les seules choses certaines ». Si je peux vous aider sur la fiscalité du bitcoin, je crains ne rien pouvoir faire contre l'aspect inéluctable de votre mort.

Malgré les avertissements émis par les gouvernements et les banques centrales sur l'utilisation du bitcoin et sa nature perturbatrice (voir le [Chapitre 1](#)), la plupart des pays sont assez satisfaits de la mise en œuvre de cette monnaie électronique, et ceci pour une raison très simple : les taxes.

Comme la crypto-monnaie peut s'apparenter à un revenu ou à une rémunération, elle peut être taxée. Ajoutez à cette observation que l'utilisation du bitcoin pour payer des produits et des services est taxée dans certains pays. Aussi longtemps qu'un état peut taxer les résultats économiques d'une nouvelle technologie, il n'a aucune raison majeure de s'y opposer.



N'oubliez jamais que le paysage fiscal peut changer à tout moment. Par conséquent, renseignez-vous auprès de votre organisme fiscal pour savoir comment utiliser le bitcoin, et si vous devrez payer des taxes sur cette utilisation. Des pays comme le Brésil, le Canada, la Finlande, la Bulgarie, et le Danemark ont émis des directives sur les taxes appliquées à l'utilisation du bitcoin. Toutes ces directives ne sont pas encore appliquées au moment où nous écrivons ces lignes.



D'autres pays comme la Belgique, la Grèce, Hong Kong, le Japon, et la Nouvelle-Zélande n'ont pas défini de taxe sur le bitcoin ou d'autres monnaies virtuelles.

Mais soyons certains que chaque pays regarde de près le bitcoin et son impact sur l'économie. Étant donné la nature décentralisée et globale du produit, il semblerait logique qu'une réglementation au niveau mondial soit définie avant que des pays se lancent dans l'édiction d'une réglementation locale comme ils le feraient pour une monnaie standard. Par exemple, de nombreux pays ont leurs propres lois pour lutter contre le blanchiment d'argent et le financement du terrorisme (AML/CFT) via l'organisation intergouvernementale du Groupe d'action financière (GAFI). Il est possible que des accords intergouvernementaux soient exigés par certaines nations avant qu'elles ne mettent en place une réglementation, ou des directives fiscales sur le bitcoin et les autres crypto-monnaies à l'intérieur de leurs frontières. C'est d'ailleurs cet aspect fiscal, donc la rentrée d'argent dans les caisses de l'état, qui poussera bien des pays à réglementer et à taxer le bitcoin et son utilisation.

## La fiscalité



Les directives sur la question ne cessent d'évoluer dans chaque pays. Il est donc impossible de vous affirmer

que ce que vous lirez dans les prochaines sections est encore d'actualité.



En Europe, tout dépend des décisions prises par l'Union européenne. Mais un certain nombre de pays ont défini leurs propres directives sur la taxation du bitcoin. L'Union européenne ne tardera pas à prendre des résolutions à ce sujet, résolutions qui changeront radicalement le paysage actuel du bitcoin dans cette partie du monde. En Asie, les choses sont plus claires. Seule Singapour taxe activement le bitcoin aussi bien en tant que « monnaie d'achat et de vente » qu'en tant que « produit financier ». Pour l'achat des marchandises, de la TVA est appliquée à l'entreprise locale pour l'achat ou la vente de produits.

Dans cette section, nous présentons les pays qui appliquent une taxe sur le bitcoin. Toutefois, il est probable que les choses aient évolué depuis que nous avons écrit ces lignes.

## Australie

La taxe GST sur les produits et les services est applicable aux transactions réalisées en bitcoins au-dessus de 10 000 \$ australiens. Mais une directive récente a proposé de traiter le bitcoin et les autres monnaies virtuelles comme les « monnaies réelles »,

entraînant une taxation différente dans un futur proche.

## Brésil

La Receita Federal du Brésil a défini les règles de taxation suivantes : les monnaies électroniques sont considérées comme des actifs financiers et sont taxées à hauteur de 15 % au moment de la vente. Cependant, tout bitcoin vendu en dessous de 35 000 réaux n'est pas taxé. Enfin, toute personne possédant plus de 1 000 réaux en monnaie électronique doit les déclarer sur sa feuille d'impôt.

## Bulgarie

La Bulgarie est l'un des quelques pays européens qui taxent le bitcoin. La National Reserve Agency a décidé que la vente de monnaies électroniques serait traitée comme la vente d'actifs financiers. Ainsi, les plus-values sont taxées à hauteur de 10 %. Les gains provenant d'activités commerciales facturées en bitcoins ou avec une autre monnaie électronique sont taxés au même niveau que ceux réalisés avec la monnaie locale du pays.

## Canada

Au Canada, les transactions correspondant à l'achat et à la vente de marchandises et de services tombent dans la catégorie des échanges. Ainsi, tout profit réalisé est considéré comme un revenu.

Chaque transaction est appréciée au cas par cas, et toute activité destinée à réaliser des profits est considérée comme un revenu qui doit être fiscalement déclaré à la fin de l'année. Les valeurs des marchandises et des services provenant d'opérations d'échange doivent être déclarées dans les revenus, car elles sont supposées être le fruit d'activités commerciales.

## Finlande

La Finlande apparaît un peu comme un drôle d'oiseau en ce sens que le gouvernement applique une taxe sur les plus-values et sur les gains réalisés en participant au minage. En 2014, la Finlande considéra le bitcoin comme une matière première, car il ne réunissait pas toutes les conditions permettant de le définir comme une monnaie. Il en résulte aujourd'hui une taxation du bitcoin assez confuse en Finlande. Il est conseillé de se renseigner auprès d'un représentant local.

## France

En France, les gains tirés d'unités de compte virtuelles stockées sur un support électronique comme les bitcoins sont soumis à l'impôt sur le revenu quand ils sont occasionnels, et cela au titre des bénéfices non commerciaux. En revanche, dès que cette activité devient régulière, la déclaration se fait au titre des bénéfices industriels et commerciaux. Il existe ensuite d'autres subtilités fiscales inhérentes à la complexité du droit français en la matière.

## Allemagne

L'Allemagne est sans doute l'état d'Europe le plus avancé en matière de taxation du bitcoin. Ainsi, n'importe quel montant de bitcoins détenu depuis plus d'un an est exempté de la taxe de 25 % sur les plus-values. En Allemagne, le bitcoin est considéré comme une « monnaie privée ».

## Île de Man

L'Île de Man, un territoire autonome dépendant de la couronne britannique, est l'un des rares endroits où un cadre réglementaire intelligent a été mis en place pour les monnaies électroniques. Les plateformes installées à l'Île de Man doivent adhérer aux directives contre le blanchiment d'argent et sur la connaissance du client, ainsi que sur la lutte contre le financement du

terrorisme. Le respect de ces règles est renforcé par le régulateur financier de l'île de Man, et par la FSA (Financial Services Authority).

Contrairement à la majorité des autres pays, l'île de Man met activement en œuvre les étapes nécessaires à la création d'un cadre réglementaire pour les monnaies électroniques. Le bitcoin et les autres crypto-monnaies ne tombent pas sous le coup des activités réglementées par la FSA de l'île. En revanche, les sociétés qui utilisent les crypto-monnaies doivent se soumettre aux lois AML/CFT introduisant les amendements de 2015 sur les produits d'activités criminelles. Une telle approche permet aux startups de s'enregistrer sans être contraintes par des exigences réglementaires radicales. Cela favorise l'entrepreneuriat sur l'île et permet au secteur de la crypto-monnaie de prospérer à mesure du développement d'une réglementation au fil des ans. C'est une impulsion qui aidera à légitimiser le bitcoin à long terme, puisque la monnaie électronique offre de nombreux avantages (dont vous ne doutez pas un instant depuis que vous avez commencé la lecture de ce livre).

## Les Pays-Bas

Aux Pays-Bas, le bitcoin est considéré comme n'importe quelle autre devise étrangère à laquelle est

ainsi appliquée la même taxation.

## Slovénie

La Slovénie ne taxe pas la vente de bitcoins aux plateformes de change ou aux autres membres de la communauté. En revanche, le bitcoin est sujet à l'impôt sur le revenu comme la monnaie standard. Le montant de cet impôt est calculé selon le taux de change BTC/EUR au moment de la transaction.

## Royaume-Uni

Le Royaume-Uni va plus loin en excluant les monnaies électroniques du champ de la valeur ajoutée, ce qui est particulièrement apprécié par les entreprises. Au moment de l'écriture de ce livre, Jersey, un autre territoire autonome sous dépendance britannique, annonce vouloir appliquer une légère réglementation sur le bitcoin d'ici quelque temps.

## USA

Les États-Unis se demandent toujours s'il faut taxer le bitcoin à un niveau fédéral et comment. Du fait de la méconnaissance de l'impact qu'aura le bitcoin sur l'économie, il est difficile de statuer sur un pourcentage de taxation approprié, et de définir quelles personnes et quelles activités tomberont dans cette catégorie.

Dans l'esprit, ceux qui perçoivent un revenu en monnaies virtuelles telles que le bitcoin seront imposés. Cependant, ce revenu peut faire partie de l'une des quatre catégories suivantes : salaire, revenu annexe, revenu d'échanges, et gains aux jeux. Un pourcentage spécifique s'applique à chacune de ces catégories.

Avec la monnaie virtuelle, l'évasion fiscale est impossible. C'est d'ailleurs un des nombreux travers financiers que les experts du bitcoin veulent éviter en collaborant avec les représentants du gouvernement pour définir un cadre de régulation approprié.



Les USA devront sortir de leur relatif mutisme sur la réglementation du bitcoin. Chaque état peut élaborer ses propres lois et obligations sur l'utilisation des bitcoins pour les particuliers et les entreprises. Ainsi, des états peuvent parfaitement décider de ne pas réglementer le bitcoin selon que la crypto-monnaie est ou non assimilée à une devise, à un actif numérique, ou à un produit d'échange.

De ce fait, il faudra du temps avant que le législateur et les régulateurs financiers trouvent un accord sur la réglementation de l'utilisation des bitcoins. Certaines régions ont défini des directives fiscales sur le bitcoin, alors que le gouvernement cherche encore à savoir quel sera l'impact financier de la monnaie électronique sur



les économies locales avant d'aller plus loin dans la réglementation.

## Aide sur la fiscalité du bitcoin

Le bitcoin n'en est qu'à ses débuts. De ce fait, il est difficile de définir et de vous présenter un cadre fiscal global s'appliquant aux transactions réalisées dans cette monnaie virtuelle. Heureusement, il existe quelques services et sociétés qui peuvent aider les utilisateurs à calculer le montant des taxes potentielles à payer.

Gardez à l'esprit que ces services n'existent pas dans tous les pays. Bien qu'il semble plausible que ce genre d'activité se développera dans les années à venir, il n'existe encore aucun projet officiel allant dans cette direction.



Voici quelques services et sociétés qui aident les utilisateurs du bitcoin dans le calcul des éventuelles taxes :

- » Un logiciel gratuit appelé LibraTax ([www.libra.tech](http://www.libra.tech)) prend en compte le bitcoin. Il peut calculer la taxe sur les plus-values ainsi que les pertes (pour les déductions) et donner un aperçu sur le revenu en bitcoins imposable. Pour une faible contrepartie financière, cette société créera un rapport détaillé

pour vous aider à économiser votre argent et votre temps.

- » BitcoinTaxes (<https://bitcoin.tax>) est une plateforme de calcul des taxes sur les plus-values et les revenus selon les réglementations en vigueur. Ce site prend en charge le bitcoin et les autres monnaies électroniques comme Litecoin et Dogecoin. Les données de vos transactions peuvent être importées depuis la majorité des plateformes de change ou de bitcoins, et le calcul se fait dans une dizaine de devises. Le service est gratuit jusqu'à 100 transactions. Au-delà, vous devrez vous acquitter d'un abonnement Premium de 19,95 \$ par an. Avec cette formule, vous pourrez importer vos transactions directement depuis la chaîne de blocs.

## La réglementation du bitcoin à travers le monde

---

Les réglementations sur le bitcoin diffèrent selon les pays, exactement comme les taxes que nous connaissons aujourd'hui. Dans certains pays, elle diffère même d'un état ou d'une région à une autre. En effet, aucune règle n'est gravée dans le marbre, et certains pays ont même décrété qu'ils ne réglementeraient pas le bitcoin.



Il existe très peu d'endroits au monde où des règles ont été édictées et sont appliquées. La majorité des pays ont décidé d'effectuer des mises en garde en expliquant les risques qui pèsent sur le bitcoin, car il n'est pas contrôlé par une autorité centrale, et qu'il n'a aucun actif physique comme équivalent pour en assurer la valeur.

Il reste pourtant à démontrer que le monde n'est pas prêt pour cette monnaie marginale qui vient mettre à mal le système financier tel que nous le connaissons depuis toujours. En effet, transférer le pouvoir de services centralisés à l'utilisateur est une bombe atomique dans le monde de la finance.

Cela va sans dire que la plupart des gouvernements et des institutions financières sont conscients de l'évolution de ce paradigme. Et même si divers pays ont décidé de taxer le bitcoin, il n'en demeure pas moins que cette monnaie électronique aura un impact majeur sur les économies locales, avec des incidences positives ou négatives sur les institutions financières actuelles.

## Réglementer avec BitLicense

Il semble difficile d'appliquer au bitcoin des réglementations existantes sans obtenir quelques effets allant à l'encontre de la philosophie de cette crypto-

monnaie. Nous pouvons donner comme exemple la réglementation BitLicense de l'état de New York. Une autorité centrale a édicté des règles pour les sociétés utilisant le bitcoin dans l'état de New York, dont une grande proportion de la communauté bitcoin est plutôt intransigente sur le sujet.



La principale préoccupation de ces sociétés utilisant le bitcoin concerne cette réglementation BitLicense dont l'une des mesures obligeait de communiquer, à l'état de New York, des informations sur leurs clients. Beaucoup de leaders de l'industrie y virent une atteinte à la vie privée des clients, amenant quelques sociétés à cesser leur activité dans l'état de New York.

La demande de Bitlicense prévoit 5 000 \$ de frais non récupérables qui s'ajoutent à d'autres coûts juridiques pouvant aller jusqu'à 20 000 \$. Il n'y a aucune garantie de succès, et les sociétés du bitcoin sont obligées de fournir aux autorités des détails sur leur modèle économique et sur leurs clients.

Cerise sur le gâteau, la réglementation BitLicense contient quelques directives sur le blanchiment d'argent qui contrastent avec les directives fédérales. Pour couronner le tout, les sociétés du bitcoin sont bien plus contrôlées que les institutions financières traditionnelles qui ont pourtant des antécédents de

fraude, de corruption, et de mauvaise gestion des fonds qui leur sont confiés.



La réglementation du bitcoin a pour but de légitimer la monnaie électronique. Cependant, nous pensons que le BitLicense est l'exemple parfait de ce qu'il ne faut pas faire. Les exigences réglementaires mises en place entraveront le développement du bitcoin dans l'état de New York, et les frais excessifs qui lui sont associés pour obtenir l'agrément sont insupportables pour la majorité des entreprises.

La somme de 25 000 \$ peut sembler acceptable pour réaliser des activités commerciales dans l'état de New York, mais la majorité des sociétés du bitcoin ont une vision à long terme en tête. Le problème est que plus il y aura de sociétés qui demanderont cet agrément, plus cela incitera d'autres états à adopter cette réglementation. En le refusant et en refusant alors de travailler avec l'état de New York, les entreprises du bitcoin envoient un message très clair : la réglementation du bitcoin est une orientation positive, mais lui appliquer les mêmes réglementations qu'aux opérations financières standard serait une erreur.

## Réglementer partout

D'autres pays à travers le monde n'ont pas avancé à la même vitesse en matière de réglementation du bitcoin. Ainsi, les Pays-Bas et la Finlande ont décidé que le bitcoin se verrait appliquer une taxe sur les plus-values, sans édicter d'autres mesures réglementaires. Ces deux pays sont adeptes de la politique du « laisser-faire » tant que l'Union européenne ne statue pas sur la nécessité ou non de réglementer le bitcoin.

Les pays d'Asie ont essayé d'empêcher des processeurs de paiement tiers d'utiliser le bitcoin. Aucune loi ne proscrit le bitcoin dans les pays asiatiques – à l'exception du Vietnam – mais les banques centrales font tout ce qu'elles peuvent pour décourager les processeurs de paiement d'accepter le BTC.

Ces prochaines années joueront un rôle charnière en matière de réglementation du bitcoin et sur son adoption en masse. Une discussion saine doit prendre place entre les régulateurs financiers et les experts de l'industrie du bitcoin. Aujourd'hui, il est impossible de dire quels pays autoriseront ou proscrireont le bitcoin dans les années à venir.

## **Agréer ou non les sociétés de transfert de fonds ?**

Une question essentielle se pose lorsqu'on analyse le bitcoin en tant que support de transfert de fonds. Une société de transfert de fonds est une entité commerciale qui fournit des services de transfert d'argent ou des instruments de paiement.

Comme le bitcoin peut être dépensé, échangé, et acheté, il est transféré tout autour du monde. Cela suffit-il à considérer chaque utilisateur du bitcoin comme une entité de transfert de fonds ?



En fait, tout dépend du pays où vous résidez. Ainsi, dès qu'un particulier commence à échanger des bitcoins contre des devises standard auprès d'autres utilisateurs afin d'obtenir des gains personnels, un agrément de transfert de fonds peut être exigé.

## LE BITCOIN INTERDIT DANS PLUSIEURS PAYS

Le gouvernement vietnamien a officiellement interdit l'utilisation du bitcoin, même si aucune loi n'indique spécifiquement les peines encourues pour les contrevenants.

Le même principe s'applique en Bolivie. La banque centrale du pays, El Banco Central, a officiellement interdit toute monnaie non émise ou agréée par le gouvernement. Cette règle s'applique au bitcoin ainsi qu'aux autres monnaies électroniques telles que Namecoin, Feathercoin, Dogecoin, Quark, et Peercoin. Cette politique a été mise en place en 2014 disant clairement qu'il « est

illégal d'utiliser tout type de monnaie non émise et non contrôlée par un gouvernement ou une entité agréée. »

Aucune monnaie virtuelle n'est émise ou contrôlée par une autorité centrale. De facto, la Bolivie ne va pas adopter de sitôt les monnaies électroniques.

La Colombie est un autre pays sud-américain qui envisage d'interdire le bitcoin. Cette monnaie peut avoir un impact majeur sur les économies locales, et plus spécialement dans les pays où l'inflation et l'hyperinflation sont des problèmes importants. En Colombie, il est difficile de savoir si l'interdiction portera sur les transactions commerciales réalisées en bitcoins, ou sur la vente et l'achat de bitcoins sur les plateformes de change, ou bien encore sur ces deux activités.

L'Équateur décida d'interdire le bitcoin en 2014, ainsi que toute autre forme de monnaie électronique décentralisée. Toutefois, l'Assemblée nationale de l'Équateur a établi des directives pour la création de sa propre devise centralisée. Les responsables gouvernementaux étant autorisés à payer avec des « monnaies électroniques », il va être intéressant de voir comment ce projet fonctionnera dans le futur.

L'Islande adopte une position différente. Ainsi, l'utilisation du bitcoin comme moyen de réaliser des transactions n'est pas interdite par ce pays. En revanche, il n'est pas permis d'acheter et de vendre des bitcoins via des plateformes de change étrangères. En effet, cela constitue un mouvement de capitaux en dehors du pays qui est une violation des contrôles de capitaux effectués par l'Islande.



Le Kirghizstan n'est pas très enthousiaste à l'égard du bitcoin. La Banque nationale de la République kirghize considère l'utilisation des monnaies électroniques comme une forme de paiement illégal. La seule monnaie légale dans ce pays est le som.

D'autres pays dans le monde regardent de près le bitcoin afin d'en mesurer l'impact sur l'économie locale. Davantage d'états interdiront ou autoriseront le bitcoin à l'avenir en fonction de l'établissement d'un cadre de réglementation valable sur les différents continents.

Le bitcoin enthousiasme tous ceux qui souhaitent participer au processus de minage dans l'optique de générer d'autres bitcoins et de confirmer des transactions. Mais il ne s'agit pas ici de transférer de l'argent. En revanche, c'est exactement ce qu'il se passe lors de la vente de bitcoins à d'autres utilisateurs. Cependant, rien n'a encore été clairement édicté en la matière.

Enfin, les opérateurs de change bitcoin – des particuliers ou des entreprises qui convertissent le bitcoin de et vers des devises standard – doivent obtenir un agrément de transfert de fonds dans la plupart des juridictions. Cet agrément est nécessaire en fonction de la nature des transactions réalisées. Une des exceptions les plus significatives est celle de l'Île de Man. Dans cette juridiction, les sociétés de la crypto-monnaie doivent agir en conformité avec les directives

de l'AML/CFT supervisées par la Financial Services Authority de l'île. En revanche, leur activité principale n'est pas soumise à l'obtention d'un agrément selon les directives de la FSA.

# Chapitre 10

## Bitcoin et sécurité

---

### DANS CE CHAPITRE

- » La sécurité dans un modèle décentralisé
  - » Éviter les redoutables attaques des 51 %
  - » Éliminer les dangers de la double dépense
- 

Le bitcoin est-il sécurisé ? L'une des plus grandes préoccupations des potentiels utilisateurs et des utilisateurs actifs est de savoir si l'écosystème du bitcoin est suffisamment sécurisé pour résister aux attaques des hackers (pirates) – c'est-à-dire des personnes qui cherchent à dépenser plusieurs fois le montant du solde de leur compte de bitcoins.

La réponse à cette question ne saurait se limiter à un simple oui, et risque d'imposer l'utilisation d'une terminologie très technique. Ce chapitre couvre les explications de bases de la façon dont le bitcoin est sécurisé, et ce qui est actuellement mis en œuvre pour le sécuriser davantage du fait de l'expansion de cet écosystème.

# Le réseau bitcoin : Une présentation de son fonctionnement

---

Si l'on en croit les médias traditionnels, le réseau du bitcoin et son protocole ont été attaqués plusieurs fois dans le passé. Il n'a d'ailleurs pas totalement résisté à la vague d'attaque cyber du vendredi 12 mai 2017, mais au même titre que des institutions publiques et des entreprises, puisque 200 000 structures ont subi des dommages partout dans le monde.

Par conséquent, le bitcoin n'est pas plus en danger que n'importe quelle autre activité sur Internet. Il est donc impossible de contredire ces médias. En effet, depuis toutes ses années d'existence, des utilisateurs ont perdu des bitcoins sans pour autant engager la responsabilité du réseau lui-même. Ainsi, il faut se pencher sur ses services associés, comme les plateformes de change et les portefeuilles qui eux, en revanche, peuvent être assez mal protégés. Or, dès que ces services sont attaqués, les utilisateurs perdent de l'argent. Mais cela est totalement indépendant de potentielles faiblesses sur le réseau bitcoin appréhendé en tant que réseau décentralisé.

## Qu'est-ce qui le rend si sûr ?

## Pourquoi le réseau bitcoin est-il si sûr ? Voyons cela :

- » Le réseau bitcoin est décentralisé, et chaque individu assure qu'il n'existe pas de point central défaillant pouvant faciliter une attaque du protocole bitcoin. Chaque utilisateur peut être la victime d'un hacker, mais cela n'aura aucun impact sur le réseau. Ainsi, même si tous les utilisateurs d'un pays étaient victimes d'une attaque au même moment, le réseau bitcoin serait épargné, donc aucunement impacté.
- » Le réseau bitcoin utilise une puissante cryptographie pour garantir l'intégrité et la chronologie de la chaîne de blocs et de toutes les transactions associées. En théorie, ce niveau de cryptage peut être attaqué, mais cela exigerait de combiner pendant des années la puissance de calcul de tous les super ordinateurs existants à ce jour pour avoir une infime chance de découvrir ce nombre à 15 chiffres.
- » Chaque adresse de portefeuille est protégée par une clé privée qui doit être fournie chaque fois qu'une transaction sortante est diffusée sur le réseau. Les utilisateurs qui ont installé un logiciel de portefeuille sur leur ordinateur ou leur périphérique mobile sont les seuls propriétaires de leur clé privée. De ce fait, cette clé ne peut être découverte que si l'appareil en question est lui-même attaqué. Dans ce cas, la faute pèse sur l'utilisateur, pas sur le réseau bitcoin.

- » La création de nouveaux bitcoins, opération répondant au nom de *minage* (voir le [Chapitre 11](#)), fonctionne sur un système de consensus réparti qui confirme ou non les transactions diffusées sur le réseau bitcoin. Le minage repose sur des algorithmes informatiques très complexes. Du matériel dédié est requis pour miner les bitcoins. D'ailleurs, le nombre de ces appareils augmente mensuellement. C'est donc dans ce domaine que la décentralisation joue un rôle clé. Ainsi, les gouvernements ne peuvent pas empêcher la création de nouveaux bitcoins puisqu'il n'existe pas de point d'échec central.



Pour davantage d'explications sur le réseau bitcoin, lisez l'article de Satoshi Nakamoto à l'adresse <https://bitcoin.org/bitcoin.pdf> ou sa traduction française sur <https://www.slideshare.net/nabilbouzerna/bitcoin-a-peertopeer-electronic-cash-system-traduction-fr>.

## Le rôle des nœuds bitcoin

Les utilisateurs ne représentent pas la seule force motrice en termes de sécurité du réseau bitcoin. Ces dernières années, des nœuds bitcoin dédiés ont été ajoutés sur le réseau dans l'unique but de recevoir et de diffuser de nouvelles transactions des autres

utilisateurs et nœuds du réseau. Cet ajout a élevé l'aspect décentralisé du bitcoin à un niveau supérieur.



Chaque nœud bitcoin est un périphérique – assimilable à un ordinateur, un mobile, ou même à de petits dispositifs comme le Raspberry Pi 2 – qui contient la totalité de la chaîne de blocs depuis l'apparition du premier bloc en 2009. Le bloc genesis fut donc le premier bloc de données sur le réseau bitcoin. Il fut attribué à Satoshi Nakamoto pour 50 bitcoins. Depuis cette époque, les utilisateurs de bitcoins n'ont cessé de générer de nouveaux bitcoins et d'en diffuser via des transactions dans le monde entier.



Un nœud bitcoin dispose d'un logiciel client installé, mais il n'envoie et ne transfère jamais de l'argent de son propre chef, sauf si le propriétaire du nœud en décide autrement. Ces nœuds sont des sources supplémentaires où est stockée la totalité de la chaîne de blocs afin de vérifier l'intégrité, la neutralité, et la chronologie de toutes les transactions bitcoin réalisées entre le bloc genesis et aujourd'hui. (Consultez le [Chapitre 7](#) pour plus de détails sur la chaîne de blocs.)

Exécuter un nœud bitcoin ne récompense pas son propriétaire avec des bitcoins supplémentaires. Le seul objectif poursuivi par un nœud bitcoin est le renforcement du réseau. Au moment où nous écrivons ce livre, il existe plus de 7000 nœuds bitcoin en cours

qui s'enrichissent continuellement d'autres nœuds. Pour plus d'informations sur la localisation des nœuds bitcoin spécifiques, visitez le site Bitnodes à <https://getaddr.bitnodes.io/>.

## Protéger le bitcoin contre les hackers

---

Comme mentionné précédemment, le réseau bitcoin est une technologie sûre qui ne peut pas être attaquée, même par les plus puissants ordinateurs ou les pirates les plus expérimentés du monde. La cryptographie – une technique de sécurisation des communications qui utilise de longues séquences de codes secrets impossibles à découvrir par hasard – joue un rôle important dans la sécurisation du bitcoin. Lorsqu'elle est correctement implémentée, la cryptographie peut rendre un système extrêmement fiable.

Ces dernières années, les médias de l'information ont commis des erreurs dans leurs explications sur le fonctionnement du bitcoin. Contrairement à la croyance populaire, le bitcoin n'est pas exécuté par une seule personne ou une seule autorité, et il n'y a pas de « chef ou de directeur général du bitcoin ». Chacun joue un rôle sur le réseau bitcoin, et tous les



utilisateurs y sont égaux. De facto, le réseau n'est pas une cible intéressante pour les hackers.

Essayer de pirater le réseau bitcoin reviendrait à essayer de pirater l'Internet. C'est impossible. Le bitcoin et l'Internet sont tous deux décentralisés, sans point de défaillance central. Si une partie est attaquée, le réseau contourne le problème et continue à fonctionner comme si de rien n'était. Le même principe s'applique au bitcoin.



L'absence de point de défaillance central signifie qu'il n'y a pas de bouton marche/arrêt sur le réseau bitcoin lui-même. Ce réseau couvre la totalité du globe. Il est donc impossible d'éteindre au même moment chaque ordinateur ou d'autres périphériques connectés au réseau bitcoin. Aucun gouvernement n'en serait capable. Les états ont le pouvoir d'interdire l'utilisation du bitcoin, mais cela ne signifie pas que ce réseau devienne inopérant dans ces pays.

De plus, rien ne peut inciter les hackers à pirater le réseau bitcoin, car ils n'en tireraient aucun profit. Tous les précédents blocs du réseau incluent des BTC qui ont déjà été remis à d'autres utilisateurs du bitcoin, et il n'y a aucun moyen de changer cela. Rien n'empêchera de générer de nouveaux bitcoins, même si le réseau était piraté (ce qui est d'ailleurs impossible), et aucun

d'eux ne pourrait tomber directement entre les mains d'un hacker.



Le réseau bitcoin est un bijou technologique qui fournit des niveaux de sécurité financière jamais vus jusqu'à présent. Malgré cela, il reste un grand nombre d'aspects du réseau – et de sa chaîne de blocs – que nous ne comprenons pas encore très bien. Pour mieux comprendre le réseau bitcoin et sa puissance technologique, il faudrait des années d'études approfondies. Pour cette raison, il est important que la communauté du bitcoin se développe. Chacun a sa vision des choses et sur la manière de les améliorer et d'exploiter leur potentiel. Prévenir les attaques est souvent bien mieux que colmater les brèches suite à une attaque réussie.

## Le piratage des services bitcoin

Si le réseau lui-même est protégé contre le piratage, il n'en va pas de même pour les plateformes. Pourquoi ? Parce que malgré le concept de la décentralisation, la majorité des services et plateformes s'appuient sur une structure de serveurs centralisés.



Ces services deviennent des cibles « faciles » pour les hackers puisqu'ils présentent un point de défaillance central. Il devient donc possible de bloquer son activité.

En revanche, si un service bitcoin est attaqué, cela n'aura aucun impact sur le réseau lui-même, car ces éléments ne sont pas liés les uns aux autres.



Les services bitcoin utilisent la chaîne de blocs pour vérifier et gérer des transactions, mais ils ne sont pas connectés à la chaîne de blocs elle-même. Certaines personnes pensent que si une plateforme de change est attaquée, leur connexion à la chaîne de blocs rendra alors le réseau bitcoin vulnérable. Ce n'est pas le cas puisque les plateformes sont des services mis en place au sommet de la chaîne de blocs, mais d'une manière centralisée.

En réalité, aucune connexion directe n'existe entre le réseau bitcoin et les services. Les seules connexions qui existent entre les utilisateurs et la chaîne de blocs viennent des porte-monnaie qui se situent, d'une certaine manière, sur la couche supérieure de la chaîne de blocs elle-même. L'interaction et l'altération directes de la chaîne de blocs par des utilisateurs individuels sont impossibles. De ce fait, si un utilisateur est piraté, cela ne perturbera pas le réseau bitcoin. Ce principe s'applique aux services bitcoin. Toute attaque n'aura aucun effet direct sur le fonctionnement du réseau. Tous les services bitcoin diffusent certains types de transactions sur le réseau

bitcoin. Si ces transactions ne sont jamais relayées, le réseau bitcoin continuera à fonctionner comme avant.



En son cœur, le réseau bitcoin n'est jamais affecté par tout ce qui se déroule hors de sa portée immédiate. Il ne peut y avoir un problème que si le réseau bitcoin est attaqué et altéré à la hauteur de 51 % de la puissance totale du calcul du minage (voir la prochaine section). Toutefois, disposer de cette puissance est quasiment impossible pour tout individu ou autorité gouvernementale.

Enfin, il est plus lucratif d'attaquer des services bitcoin que le réseau lui-même. Ainsi, les plateformes de change stockent les fonds de nombreux clients. Qui dit fonds dit appât pour les hackers exactement comme pour votre compte courant. Au fil des ans, de nombreuses plateformes de change ont été victimes de ces piratages à cause d'un manque évident de mesures de sécurité efficaces.



Ces attaques n'ont jamais mis à mal la chaîne de blocs. Aussi longtemps qu'il y aura, ne serait-ce qu'un utilisateur exécutant un logiciel bitcoin sur n'importe quel appareil connecté, la chaîne de blocs continuera à faire ce pour quoi elle est faite. Chaque jour, de plus en plus de périphériques exécutent un logiciel client qui participe à la sécurisation du réseau bitcoin.

# Surveiller l'attaque des 51 %

---

Parmi les quelques événements qui peuvent porter atteinte de manière irréparable au réseau bitcoin, notons l'attaque des 51 %. Pour faire simple, disons qu'une attaque des 51 % signifie qu'un mineur ou qu'une coopérative minière détient 51 % de la capacité totale de minage. Cela peut alors conduire à la création d'une chaîne de blocs secondaire qui pourrait alors considérer comme invalides toutes les anciennes transactions de la « vieille » chaîne de blocs.

## L'attaque des 51 % en théorie

Bien que cette attaque semble improbable dans le monde du bitcoin, elle n'est pas impossible. Lorsqu'un hacker détient 51 % (ou plus) de la puissance de calcul du réseau bitcoin, il est en capacité d'exclure et de modifier l'ordre des transactions tant qu'il contrôle la totalité de la chaîne de blocs.



Une attaque des 51 % pourrait avoir des conséquences désastreuses sur la totalité du réseau bitcoin. Par exemple, la personne, le groupe, ou l'entité qui détient ces 51 %, détient aussi le pouvoir d'inverser les transactions en cours d'envoi, et cela tant qu'il garde ce contrôle. La double dépense, c'est-à-dire la possibilité de dépenser deux fois la même quantité de bitcoins –

deviendrait un problème réel, et il serait impossible de savoir quels transferts sont légitimes ou non (vous en saurez davantage à ce sujet dans ce chapitre).

Ceux qui détiennent ces 51 % pourraient valider des transactions sans obtenir de confirmation réseau. De plus, les mineurs se trouveraient dans l'impossibilité de miner des blocs valides sur le réseau, tout le bénéfice en revenant alors à ceux qui détiennent la puissance de calcul s'ils le désirent. C'est pour cette raison que les experts du bitcoin veulent s'assurer qu'une attaque des 51 % ne puisse survenir sous quelque circonstance que ce soit, même si, dans l'absolu, il est quasiment impossible de l'anticiper.

Mais il y a quelques points supplémentaires à prendre en considération dans cette approche théorique. Une des premières choses que pourrait faire le hacker c'est d'inverser les transactions bitcoin des autres utilisateurs, car ils n'ont aucun contrôle sur cette opération. Seules leurs transactions seront affectées, infligeant des dommages majeurs à la totalité du réseau bitcoin.

## COMPRENDRE LE THEORYCRAFTING

Le theorycrafting se réfère à une stratégie consistant à anticiper un fait qui n'arrivera sans doute jamais.

Dans le monde du bitcoin, cela signifie la mise en évidence de failles dans le réseau avant qu'elles ne soient exploitées par des personnes mal intentionnées. Ainsi, il est préférable d'être alarmiste plutôt que désolé. D'ailleurs, les développeurs travaillent constamment à l'amélioration de la sécurité du réseau.

Lorsqu'une technologie évolue, les développeurs doivent rester en alerte et réagir aux avancées technologiques. La sécurité est une créature en perpétuelle évolution. Si on néglige cet aspect, de gros risques sont alors encourus. Heureusement, les développeurs du bitcoin sont vigilants pour nous.

Empêcher les transactions des autres utilisateurs est impossible, car le pirate n'aura que le pouvoir d'éviter leurs confirmations pour qu'elles soient valides sur le réseau. Or, ces confirmations proviennent de la création de nouveaux blocs sur le réseau bitcoin que l'attaque des 51 % peut totalement annihiler. Par ailleurs, créer de la monnaie à partir de rien, voire changer le nombre de bitcoins rétribués par bloc, sont deux actions majeures que l'on ne peut pas altérer. En possédant 51 % de la puissance de calcul du réseau bitcoin, il y a beaucoup de choses que le hacker pourra affecter à volonté. Envoyer de l'argent auquel il n'a pas accès ne fait pas partie de ces possibilités.



La plupart des experts en sécurité ne s'attendent pas à voir de sitôt une attaque des 51 %. Pourquoi ? Parce que

seule la perspective de la double dépense peut inciter un hacker à vouloir posséder ces fameux 51 %. Sans bitcoins dans leur portefeuille, perpétrer une telle attaque avec succès n'offrira cependant aucun gain d'argent.

## Quelle est la probabilité d'une attaque des 51 % ?

Perpétrer une attaque des 51 % en tant que mineur ou hacker est quasiment impossible. Toutefois, ces dernières années, quelques coopératives de mineurs ne furent pas loin de posséder 50 % (ou plus) de la puissance de calcul du réseau. Suite à des accords opportuns, ces attaques ont été contrecarrées avec succès.

Ghash.io, qui fut l'une des plus importantes coopératives minières au monde ces dernières années a réuni, de manière totalement involontaire, toutes les conditions d'une attaque des 51 %. La dernière fois où [Ghash.io](https://github.com) approcha les 51 % fut en juillet 2014. Cela obligea la communauté bitcoin à entrer en discussion avec les responsables de la coopérative et de la communauté de minage afin de trouver une solution.

Des mesures temporaires furent alors prises, dont un engagement de la part de [Ghash.io](https://github.com) de ne jamais



excéder 29,99 % de la totalité du taux de hachage (c'est-à-dire la puissance de calcul totale mise au service du réseau bitcoin par les mineurs). Bien que ce pourcentage soit relativement élevé pour une seule coopérative minière, cela n'en reste pas moins une valeur tampon contre quiconque chercherait à exécuter une attaque des 51 % sur le réseau.

Ce fut la seconde fois en moins d'un an que [Ghash.io](http://Ghash.io) approcha – ou dépassa – la marque des 51 % de la puissance de calcul totale du réseau. En janvier 2014, la coopérative fut très près de posséder ces 51 % fatidiques, ce qui entraîna la suspension de nouveaux enregistrements de compte sur une assez longue période.



Au moment de la rédaction de ce livre, le réseau informatique du réseau bitcoin se répartissait sur plusieurs coopératives minières. La plus importante d'entre elles est F2pool en Chine. Elle détient 24 % du réseau, suivi par AntPoll (16 %), BTCChina (13 %), et [BW.com](http://BW.com) (10 %). Pour obtenir des informations mises à jour, consultez le site [https://en.bitcoin.it/wiki/Comparison\\_of\\_mining](https://en.bitcoin.it/wiki/Comparison_of_mining)

Toutes les coopératives minières mentionnées ci-dessus sont dirigées par des opérateurs chinois, faisant ainsi de la Chine le propriétaire de plus de la moitié de la puissance de calcul du réseau bitcoin.

Après le fiasco de 2014, [Ghash.io](#) disparut de la scène du minage du bitcoin. Fin 2014, la principale société, [CEX.io](#), décida d'interrompre ses services de cloud mining suite à la baisse du cours du bitcoin, ce qui la rendit peu rentable pour exploiter l'équipement de minage de [Ghash.io](#). Si le service de cloud mining de [CEX.io](#) redémarre dans le futur, il sera intéressant de voir si [Ghash.io](#) retrouvera aussi sa splendeur d'antan.

## Double dépense

---

Un des points les plus névralgiques du bitcoin est la possibilité pour un hacker d'effectuer une double dépense de son argent. En théorie, une double dépense peut parfaitement survenir et, je vais même vous l'avouer, elle est déjà survenue. Cependant, le facteur risque associé à un tel évènement est proche de zéro. Mais en quoi consiste réellement une attaque dite de double dépense ?

## Théorie sur l'attaque de la double dépense

Comme son nom l'indique, une attaque de la double dépense permet à un utilisateur de dépenser deux fois tout le solde de son compte. Par exemple, si une personne détient 5 bitcoins dans son portefeuille, elle

peut théoriquement en dépenser 10 suite à une double dépense. Cependant, le réseau bitcoin dispose de plusieurs règles pour éviter la double dépense, ce qui en fait alors un évènement très rare.

Chaque transaction bitcoin diffusée sur la chaîne de blocs est vérifiée par tous les nœuds individuels du réseau. Une transaction consiste en une entrée, qui est la même que la dernière sortie non utilisée associée au solde de bitcoin en question. Or, chaque sortie non utilisée ne peut être dépensée qu'une seule fois, ce qui doit rendre totalement impossible la double dépense.

## Race attaque



Les attaques de la double dépense sont très rares aujourd'hui. Mais il y a toujours des risques qu'un utilisateur en soit victime. Pour des raisons pratiques, les commerçants et les traders acceptent des paiements en bitcoins sans confirmation – ce qui ouvre grand la porte à une double dépense. En effet, les risques de la double dépense se réduisent proportionnellement au nombre de conformations requises pour valider une transaction bitcoin.

Les commerçants prennent des mesures pour se protéger contre les attaques de la double dépense. D'abord, il est conseillé de travailler avec un processeur de paiement qui négocie les risques au nom du

commerçant. La majorité des processeurs de paiement protègent le commerçant contre des dommages financiers, et cela même quand il s'agit d'une double dépense.

En outre, les commerçants et les utilisateurs privés peuvent modifier les paramètres de leur logiciel client afin de refuser les connexions entrantes et de ne se connecter qu'aux nœuds fiables du réseau. En faisant cela, vous neutralisez le risque d'une double dépense, bien que les six conformations réseau soient toujours recommandées à ce niveau.

Divers types d'attaques de double dépense peuvent être réalisées contre le réseau bitcoin. L'une d'entre elles est appelée race attaque. Elle dispose d'une fenêtre de tir tant que la transaction n'a reçu aucune confirmation sur le réseau.



L'attente des confirmations est le meilleur remède à la légitimité d'une transaction, même si ce n'est pas une option très pratique pour les commerçants.

## L'attaque de Finney

Une autre forme très répandue de la double dépense est appelée attaque de Finney. Elle nécessite la participation d'un mineur de bitcoin une fois qu'un bloc a été miné sur le réseau. Malgré les précautions

prises par le commerçant, rien ne garantit l'échec d'une attaque de Finney. Toutefois, une séquence spécifique d'évènements doit se dérouler avant que l'attaque puisse causer les dommages recherchés. Comme cette méthode est relativement coûteuse et ne peut pas survenir très souvent, elle représente une faible menace pour les commerçants et les fournisseurs de services.

Les attaques de type Finney et Race peuvent se combiner pour exécuter une attaque vector76. En théorie, ce type d'attaque permet la double dépense de bitcoins tout en ayant une confirmation réseau. Une attaque réussie coûtera un bloc au hacker – le pirate doit sacrifier un bloc en ne le diffusant pas sur le réseau, mais en le relayant sur le nœud attaqué dans l'espoir de collecter le produit/service avant que le réseau ne s'aperçoive qu'il s'agit d'une attaque. On donne également à l'attaque Vector76 le nom d'attaque à une confirmation.

## **Attaque force brutale**

Enfin, il existe l'attaque force brutale et l'attaque des 51 % (ou attaque > 50 %) qui nécessitent une grande puissance de calcul. Aucune de ces attaques n'est probable dans la mesure où le hacker devra

contrôler une quantité impressionnante de la puissance de calcul de minage.

L'attaque force brutale fonctionne de la manière suivante :

- 1. Le pirate soumet une transaction au commerçant/réseau qui paye une commande tout en minant privativement une branche (fork) dans la chaîne de blocs incluant une transaction de type double dépense.**
- 2. Après avoir attendu pour n confirmations, le commerçant envoie le produit.**
- 3. Si le hacker parvient à trouver plus que ces n blocs à ce moment précis, il casse sa branche et récupère son argent. Sinon, il peut continuer à développer ce branchement avec l'espoir qu'il soit capté sur le réseau. Si au bout du compte l'attaque échoue, le commerçant est payé comme si de rien n'était.**

Le succès de cette attaque dépend de la vitesse (fréquence de hash) du pirate et du nombre des confirmations pour le magasin/service. Par exemple, si l'attaquant possède 10 % de la puissance de calcul (fréquence de hash) du réseau bitcoin et que le marchand attende 6 confirmations, la probabilité de succès d'une telle attaque sera de 0,1 %.

Comme décrit dans la précédente section, une attaque des 51 % (ou attaque >50) ne peut réussir que si le malfaiteur contrôle plus de 50 % de la puissance de calcul du réseau bitcoin. Comme le malfaiteur peut générer les blocs dans une cadence plus soutenue que le reste du réseau, il peut créer sa propre chaîne de blocs jusqu'à ce qu'elle soit plus longue que la partie « intègre » du réseau. Aucune obligation de confirmations ne peut prévenir cette attaque.



La plus grande menace pour les commerçants et les fournisseurs de service bitcoin reste l'attaque des 51 % qui entraîne indirectement le succès d'une attaque de force brutale. Étant donné la puissance de calcul actuelle du réseau bitcoin, il semble peu probable qu'une attaque puisse être perpétrée avec succès.



Un des soucis majeurs du réseau bitcoin est l'existence d'un grand nombre de services centralisés. Presque toutes les plateformes de change et la majorité des coopératives minières de bitcoin sont des services centralisés. Si une plateforme de change est attaquée, la chaîne de blocs ne sera pas directement impactée. Mais lorsqu'une importante coopérative de mineurs est attaquée, le scénario risque de ne pas être tout à fait le même. Heureusement qu'aucune coopérative de minage ne contrôle la moitié du réseau. En effet, la plus significative d'entre elles se limite à 25 % de la

puissance de calcul totale du réseau. Mais ce pourcentage est suffisant pour perpétrer une « attaque de force brutale ».



# Chapitre 11

## Le minage de bitcoins

---

### DANS CE CHAPITRE

- » Découvrir les fondamentaux du minage
  - » Comprendre le cloud mining
  - » Décider ou non de devenir mineur
- 

Le concept de minage a révolutionné le processus de création des bitcoins jusqu'à ce que ce chiffre atteigne la limite des 21 millions à l'horizon 2140. Les bitcoins ne naissent pas par enchantement, ni du fait d'une banque ou d'un gouvernement, mais de la résolution d'équations mathématiques très complexes.



Sans les mineurs de bitcoins, aucune nouvelle unité ne verrait le jour. Cela signifie aussi qu'aucune transaction ne pourrait être confirmée sur le réseau. Cela induirait donc une grande perte d'intérêt dans l'utilisation des bitcoins.

Le minage enregistre aussi des transactions dans le livre public appelé chaîne de blocs (voir le [Chapitre 7](#) pour plus d'informations à ce sujet). En

effet, chaque transaction est enregistrée dans un bloc de données qui doit alors être découvert par des mineurs de bitcoins. Dès qu'une transaction est intégrée à un bloc, elle reçoit de facto une confirmation.

Le minage de bitcoins est devenu un processus complexe et très gourmand en ressources informatiques. Plus il y a de personnes qui concourent au minage du bloc suivant, plus le taux de difficulté associé à ces équations mathématiques augmente. De ce fait, le trafic des nouveaux blocs minés reste stable au rythme d'un bloc toutes les 10 minutes. Ainsi, il est possible de connaître l'année durant laquelle le dernier bloc sera miné.

Les frais d'électricité et les coûts d'investissement nécessaires aux opérations de minage sont substantiels. Le minage domestique est devenu quasi impossible, sauf pour ceux qui payent l'électricité à un prix super intéressant. C'est la raison pour laquelle la majorité des mineurs possèdent du matériel en Chine où l'électricité est la moins chère du monde.

## **Descendre dans la mine**

---

Pour exploiter la mine bitcoin, vous n'aurez pas besoin de lampe et de canaris.

L'objectif principal du minage est de créer un écosystème pour les nœuds bitcoin afin de déterminer (oh... jeu de mots !) si une transaction diffusée sur le réseau est ou non valide. Comme mentionné depuis le début de ce livre, au moins six confirmations sur le réseau sont requises pour valider « officiellement » une transaction.



La grande consommation énergétique du minage et de sa complexité tient à l'implémentation de l'algorithme SHA – 256 qui complexifie le calcul du hachage d'un bloc.

En plus, la difficulté du minage est recalculée par le réseau tous les 2016 blocs, et ne diminue presque jamais. Le facteur de difficulté dépend de la puissance de calcul totale qui a été utilisée pour les 2016 blocs précédents sur une période de deux semaines, et compense une hausse ou une baisse de la puissance de calcul de minage, afin d'obtenir une stabilité.

Au début du bitcoin, tout bloc miné rapportait 50 bitcoins au mineur. Mais comme le nombre de mineurs ne cessa d'augmenter, cette somme fut partagée entre les mineurs d'une coopérative minière lorsqu'elle parvenait à miner le bloc suivant. Au moment de l'écriture de ce livre, la récompense pour le minage d'un bloc est de 25 BTC, laissant supposer qu'elle tombera à 12,5 d'ici quelques années.



Les transactions bitcoin peuvent se voir appliquer des frais qui sont versés aux mineurs ayant inclus cette transaction dans le bloc miné suivant. Bien que la grande partie du revenu lié au minage consiste en une « rémunération » du bloc en cours, ces frais joueront un rôle majeur dans les futurs gains réalisés avec les opérations de minage.

Au fil des ans, l'écosystème de minage du bitcoin a connu des changements drastiques. Le minage requiert désormais un matériel dédié qui peut s'avérer rentable. Comme nous l'avons déjà indiqué, le minage consomme beaucoup d'électricité, et le matériel qui y est dédié doit être continuellement entretenu.

La fluctuation du revenu tiré du minage va conduire, tôt ou tard, les mineurs à disparaître au profit des coopératives minières. Grouper la puissance de calcul de mineurs individuels augmente les chances de découvrir le bloc suivant, et la « rétribution » est répartie en fonction de la puissance offerte par chacun des mineurs.

## Comprendre le fonctionnement du minage

---

Contrairement à la monnaie fiduciaire où la masse monétaire peut augmenter à la demande des états qui

font alors tourner la planche à billets, le bitcoin est limité dans sa quantité. En 2140, il devrait y avoir 21 millions de bitcoins en circulation, pas un de plus ni de moins. Jusqu'à cette date, les mineurs utiliseront leur matériel informatique dédié pour créer de nouveaux bitcoins sur le réseau.

Dès que des transactions sont diffusées sur le réseau, elles sont récupérées par des mineurs et « converties » en blocs. Ce bloc doit être vérifié par les mineurs. Une fois fait, toutes les transactions qu'il contient sont enregistrées dans la chaîne de blocs. Chaque bloc supplémentaire découvert sur le réseau après cette opération se voit attribuer une confirmation réseau supplémentaire.

Les mineurs de bitcoins jouent un rôle clé puisqu'ils vérifient l'intégrité des blocs du bitcoin. Ensuite, une formule mathématique complexe est appliquée à ce bloc de données, ce qui le convertit en une autre entité.



Ce bloc désormais « différent » consiste en une séquence de lettres et de chiffres aléatoires plus courte, connue sous le nom de hash. Les hash sont plus faciles à calculer qu'un bloc de données complet. En effet, les nouveaux blocs sont créés et minés toutes les dix minutes environ. Comme nous l'avons indiqué, ces hash sont informatiquement très difficiles à résoudre et exigent du matériel supplémentaire.

Une fois le hash résolu, il est stocké sur la chaîne de blocs bitcoin avec le bloc dont il est issu. Ce procédé valide toutes les transactions enregistrées dans ce bloc et indique qu'il bénéficie d'une confirmation. Bien que les hash soient plus faciles à résoudre que la totalité des blocs, la difficulté augmente avec la puissance du réseau afin de conserver le rythme de création d'un bloc toutes les dix minutes.



Utiliser des hash reste une option intéressante. Cette solution cryptographique est complètement inviolable et agit comme une preuve de confirmation du bloc précédent. Chaque hash est basé sur le hash du bloc précédent et en confirme la validité, ainsi que de tous ceux qui le précèdent.

Dans la mesure où le matériel de minage est utilisé par des particuliers, des sociétés, et même des fabricants de matériel, il est impossible d'évaluer le nombre de personnes qui participent activement au minage. Il existe une assez forte concurrence entre les mineurs qui sont récompensés de leur service à hauteur de 25 BTC par bloc.

Malgré la difficulté grandissante du minage, il y a de plus en plus de puissance informatique régulièrement mise au service du réseau bitcoin. Ce renforcement du réseau donne une chance supplémentaire aux mineurs de découvrir le bloc suivant – et de gagner des bitcoins

en fonction de la puissance de leur participation au minage – tout en renforçant la sécurité du réseau.

## Cloud mining

---

Désolé d'insister sur le fait qu'en matière de minage de bitcoin, les coûts d'électricité, de maintenance, le bruit et la chaleur des machines découragent le particulier à devenir mineur. L'idéal étant de rejoindre des centres de données. Comme cela n'est pas possible pour tout le monde, il existe des sociétés qui louent leur matériel de minage à travers un service appelé cloud mining.

Aussi intéressante que cette technologie puisse paraître, le cloud mining a ses avantages et ses inconvénients. Tout d'abord, il est important de noter que toutes les sociétés offrant ce service ne sont pas forcément légales. Diverses escroqueries ont eu lieu, sortes de pyramides à la Ponzi (pour ceux qui connaissent l'histoire de Charles Ponzi qui abusa de la crédulité de nombreuses personnes en élaborant une chaîne d'emprunt où les intérêts versés aux épargnants sont prélevés sur les sommes placées par les nouveaux souscripteurs). Cela étant dit, il existe quelques avantages dans le cloud mining si vous effectuez votre location auprès d'une société légale telle que Genesis Mining.



La rentabilité du cloud mining dépend du cours du bitcoin. Ainsi, pour la majorité des services de cloud mining, un cours du bitcoin de 320 \$ (au cours actuel du minage) est nécessaire pour dégager des bénéfices.

## Les avantages du cloud mining

Il faut de l'argent pour générer de l'argent, même en matière de bitcoin. Il est donc impossible de se lancer dans le cloud mining sans un investissement préalable. Toutefois, le cloud mining élimine certains facteurs, comme l'investissement dans un matériel de minage.



En effet, comme n'importe quel service de « nuage informatique » (oui, le cloud !), lorsque vous adhérez à un service de cloud mining, vous louez du matériel auprès d'une société. Elle achète la machine et configure le logiciel dédié à l'opération de minage. Aucun frais de transport ne vous sera facturé puisque le matériel est hébergé dans les locaux de la société de cloud mining. Ce dispositif réduit grandement les coûts d'investissement.

Votre investissement initial consistera dans la location elle-même. Elle peut se faire sur une base annuelle, voire perpétuelle. La société minera en votre nom sur la période d'engagement souscrite. Le tarif appliqué varie d'une société à une autre.



En échange, vous commencerez à miner quelques minutes après avoir terminé votre commande. Vous n'aurez aucun paramétrage à faire car, en général, le fournisseur de ce service vous relie automatiquement à une coopérative de mineurs. Les gains ne vont pas être immédiats et dépendront largement de la société de cloud mining qui souhaitera ou non obtenir rapidement un retour sur investissement.



En l'absence de frais de transport et de TVA, le cloud mining semble être un pari intéressant à prendre. Mais il faut considérer le temps qui devra s'écouler avant que vous ne profitiez de vos premiers revenus. Cela dépend en effet de plusieurs facteurs : le cours du bitcoin, la difficulté du minage qui change tous les 2016 blocs, et la puissance de calcul ciblée par le réseau bitcoin.

## Les inconvénients du cloud mining

Il est rare que les avantages procurés par un service ne soient pas modérés par quelques inconvénients. C'est le cas en matière de cloud mining.



En tant que client, vous n'aurez aucun contrôle sur le matériel loué, car vous ne pouvez pas y accéder physiquement ou à distance. Vous dépendez

entièrement d'un fournisseur de service tierce partie centralisé. C'est donc ici que commencent la majorité des problèmes liés au cloud mining, lorsque les clients ne se sentent pas rémunérés correctement. Plusieurs raisons expliquent la faiblesse de la rémunération : des coûts de maintenance inattendus, l'augmentation du prix du service, la variation du coût de l'électricité, et celle du cours du bitcoin.

Une fois encore, il n'y a aucun moyen de comprendre pourquoi les gains sont si réduits pendant une certaine période. Le client est donc, dans un certain sens, otage du fournisseur de ce service. C'est ce que cherche à changer le bitcoin en donnant à chaque utilisateur individuel un contrôle total, et cela à tout moment.

Un autre inconvénient du cloud mining tient aux frais d'électricité et de maintenance. En effet, comme ces coûts sont pris en charge par l'opérateur de cloud mining, il les répercute sur votre location. Dans certaines parties du monde, comme en Chine, l'électricité est relativement bon marché, ce qui réduit considérablement les coûts de fonctionnement du dispositif.



Une des plus grosses erreurs est de croire qu'avec le cloud mining, vous achetez une certaine quantité de puissance de calcul qui vous rapportera la totalité des gains qu'elle produit dans ce système. Ce n'est jamais

le cas puisque le montant des frais d'électricité et de maintenance qui vous incombe est calculé sur ladite puissance de calcul que vous « louez » auprès de ce fournisseur de service.

Le cloud mining reste profitable pour des investisseurs intelligents qui auront effectué des recherches et des calculs préalables. Ne vous basez jamais sur les projections faites par l'opérateur de cloud mining, car trop d'éléments en feront varier les résultats. De plus, il y a peu de sociétés de cloud mining qui effectuent des calculs très prudents. De ce fait, on vous fait miroiter des gains qui seront très éloignés de la réalité. Il y a donc de la déception dans l'air.

## Les risques liés au cloud mining



Le plus grand risque associé au cloud mining est le service fourni par une société illégale. Bien qu'elle détaille ses activités, rien ne vous en prouve la véracité.

Ajoutez à cela que, à chaque fois qu'une société de cloud mining est piratée – ce qui arrive assez fréquemment – les gains du client s'en trouvent tout aussi affectés. Les fonds de l'utilisateur disparaissent, et le fournisseur se voit obligé de réduire les gains du minage pendant une longue période, le temps de récupérer les pertes.



Une des sociétés de cloud mining les plus réputées est Genesis Mining ([www.genesis-mining.com](http://www.genesis-mining.com)). Située à Hong Kong, elle a lancé son service de cloud mining en 2013, et offre des contrats perpétuels à des prix tout à fait intéressants. Contrairement à la plupart des autres sociétés, aucun frais supplémentaire ou caché n'est appliqué lorsque vous souscrivez un contrat de cloud mining auprès de Genesis Mining. De ce fait, ce service est l'un des préférés des mineurs.



Si vous souscrivez un contrat de cloud mining, n'oubliez jamais que ce domaine d'activité est en constante évolution et que des propositions plus alléchantes les unes que les autres ne cessent de voir le jour. Donc, avant de vous décider, vérifiez les différentes offres afin de choisir le service qui regroupe plus d'avantages que d'inconvénients. Ne vous laissez pas influencer par des offres qui paraissent vraiment trop belles pour être honnêtes.

## Sécuriser le bitcoin grâce au minage

---

Le niveau de sécurité du bitcoin augmente en fonction du nombre de personnes qui utilisent un nœud bitcoin et/ou de la puissance de calcul de la procédure de minage.



Comme discuté au [Chapitre 10](#), une des plus grandes menaces à laquelle le bitcoin est exposé s'appelle l'attaque des 51 %. Plus le processus de minage dispose de puissance de calcul, plus les risques de voir des individus ou des coopératives minières posséder plus de 50 % de la puissance du réseau sont réduits.

Pour un mineur, le gain d'argent est la raison principale qui le pousse à dédier un matériel puissant au minage. Cependant, il existe des mineurs qui accomplissent cette tâche pour renforcer la sécurité du réseau bitcoin, ne voyant dans le gain d'argent qu'un effet transversal de leur participation. En fonction du côté de la barrière où l'on se place, le minage sécurise le réseau en confirmant des transactions et en développant la chaîne de blocs.

Le minage protège aussi la neutralité du réseau en empêchant une personne ou une coopérative minière de disposer d'une puissance suffisante pour bloquer d'autres transactions. Comme l'explique le [Chapitre 10](#), quiconque parviendrait à obtenir cette puissance pourrait confirmer ses propres blocs et laisser tous les autres sans aucune confirmation pendant une période indéfinie.



Le minage de bitcoins augmente, pour un individu ou une coopérative de mineurs, la difficulté d'inverser une transaction précédente, car tous les blocs qui suivent

cette transaction auront besoin d'être réécrits. Plus le temps passe et plus les blocs du réseau obtiennent des confirmations supplémentaires, ce qui est crucial pour permettre à la chaîne de blocs de générer des nouveaux blocs environ toutes les dix minutes.

Au fil du temps, le minage de bitcoins devient de plus en plus gourmand en ressources matérielles. Chaque bloc individuel trouvé sur le réseau exige un certain nombre d'interventions pour être considéré comme validé, état qui est ensuite vérifié par tous les nœuds bitcoin du réseau. Une fois que ces nœuds ont la preuve de la validité du bloc, de nouvelles unités seront disséminées de manière décentralisée, motivant ainsi les mineurs à consacrer des ressources au réseau bitcoin. Plus il y a de ressources et plus le niveau de sécurité est élevé. Ce cycle ne cesse de se répéter en boucle.

## **Lancer votre minage**

---

Il est plus difficile aujourd'hui d'entrer dans la danse du minage. Le matériel de minage a évolué ces dernières années à une cadence accélérée afin de répondre aux besoins de puissance des calculs complexes nécessaires à la résolution des blocs. Mais il existe encore des opportunités pour s'engager dans le minage en supposant que vous disposiez de ressources

substantielles et que vous effectuiez quelques calculs préalables.

## Utiliser le bon matériel

Lorsque le bitcoin fut créé en 2009, le processus de minage était fort simple. L'utilisateur devait simplement installer le logiciel client, le synchroniser avec le réseau, et vérifier que l'option de minage était bien activée. N'importe quel type de CPU (processeur) – même d'ordinateurs portables – pouvait miner des bitcoins, car il n'y avait aucune concurrence sur le réseau. En réalité, durant les premières semaines, on pouvait compter les mineurs sur les dix doigts de la main (ou presque).

Il ne fallut pas attendre longtemps pour que l'enthousiasme autour du bitcoin amène les développeurs à modifier le code afin que les cartes graphiques (GPU) prennent en charge les calculs. Même si elle est conçue pour des jeux vidéo, une carte graphique est capable de réaliser des calculs de données intensifs à une cadence élevée.



La différence entre la vitesse de minage d'un CPU et d'un GPU est tout bonnement astronomique. La productivité augmente de manière exponentielle, et les premiers GPU qui se lancèrent dans cette opération

décuplèrent la puissance du réseau. Malgré cette puissance accrue, les nouveaux blocs ne continuèrent à apparaître que toutes les dix minutes, à cause de la progression du niveau de difficulté du minage.

Il y a quelques années, le minage par CPU et GPU est devenu obsolète face à l'arrivée des FPGA. Un FPGA (Field Programmable Gate Array) est un circuit intégré reprogrammable, capable de produire une puissance de calcul similaire à celle des GPU de 2013, et cela en consommant moins d'énergie que les cartes graphiques. Mais, peu de mineurs passèrent rapidement du CPU au GPU puis au FPGA.

Toutefois, le commerce matériel du minage poursuivit son évolution, et les FPGA ne furent utilisés que sur une courte période. En effet, les ASIC apparurent en 2013, abaissant encore plus la consommation électrique et dépassant sensiblement en performance les GPU et les FPGA.

Cela dit, il existe des inconvénients liés au minage avec un ASIC. Bien que la consommation soit sensiblement inférieure à celle des cartes graphiques, le bruit est en revanche très important. De plus, les mineurs ASIC dégagent énormément de chaleur et ont besoin d'être ventilés, car la température peut dépasser les 65 degrés.



Acheter un mineur ASIC engendre des frais de transport – ces machines sont assez lourdes. Ajoutez à ces frais des taxes d'importation. Tout bien considéré, aujourd'hui les ASIC représentent un investissement coûteux sans jamais être certain de réaliser des profits suffisants pour rentrer dans ses frais.

Enfin, les ASIC peuvent produire de la puissance de calcul tant qu'ils ne se heurtent pas à une certaine limite. La plupart des périphériques ne sont pas capables de produire plus 1,5 TH/s (terrahash) de puissance de calcul, forçant les clients à acheter ces machines en nombre s'ils veulent démarrer une activité sérieuse de minage.



Il n'est pas surprenant de découvrir que la plupart des gens ont abandonné l'aspect matériel personnel du minage de bitcoin pour s'orienter vers le cloud mining (même s'il y a des risques associés aux sociétés de cloud mining du bitcoin). Et le faible prix du bitcoin n'aide pas dans ce domaine. Voyez la précédente section sur le cloud mining consacré aux mesures à prendre pour vous protéger.

## Calculer vos frais

Que vous décidiez d'investir dans du matériel ou d'opter pour un contrat de cloud mining, vous devrez

déterminer les coûts, les gains, et le temps au bout duquel vous aurez rentabilisé votre investissement initial.



Le coût du minage ne s'arrête pas à l'achat de matériel, aux frais logistiques, et aux taxes d'importation. Un des principaux pôles de dépense concerne le prix du kilowattheure (kWh) d'électricité qui fluctue d'un pays à un autre.



Dans bien des pays, ce prix est si prohibitif que le minage du bitcoin ne rapportera absolument rien. Prenez votre dernière facture d'électricité, et calculez le prix du kWh (ce prix est souvent indiqué sur la facture), puis celui de la consommation quotidienne de votre matériel de minage.

Par exemple, un mineur de bitcoins de 600 watts consommera 12,4 kWh par jour. En effet,  $600 \text{ W} \times 24 \text{ heures/jour} = 14\,400 \text{ Wh}$  soit 12,4 kWh. Si le prix du kilowatt est de 0,14490 €, votre consommation journalière sera de 1,79 €.



Ce coût doit être ramené au revenu quotidien de votre activité de minage. Ces gains dépendront principalement du cours du bitcoin. Mais l'électricité n'est pas le seul secteur de dépenses. En tant que propriétaire du matériel de minage, vous aurez en charge son entretien et ses réparations. Certains

mineurs ASIC sont livrés sans alimentation. Vous êtes alors obligé de rajouter cet achat à la note.

Mais l'investissement le plus élevé concerne le temps que vous passerez et les efforts que vous consentirez pour optimiser vos gains. La majorité des matériels de minage fonctionneront au meilleur de leurs capacités. Toutefois, des réglages peuvent toujours être faits. Il n'est pas rare que des constructeurs réalisent périodiquement une nouvelle version de leur firmware afin de corriger des bogues.

## UTILISER UN CALCULATEUR DE RENTABILITÉ

Il n'est pas nécessaire d'être calé en mathématique pour calculer les coûts et les gains potentiels du minage. Plusieurs sites Web sont spécialisés dans ce type de calcul. Vous saisissez diverses informations matérielles et les coûts de l'électricité.

Ne négligez pas ces sites Web de calcul de la rentabilité du minage. Ils vous donneront une estimation quotidienne et future de cette opération. Le facteur de difficulté du minage s'ajuste tous les 2016 blocs, affectant ainsi vos gains de minage. Lorsque la difficulté augmente, les gains diminuent lentement. En revanche, vos gains augmentent quand cette difficulté diminue.

Pour trouver une liste des calculateurs de rentabilité, consultez la page

[http://didaquest.org/wiki/Bitcoin#Calculateur Bitcoin](http://didaquest.org/wiki/Bitcoin#Calculateur_Bitcoin)

# Les dix commandements

## DANS CETTE PARTIE

- » Dix façons d'utiliser des bitcoins
- » Trouver d'autres monnaies alternatives
- » Découvrir dix ressources en ligne consacrées au bitcoin

## Chapitre 12

# Dix façons d'utiliser des bitcoins

---

### DANS CE CHAPITRE

- » Découvrir les investissements possibles
  - » Explorer le potentiel pédagogique exponentiel
  - » Dépenser des bitcoins !
- 

Le bitcoin peut être utilisé de différentes manières. La seule limite tient à l'adoption, par les commerçants, de ce moyen de paiement. Plus la popularité du bitcoin gagnera le grand public et les commerçants, plus vous pourrez acheter de choses avec cette crypto-monnaie. Génial !

Que vous utilisiez le bitcoin comme une forme de monnaie virtuelle pédagogique, de revenu supplémentaire, ou d'investissement, le bitcoin permet de faire tout ce que vous pouvez imaginer. Ce chapitre suggère dix façons d'utiliser le bitcoin, bien qu'il y ait beaucoup, beaucoup, beaucoup d'options à votre disposition.

## Utiliser le bitcoin comme véhicule d'investissement

---

La plupart des gens voient dans le bitcoin un investissement. Avec une capacité totale de 21 millions de bitcoins à l'horizon 2140, et le cours assez faible, il y a de réelles opportunités de réaliser des plus-values en jouant sur la volatilité de cette crypto-monnaie.



« Boursicoter » avec le prix du marché du bitcoin est très tentant. Toutefois, n'oubliez pas qu'à ce petit jeu les pertes surviennent bien plus souvent que les gains.

D'autres utilisations du bitcoin en tant que véhicule d'investissement existent. Investir dans le bitcoin est une opération qui s'apprécie sur le long terme, afin d'équilibrer les phases de pertes et de profits. Le bitcoin est une monnaie relativement jeune avec ses six années d'existence. Il y a donc encore beaucoup de chemin à faire avant de parvenir à convaincre les gens que le bitcoin ne se limite pas à un véhicule d'investissement susceptible de rapporter de l'argent en jouant sur ses fluctuations.

## Utiliser le bitcoin comme outil pédagogique

---

L'objectif principal du bitcoin est d'informer tout un chacun sur le potentiel de la chaîne de blocs et sur la possibilité offerte aux utilisateurs de prendre le contrôle de leur vie. Cela va bien au-delà d'un simple aspect financier. Mais le bitcoin concerne aussi l'utilisation des services qui lui sont associés, des plateformes de change, de sa technologie et, plus important encore, sur la manière que nous avons de percevoir le monde.

Quoi que vous regardiez dans la vie, vous ne verrez que fraude, corruption, défaut de gestion, restrictions financières, liberté d'expression muselée, et bien d'autres aberrations. Lorsque Satoshi Nakamoto créa le bitcoin, l'idée ne fut pas de mettre en place une nouvelle race de technologie marginale, mais de démontrer qu'il pouvait exister des solutions décentralisées pour améliorer la vie de chacun.



Aujourd'hui, beaucoup de personnes n'apprécient que l'aspect financier de cette technologie. Il existe pourtant un vaste espace d'amélioration de ce marché, et le bitcoin est un outil pédagogique très plaisant à employer pour expliquer ce que nous pouvons changer dans le système financier actuel.

Mais le processus pédagogique du bitcoin va encore plus loin que ces aspects financiers et technologiques. Le potentiel de la chaîne de blocs et du bitcoin 2.0 est

bien plus étendu, comme vous pouvez le lire au [Chapitre 7](#). Une fois que vous aurez compris la fonction du bitcoin et de sa chaîne de blocs, amis lecteurs, vous pourrez en mesurer librement le potentiel dans tous les aspects de la vie quotidienne. Réfléchissez un instant, par exemple, sur le nombre de consensus qui pourraient être obtenus sans faire entrer dans cette équation l'élément humain. Le vote électronique, la négociation et la modification des contrats, la signature et le stockage de documents, et la refonte des transactions peer-to-peer ne sont que quelques exemples parmi d'autres.

## Dépenser des bitcoins pour vos besoins quotidiens

---

Beaucoup de personnes sont attirées par le bitcoin, car il représente un moyen de paiement électronique. Ces dernières années, de plus en plus de lieux l'ont accepté du fait de ses coûts réduits, de l'instantanéité des transactions, de l'absence de fraude ou de rétrofacturation.

Il en résulte que le bitcoin est devenu une forme viable de paiement, aussi bien en ligne qu'en boutique, et cela dans le monde entier. L'écosystème du bitcoin est principalement utilisé pour envoyer des fonds aux



quatre coins de notre planète, démontrant ainsi que le commerce est un facteur essentiel dans la survie de l'écosystème.



Face au nombre de commerçants en tout genre qui existent pour tout type de produits et de services, le bitcoin commence à s'implanter comme un véritable moyen de paiement.

Une option intéressante pour dépenser des bitcoins réside dans des services et des sociétés qui livrent de la nourriture à domicile. Vous êtes un fan de Starbuck ? Pourquoi ne pas payer votre prochain café en bitcoins ? Les possibilités sont infinies.

Une recherche rapide sur Internet vous montera les différentes manières de dépenser votre monnaie électronique, et cela dans des secteurs que vous n'imaginiez même pas. Utilisez les mots-clés suivants :

- » Dépenser ses bitcoins
- » Utiliser ses bitcoins
- » Payer avec des bitcoins
- » Nous acceptons les bitcoins

## Vos loisirs en bitcoins

---

Le bitcoin est géré de manière à attirer des gens appartenant à des niveaux sociaux très différents.

Ainsi, le bitcoin pourra être utilisé pour couvrir des dépenses moins quotidiennes comme des réservations de vols et d'hôtels. Bien que tous les vols et hôtels ne puissent pas être réglés en bitcoins, de nombreux services restent à votre disposition pour faciliter cette procédure, comme BTCtrip (<https://btctrip.com>).

Ces sociétés ont observé un fait intéressant : les clients qui paient en bitcoins ont tendance à dépenser plus pour leurs vols et leurs hôtels. La raison précise de ce comportement demeure inconnue, mais cela démontre aux commerçants tous les bénéfices qu'ils peuvent tirer de l'acceptation de ce moyen de paiement.

## Œuvres caritatives en bitcoins

Un des aspects les plus importants de notre vie est de pouvoir aider tous ceux qui sont dans le besoin. Les dons réalisés en bitcoins peuvent être envoyés à diverses associations caritatives, dont la Croix rouge et Greenpeace. Ces dons peuvent être déduits des impôts, même s'ils sont effectués en bitcoins.

Le plus grand avantage du bitcoin dans ce domaine est de pouvoir envoyer directement des fonds à des personnes nécessiteuses, plutôt que de passer par une association. Au moment du tremblement de terre au Népal, beaucoup d'utilisateurs du bitcoin envoyèrent

des dons directement au Nepal Relief Fund. De ce fait, l'argent fut affecté plus rapidement, et les utilisateurs du bitcoin purent aider de nombreuses personnes sinistrées dans cette région.

## Jouer en ligne

En fonction de votre lieu de résidence, le jeu et les paris en ligne sont peut-être illégaux. Par conséquent, vérifiez cet état de fait auprès des administrations locales.

Si le jeu en ligne est autorisé dans votre pays, sachez que le bitcoin représente un moyen de paiement alternatif aux cartes bancaires et aux virements. Aucun détail n'est requis, et aucune vérification de documents n'est exigée. Vous déposez vos fonds et vous jouez ! Les transferts de bitcoins sont rapides et non remboursables, ce qui en fait un moyen de paiement idéal pour les fournisseurs de ces services en ligne tels que les casinos.



Attention ! Le jeu peut isoler, rendre dépressif et agressif. Agissez toujours en personne responsable, en « bon père de famille » comme le veut cet adage du droit français.

## Investir dans des métaux

## précieux : l'étalon-or réinventé

Bien qu'il s'agisse ici encore d'entrevoir le bitcoin comme véhicule d'investissement, peu de personnes pensent à l'utiliser pour acheter des métaux précieux, comme de l'or ou de l'argent.

Il existe de nombreuses plateformes en ligne qui permettent aux utilisateurs d'échanger des bitcoins contre des métaux précieux, comme dans une sorte de cotation boursière. Certaines ont connu une belle réussite au fil des ans. Effectuez toujours des recherches personnelles avant d'accorder votre confiance à n'importe quelle plateforme.



Vaultoro ([www.vaultoro.com](http://www.vaultoro.com)) est la plus populaire des plateformes en ligne au moment où nous écrivons ces lignes. Elle se focalise principalement sur l'or et le bitcoin. Penchez-vous également sur MidasRezerv (<https://midasrezerv.com>), Uphold (<https://uphold.com>), et BitGold (<https://bitgold.com>). Agissez toujours de manière avisée en vous basant sur la notoriété de ces sociétés avant d'investir.

## Le plaisir d'offrir des bitcoins

Le bitcoin est un cadeau idéal pour vos amis, votre famille, et toutes les personnes que vous aimez.



Plusieurs sites proposent des cartes-cadeaux en échange de bitcoins comme La maison du bitcoin (<https://lamaisondubitcoin.fr/cartes-cadeaux-bitit/>) et Bit4coin (<https://bit4coin.net/fr/bitcoins-carte-cadeau>). La carte-cadeau bitcoin est utilisable dans de nombreux magasins qui n'acceptent pourtant pas d'être directement payés en bitcoins. Mais, par l'intermédiaire de la puissance magique des cartes-cadeaux, le bitcoin peut être utilisé ou offert comme moyen de paiement.

## Payer vos factures

L'option consistant à payer ses factures en bitcoins dépend de votre lieu de résidence. Cela dit, il existe de multiples plateformes en développement qui permettent de payer vos factures en bitcoins contre une petite commission.



Les factures téléphoniques, de services, et les remboursements de prêts pourront être payés en bitcoins dans un futur proche. Certains opérateurs de téléphonie mobile étrangers acceptent d'être réglés en bitcoins. Parions que cela ne devrait pas tarder à se

démocratiser en France.

## Utiliser le bitcoin comme expérience sociale

---

Imaginons que vous soyez passionné par le bitcoin, mais que vous soyez découragé par son exploitation encore trop restreinte. Dans ce cas, pourquoi ne pas essayer de convaincre des commerçants et des consommateurs des avantages du bitcoins ? En effet, l'expansion pas à pas de cet écosystème demande du temps et requiert des efforts. Comme il n'existe pas d'autorité centrale pour prendre en charge ce travail, il incombe donc aux membres de la communauté bitcoin.

Tout cela n'est qu'une partie des possibilités du bitcoin que vous pouvez enrichir avec votre créativité afin d'utiliser cette crypto-monnaie comme personne ne l'avait encore imaginé. Chaque fois que vous avez la possibilité d'utiliser des bitcoins, partagez votre expérience avec cette communauté.

## Chapitre 13

# Dix (ou presque) autres crypto-monnaies

---

### DANS CE CHAPITRE

- » Échanges entre crypto-monnaies
  - » Un coup d'œil sur la communauté
  - » Jeu et financement participatif
- 

L'univers de la monnaie électronique grouille de développeurs impatients qui pensent pouvoir créer « le nouveau bitcoin ». Au fil des ans, un millier d'altcoins ont vu le jour, mais la plupart ont disparu aussi vite qu'elles sont apparues, car elles n'avaient pas d'autres buts que de réaliser des plus-values. Il existe cependant quelques altcoins, parallèlement au bitcoin, qui revêtent une certaine importance, même si elles n'ont pas vocation à détrôner le bitcoin.

Ce chapitre présente huit monnaies électroniques. (Pour arriver à dix comme le veut cette traditionnelle partie des livres pour les nuls, il faudrait ajouter deux fois le bitcoin, car nous pensons que deux valent mieux

qu'un. Comment ? C'est un peu tiré par les cheveux ?  
OK, je vous l'accorde !)

## Litecoin : est à l'argent ce que le bitcoin est à l'or

---

L'altcoin le plus répandu est probablement le litecoin (<https://litecoin.org/fr/>). Il utilise un algorithme (Script) totalement différent de celui du bitcoin (SHA-256). Le litecoin fut la première monnaie alternative à utiliser l'algorithme Script. Il donna aux mineurs de bitcoins un argument pour reconverter leurs GPU dépassés et tirer des revenus en minant des litecoins.

Le litecoin a réussi à rester utile pendant une longue période de temps, car il fut le premier à proposer quelque chose de nouveau. Cette idéologie initiale conduisit à la création d'une communauté significative qui resta loyale et fidèle au fil des ans.



Le seul avantage supplémentaire du litecoin, à côté de l'utilisation des GPU pour son minage, est de réduire à cinq minutes le temps séparant la création de deux blocs, contre dix minutes pour le bitcoin.

La plus grande part du succès du litecoin revient aux plateformes de change qui listent les pairs d'échange de litecoins, créant ainsi des marchés secondaires. En réalité, le litecoin peut être échangé sur la majorité des



plateformes de crypto-monnaies existantes aujourd'hui, même si seulement quelques-unes proposent d'échanger les litecoins contre une monnaie locale. Divers processeurs de paiement ont ajouté le litecoin à leur liste des monnaies, offrant ainsi la possibilité de dépenser des LTC quasiment partout où le bitcoin est accepté.

La majorité des altcoins sont basés sur l'algorithme Scrypt du litecoin.

## Dogecoin : impressionnant, fun, et surprenant

---

Le dogecoin (<http://dogecoin.com>) a été lancé comme une farce sans réel soutien, et en utilisant grossièrement l'algorithme Scrypt du litecoin. Personne n'aurait pu imaginer qu'il devienne une des principales crypto-monnaies.

Cette troisième plus grande communauté de crypto-monnaie au monde pourrait tout à fait vous séduire. Dogecoin se targue d'être une crypto-monnaie communautaire, s'obligeant ainsi à recueillir des fonds pour de bonnes causes.

\$5 Grâce au dogecoin, l'équipe de bobsleigh de la Jamaïque a pu participer aux Jeux olympiques d'hiver de Sochi en 2014, et Josh Wise, avec son numéro 98, fut

sponsorisé par la communauté du dogecoin lors de la course de NASCAR se déroulant sur le Talladega Superspeedway en mai 2014.

## Dash : plus connu sous le nom de darkcoin

---

Tout au long de ce livre, vous avez pu constater que le sujet de l'anonymat revenait fréquemment dans l'appréciation de la crypto-monnaie. Nous avons montré que le bitcoin n'offrait pas un anonymat absolu, mais plutôt un pseudonymat qui permet aux utilisateurs de masquer leur identité dans une adresse de portefeuille. Cette absence d'anonymat a permis aux différents développeurs d'altcoins de proposer des solutions potentielles à ce problème, et de développer des fonctions qui seront ou non intégrées dans les futures versions des logiciels de bitcoin.

Darkcoin, ou Dash (<http://dash.org/fr/>) est l'un des principaux pionniers en matière de développement de fonctionnalités sur l'anonymat. Evan Duffield, le principal développeur de Dash, a proposé plusieurs solutions créatives pour créer des transactions totalement autonomes et anonymes sur le réseau Dash. Dash apparaît comme l'un des altcoins anonymes les plus populaires.

# Ripple : une crypto-monnaie atypique

---

La quasi-totalité des crypto-monnaies que vous rencontrerez développent l'idéologie d'une existence décentralisée. Ripple (<https://Ripple.com>) est légèrement différente, car elle a été créée et développée par Ripple Labs. Basée sur le marché de la capitalisation, Ripple est l'une des plus importantes crypto-monnaies du moment.

Ripple commence à attirer l'attention des médias. Son protocole a été mis en place par Fidor Bank et d'autres réseaux de paiement en tant que technologie d'infrastructure de règlement. Selon certaines banques, la technologie Ripple des livres comptables distribués présente plusieurs avantages par rapport à la technologie de la chaîne de blocs du bitcoin, notamment en matière de sécurité et de prix.

# Peercoin : introduction de la preuve de travail

---

Le bitcoin et le litecoin ont une chose en commun : les nouvelles unités ne peuvent être générées que par un processus de minage. Peercoin (<https://peercoin.net>) fut l'un des premiers

« clones bitcoin » à offrir un nouveau système de génération d'argent, appelé preuve de travail allié à une preuve d'enjeu. Ainsi, l'extraction (ou minage) par la preuve de travail est utilisée pour distribuer de nouvelles unités de la crypto-monnaie (ou pièces), alors que la sécurité du réseau est assurée par la preuve de part. Ainsi, les soucis liés à la sécurité du minage du bitcoin n'ont aucun impact sur la sécurité du peercoin.

Le fonctionnement de ce dispositif repose sur la quantité d'argent qui reste sur un porte-monnaie sans être dépensé. Une fois que cet argent atteint un certain âge – c'est-à-dire l'écoulement d'une durée de temps au terme de laquelle les peercoins n'ont pas été utilisés – il génère des intérêts. Globalement, ce principe ressemble à celui des comptes courants rémunérateurs. La différence est qu'en matière de peercoin, le système reste totalement décentralisé avec des utilisateurs qui gardent en permanence le contrôle de leurs fonds.



En permettant ainsi la création de peercoins via la preuve de travail et la preuve d'enjeu, le système instaure une couche supplémentaire de stabilité du réseau, au cas où le nombre de mineurs viendrait à décliner. En outre, les développeurs ont défini un taux d'inflation fixe de 1 % par an sans limites strictes de « pièces » disponibles.

## StartCOIN : crowdfunding

---

StartCOIN concerne le financement participatif ou crowdfunding. Cette monnaie récompense les utilisateurs qui s'engagent, partagent, et détiennent des StartCOIN sur un site Web dédié appelé StartJOIN (<https://v2.startjoin.com/>).

Le financement participatif gagne en popularité, et StartCOIN présente l'avantage de permettre aux communautés de financer des idées, des concepts, et des projets. Ceux qui promettent de financer ou qui profitent d'un financement via le site Web sont récompensés en StartCOIN.

## NXT : utiliser la preuve d'enjeu pour le consensus sur les transactions

---

Le minage du bitcoin repose sur l'idée d'un consensus distribué qui valide des transactions. NXT (<http://nxt.org>) utilise la preuve d'enjeu pour obtenir ce consensus. De plus, NXT est l'une des rares crypto-monnaies qui n'a pas de processus de minage – toutes les unités de la monnaie ayant été distribuées lors de sa création. Avec un flux aussi fixe, disponible

en permanence, NXT a créé un nouvel écosystème dans le monde de la crypto-monnaie.



Le véritable intérêt de NXT est que tout utilisateur peut créer sa propre crypto-monnaie à l'intérieur de cet écosystème. Ainsi, toutes les pièces nouvellement créées sont soutenues par la monnaie NXT et peuvent être distribuées de différentes manières.

Récemment, NXT a introduit progressivement de nouvelles fonctions, comme les contrats intelligents, un service de messagerie d'arbitrage, et une plateforme de change peer-to-peer décentralisée appelée MultiGateWay.

## CasinoCoin : pour les joueurs

Voici une monnaie qui démontre l'avantage que l'on peut tirer d'un nom significatif. En effet, CasinoCoin (<http://casinocoin.org>) laisse logiquement penser que cette crypto-monnaie est dédiée au marché du casino.

CasinoCoin emploie la même technologie que le litecoin (l'algorithme Scrypt), mais en utilisant un nom clairement identifié par tout un chacun dans le monde entier ; il permet au public de comprendre immédiatement la filiation qui existe entre cette monnaie et le jeu.

# **Sommaire**

[Couverture](#)

[Bitcoin pour les Nuls poche](#)

[Copyright](#)

[Introduction](#)

[À propos de ce livre](#)

[Nos présomptions](#)

[Les icônes utilisées dans ce livre](#)

[Et maintenant ?](#)

[I. Les fondamentaux du bitcoin](#)

[Chapitre 1. Présentation du bitcoin](#)

[L'origine du bitcoin](#)

[Un peu de technique](#)

[Le fonctionnement des bitcoins](#)

[Utilisation anonyme des bitcoins](#)

[Croire dans le bitcoin](#)

[Chapitre 2. Acheter et stocker des bitcoins](#)

[Bien commencer : Comment acquérir des bitcoins](#)

[Stocker vos bitcoins : sécuriser les échanges](#)

[Crypter vos bitcoins](#)

[Acheter des bitcoins en personne](#)

[Hot wallets et stockage à froid](#)

## [Chapitre 3. Bitcoin : les pour et les contre](#)

[Les pour du bitcoin](#)

[Les inconvénients du bitcoin](#)

## [Chapitre 4. Créer de l'argent avec le bitcoin](#)

[Le minage des bitcoins](#)

[Échanger des bitcoins](#)

[Bitcoin et financement participatif](#)

[Maintenir les bitcoins pour l'avenir](#)

[Acquérir des bitcoins](#)

## [II. Gérer des bitcoins](#)

### [Chapitre 5. Votre portefeuille de bitcoins](#)

[Déverrouiller les clés publiques et privées](#)

[Garder la main sur un portefeuille de bitcoins](#)

[Paramétrer une adresse bitcoin](#)

[La sécurité de votre portefeuille](#)

### [Chapitre 6. Les transactions bitcoin](#)



[Les principes des transactions](#)

[Recevoir des confirmations](#)

[Calculer les frais](#)

[Examiner la vitesse des transactions](#)

[Comprendre les frais de minage](#)

[Gérer les transactions multisignatures](#)

## [Chapitre 7. La chaîne de blocs](#)

[Comprendre l'analyse de la chaîne de blocs](#)

[Au-delà des transactions](#)

[Travailler avec des applications de la chaîne de blocs](#)

[En route pour le Bitcoin 2.0](#)

## [III. Bitcoins et activités commerciales](#)

### [Chapitre 8. Utilisation commerciale du bitcoin](#)

[Vendre des marchandises contre des bitcoins](#)

[Les solutions de paiement en bitcoins](#)

[Accepter les bitcoins dans votre boutique](#)

### [Chapitre 9. Rester du bon côté de la loi](#)

[Bitcoin et fiscalité](#)

[La réglementation du bitcoin à travers le monde](#)

### [Chapitre 10. Bitcoin et sécurité](#)

[Le réseau bitcoin : Une présentation de son fonctionnement](#)

[Protéger le bitcoin contre les hackers](#)

[Surveiller l'attaque des 51 %](#)

[Double dépense](#)

## [Chapitre 11. Le minage de bitcoins](#)

[Descendre dans la mine](#)

[Comprendre le fonctionnement du minage](#)

[Cloud mining](#)

[Sécuriser le bitcoin grâce au minage](#)

[Lancer votre minage](#)

## [IV. Les dix commandements](#)

### [Chapitre 12. Dix façons d'utiliser des bitcoins](#)

[Utiliser le bitcoin comme véhicule d'investissement](#)

[Utiliser le bitcoin comme outil pédagogique](#)

[Dépenser des bitcoins pour vos besoins quotidiens](#)

[Vos loisirs en bitcoins](#)

[Œuvres caritatives en bitcoins](#)

[Jouer en ligne](#)

[Investir dans des métaux précieux : l'étalon-or réinventé](#)

[Le plaisir d'offrir des bitcoins](#)

[Payer vos factures](#)

[Utiliser le bitcoin comme expérience sociale](#)

## Chapitre 13. Dix (ou presque) autres crypto-monnaies

Litecoin : est à l'argent ce que le bitcoin est à l'or

Dogecoin : impressionnant, fun, et surprenant

Dash : plus connu sous le nom de darkcoin

Ripple : une crypto-monnaie atypique

Peercoin : introduction de la preuve de travail

StartCOIN : crowdfunding

NXT : utiliser la preuve d'enjeu pour le consensus sur les transactions

CasinoCoin : pour les joueurs