Introduction

2022-03-04

# Introduction

## Qu'est-ce que Bitcoin ?

Bitcoin est un ensemble de concepts et de technologies qui constituent la base d'un écosystème de monnaie numérique. Les unités monétaires appelées bitcoin sont utilisées pour stocker et transmettre de la valeur entre les participants au réseau Bitcoin. Les utilisateurs de Bitcoin communiquent entre eux en utilisant le protocole Bitcoin principalement via Internet, bien que d'autres réseaux de transport puissent également être utilisés. La pile de protocole Bitcoin, disponible en tant que logiciel à source libre, peut être exécutée sur une large gamme d'appareils informatiques, y compris les ordinateurs portables et les smartphones, ce qui rend la technologie facilement accessible.

Remarquez comment l'unité monétaire s'appelle "bitcoin" avec un petit *b*, et le système s'appelle "Bitcoin", avec un *B* majuscule.

Les utilisateurs peuvent transférer des bitcoins sur le réseau pour faire à peu près tout ce qui peut être fait avec des devises conventionnelles, y compris acheter et vendre des biens, envoyer de l'argent à des personnes ou à des organisations ou accorder un crédit. Le bitcoin peut être acheté, vendu et échangé contre d'autres devises dans des bureaux de change spécialisés. Le bitcoin est en un sens la forme d'argent idéale pour Internet car il est rapide, sécurisé et sans frontières.

Contrairement aux monnaies traditionnelles, le bitcoin est entièrement virtuel. Il n'y a pas de pièces physiques ni même de pièces numériques en soi. Les pièces sont impliquées dans des transactions qui transfèrent de la valeur de l'expéditeur au destinataire. Les utilisateurs de Bitcoin possèdent des clés qui leur permettent de prouver la propriété du bitcoin dans le réseau Bitcoin. Avec ces clés, ils peuvent signer des transactions pour débloquer la valeur et la dépenser en la transférant à un nouveau propriétaire. Les clés sont souvent stockées dans un portefeuille numérique sur l'ordinateur ou le smartphone de chaque utilisateur. La possession de la clé qui peut signer une transaction est la seule condition préalable pour dépenser du bitcoin, mettant le contrôle entièrement entre les mains de chaque utilisateur.

Bitcoin est un système distribué pair à pair. En tant que tel, il n'y a pas de serveur "central" ou de point de contrôle. Les unités de bitcoin sont créés par un processus appelé "minage", qui implique une compétition pour trouver des solutions à un problème mathématique lors du traitement des transactions Bitcoin. Tout participant au réseau Bitcoin (c'est-à-dire toute personne utilisant un appareil exécutant la pile complète du protocole Bitcoin) peut opérer en tant que mineur, en utilisant la puissance de traitement de son ordinateur pour vérifier et enregistrer les transactions. Toutes les 10 minutes, en moyenne, un mineur de Bitcoin peut valider les transactions et est récompensé par un tout nouveau bitcoin. Essentiellement, l'extraction de Bitcoin décentralise les fonctions d'émission et de compensation de devises d'une banque centrale et remplace le besoin de cette dernière.

Le protocole Bitcoin comprend des algorithmes intégrés qui régulent la fonction de minage sur le réseau. La difficulté de la tâche de traitement que les mineurs doivent effectuer est ajustée dynamiquement de sorte qu'en moyenne, quelqu'un réussisse toutes les 10 minutes, quel que soit le nombre de mineurs (et la quantité de traitement) en compétition à tout moment. Le protocole réduit également de moitié le taux de création de nouveaux bitcoins tous les 4 ans et limite le nombre total de bitcoins qui seront créés à un total fixe juste en dessous de 21 millions de pièces. Le résultat est que le nombre de bitcoins en circulation suit de près une courbe facilement prévisible qui approche les 21 millions d'ici 2140. En raison du taux d'émission décroissant du bitcoin, sur le long terme, la monnaie Bitcoin est déflationniste. De plus, le bitcoin ne peut pas être gonflé en "imprimant" de la nouvelle monnaie au-delà du taux d'émission prévu.

Dans les coulisses, Bitcoin est aussi le nom du protocole, un réseau pair à pair et une innovation informatique distribuée. La monnaie bitcoin n'est vraiment que la première application de cette invention. Bitcoin représente l'aboutissement de décennies de recherche en cryptographie et en systèmes distribués et comprend quatre innovations clés réunies dans une combinaison unique et puissante. Bitcoin se compose de :

* Un réseau pair à pair décentralisé (le protocole Bitcoin)
* Un registre public des transactions (la chaîne de blocs)
* Un ensemble de règles pour la validation indépendante des transactions et l'émission de devises (règles de consensus)
* Un mécanisme pour parvenir à un consensus mondial décentralisé sur la chaîne de blocs valide (algorithme de Proof-of-Work (ou Preuve de travail))

En tant que développeur, je vois Bitcoin comme un Internet de l'argent, un réseau pour propager la valeur et sécuriser la propriété des actifs numériques via un calcul distribué. Il y a beaucoup plus à Bitcoin qu'il n'y paraît à première vue.

Dans ce chapitre, nous commencerons par expliquer certains des concepts et termes principaux, et obtenir le logiciel nécessaire et utiliser Bitcoin pour des transactions simples. Dans les chapitres suivants, nous commencerons à déballer les couches de technologie qui rendent Bitcoin possible et examinerons le fonctionnement interne du réseau et du protocole Bitcoin.

L'émergence d'une monnaie numérique viable est étroitement liée aux développements de la cryptographie. Cela n'est pas surprenant si l'on considère les défis fondamentaux liés à l'utilisation de bits pour représenter la valeur qui peut être échangée contre des biens et des services. Trois questions fondamentales pour quiconque accepte de l'argent numérique sont :

1. Puis-je avoir la certitude que l'argent est authentique et non contrefait ?
2. Puis-je avoir confiance que l'argent numérique ne peut être dépensé qu'une seule fois (connu sous le nom de problème de « double dépense ») ?
3. Puis-je être sûr que personne d'autre ne pourra prétendre que cet argent lui appartient et pas à moi ?

Les émetteurs de papier-monnaie luttent constamment contre le problème de la contrefaçon en utilisant des papiers et des technologies d'impression de plus en plus sophistiqués. L'argent physique résout facilement le problème des doubles dépenses, car le même billet papier ne peut pas se trouver à deux endroits à la fois. Bien sûr, l'argent conventionnel est aussi souvent stocké et transmis numériquement. Dans ces cas, les problèmes de contrefaçon et de double dépense sont traités en compensant toutes les transactions électroniques par des autorités centrales qui ont une vue globale de la monnaie en circulation. Pour la monnaie numérique, qui ne peut tirer profit des encres ésotériques ou des bandes holographiques, la cryptographie fournit la base pour faire confiance à la légitimité de la revendication de valeur d'un utilisateur. Plus précisément, les signatures numériques cryptographiques permettent à un utilisateur de signer un actif numérique ou une transaction prouvant la propriété de cet actif. Avec l'architecture appropriée, les signatures numériques peuvent également être utilisées pour résoudre le problème des doubles dépenses.

Lorsque la cryptographie a commencé à devenir plus largement disponible et comprise à la fin des années 1980, de nombreux chercheurs ont commencé à essayer d'utiliser la cryptographie pour créer des monnaies numériques. Ces premiers projets de monnaie numérique émettaient de la monnaie numérique, généralement adossée à une monnaie nationale ou à un métal précieux comme l'or.

Bien que ces anciennes monnaies numériques fonctionnaient, elles étaient centralisées et, par conséquent, faciles à attaquer par les gouvernements et les pirates. Les premières monnaies numériques utilisaient une chambre de compensation centrale pour régler toutes les transactions à intervalles réguliers, tout comme un système bancaire traditionnel. Malheureusement, dans la plupart des cas, ces monnaies numériques naissantes ont été ciblées par des gouvernements inquiets et ont finalement été dissoutes. Certains ont échoué dans des crashs spectaculaires lorsque la société mère a été liquidée brutalement. Pour être robuste contre l'intervention d'antagonistes, qu'il s'agisse de gouvernements légitimes ou d'éléments criminels, une monnaie numérique *décentralisée* était nécessaire pour éviter un seul point d'attaque. Bitcoin est un tel système, décentralisé par conception, et libre de toute autorité centrale ou point de contrôle qui peut être attaqué ou corrompu.

## Histoire de Bitcoin

Bitcoin a été inventé en 2008 avec la publication d'un article intitulé "Bitcoin : A Peer-to-Peer Electronic Cash System,"[[1]](#footnote-21) écrit sous l'alias de Satoshi Nakamoto (voir [???](#satoshi_whitepaper)). Nakamoto a combiné plusieurs inventions antérieures telles que b-money et HashCash pour créer un système de paiement électronique entièrement décentralisé qui ne repose pas sur une autorité centrale pour l'émission de devises ou le règlement et la validation des transactions. L'innovation clé consistait à utiliser un système de calcul distribué (appelé algorithme de « preuve de travail ») pour effectuer une « élection » globale toutes les 10 minutes, permettant au réseau décentralisé d'arriver à un *consensus* sur l'état des transactions. Cela résout élégamment le problème de la double dépense où une seule unité monétaire peut être dépensée deux fois. Auparavant, le problème des doubles dépenses était une faiblesse de la monnaie numérique et était résolu en compensant toutes les transactions via une chambre de compensation centrale.

Le réseau Bitcoin a démarré en 2009, sur la base d'une référence d’implémentation publiée par Nakamoto et révisée depuis par de nombreux autres programmeurs. La mise en œuvre de l'algorithme Proof-of-Work (ou Preuve de travail ou minage) qui assure la sécurité et la résilience de Bitcoin a augmenté de manière exponentielle et dépasse désormais la puissance de traitement combinée des meilleurs supercalculateurs du monde. La valeur marchande totale de Bitcoin a parfois dépassé 1 billion de dollars américains, selon le taux de change bitcoin-dollar. La transaction la plus importante traitée jusqu'à présent par le réseau était de 1,1 milliard de dollars américains, transmise instantanément et traitée pour des frais de seulement 0,68 $.

Satoshi Nakamoto s'est retiré du public en avril 2011, laissant la responsabilité de développer le code et le réseau à un groupe prospère de bénévoles. L'identité de la personne ou des personnes derrière Bitcoin est encore inconnue. Cependant, ni Satoshi Nakamoto ni personne d'autre n'exerce de contrôle individuel sur le système Bitcoin, qui fonctionne sur la base de principes mathématiques totalement transparents, d'un code à source libre et d'un consensus entre les participants. L'invention elle-même est révolutionnaire et a déjà engendré une nouvelle science dans les domaines de l'informatique distribuée, de l'économie et de l'économétrie.

L'invention de Satoshi Nakamoto est également une solution pratique et nouvelle à un problème d'informatique distribuée, connu sous le nom de "Problème des généraux byzantins". Brièvement, le problème consiste à essayer de s'entendre sur une ligne de conduite ou sur l'état d'un système en échangeant des informations sur un réseau peu fiable et potentiellement compromis. La solution de Satoshi Nakamoto, qui utilise le concept de preuve de travail pour parvenir à un consensus *sans autorité centrale de confiance*, représente une percée dans l'informatique distribuée et a une large applicabilité au-delà de la monnaie. Il peut être utilisé pour parvenir à un consensus sur les réseaux décentralisés afin de prouver l'équité des élections, des loteries, des registres d'actifs, de la notarisation numérique, etc.

## Utilisations, utilisateurs et histoires de Bitcoin

Bitcoin est une innovation dans l'ancienne technologie de l'argent. À la base, l'argent facilite simplement l'échange de valeur entre les personnes. Par conséquent, afin de bien comprendre Bitcoin et ses utilisations, nous l'examinerons du point de vue des personnes qui l'utilisent. Chacune des personnes et de leurs histoires, telles qu'énumérées ici, illustre un ou plusieurs cas d'utilisation spécifiques. Nous les verrons tout au long du livre :

Vente au détail de faible valeur en Amérique du Nord

Alice vit dans la région de la baie de Californie du Nord. Elle a entendu parler de Bitcoin par ses amis technophiles et veut commencer à l'utiliser. Nous suivrons son histoire au fur et à mesure qu'elle découvre le Bitcoin, en acquiert, puis dépense une partie de son bitcoin pour acheter une tasse de café au Bob's Cafe à Palo Alto. Cette histoire nous présentera le logiciel, les échanges et les transactions de base du point de vue d'un consommateur de détail.

Vente au détail de grande valeur en Amérique du Nord

Carol est propriétaire d'une galerie d'art à San Francisco. Elle vend des peintures chères pour Bitcoin. Cette histoire présentera les risques d'une attaque de consensus "51%" pour les détaillants d'articles de grande valeur.

Services contractuels extraterritorial

Bob, le propriétaire d'un café à Palo Alto, est en train de créer un nouveau site Web. Il a passé un contrat avec un développeur Web indien, Gopesh, qui vit à Bangalore, en Inde. Gopesh a accepté d'être payé en bitcoin. Cette histoire examinera l'utilisation de Bitcoin pour l'externalisation, les services contractuels et les virements internationaux.

Commerce en ligne

Gabriel est un jeune adolescent entreprenant à Rio de Janeiro, qui dirige une petite boutique en ligne qui vend des t-shirts, des tasses à café et des autocollants de marque Bitcoin. Gabriel est trop jeune pour avoir un compte bancaire, mais ses parents encouragent son esprit d'entreprise.

Dons caritatifs

Eugenia est directrice d'une association caritative pour enfants aux Philippines. Récemment, elle a découvert Bitcoin et souhaite l'utiliser pour atteindre un tout nouveau groupe de donateurs étrangers et nationaux afin de collecter des fonds pour son association caritative. Elle étudie également les moyens d'utiliser Bitcoin pour distribuer rapidement des fonds aux zones qui en ont besoin. Cette histoire montrera l'utilisation de Bitcoin pour la collecte de fonds mondiale à travers les devises et les frontières et l'utilisation d'un registre ouvert pour la transparence dans les organisations caritatives.

Importation/Exportation

Mohammed est un importateur d'électronique à Dubaï. Il essaie d'utiliser Bitcoin pour acheter des appareils électroniques aux États-Unis et en Chine pour les importer aux Émirats arabes unis afin d'accélérer le processus de paiement des importations. Cette histoire montrera comment Bitcoin peut être utilisé pour d'importants paiements internationaux interentreprises liés à des biens physiques.

Miner des bitcoins

Jing est un étudiant en génie informatique à Shanghai. Il a construit une plate-forme «minière» pour exploiter le bitcoin en utilisant ses compétences en ingénierie pour compléter ses revenus. Cette histoire examinera la base "industrielle" de Bitcoin : l'équipement spécialisé utilisé pour sécuriser le réseau Bitcoin et émettre de nouvelles devises.

Chacune de ces histoires est basée sur de vraies personnes et de vraies industries utilisant actuellement Bitcoin pour créer de nouveaux marchés, de nouvelles industries et des solutions innovantes aux problèmes économiques mondiaux.

## Mise en route

Bitcoin est un protocole accessible à l'aide d'une application cliente qui parle le protocole. Un "portefeuille Bitcoin" est l'interface utilisateur la plus courante du système Bitcoin, tout comme un navigateur Web est l'interface utilisateur la plus courante pour le protocole HTTP. Il existe de nombreuses implémentations et marques de portefeuilles Bitcoin, tout comme il existe de nombreuses marques de navigateurs Web (par exemple, Chrome, Safari, Firefox et Internet Explorer). Et tout comme nous avons tous nos navigateurs préférés (Mozilla Firefox, Yé !) et nos méchants (Internet Explorer, Beurk !), les portefeuilles Bitcoin varient en termes de qualité, de performances, de sécurité, de confidentialité et de fiabilité. Il existe également une implémentation de référence du protocole Bitcoin qui inclut un portefeuille, connu sous le nom de "Satoshi Client" ou "Bitcoin Core", qui est dérivé de l'implémentation originale écrite par Satoshi Nakamoto.

### Choisir un portefeuille Bitcoin

Les portefeuilles Bitcoin sont l'une des applications les plus activement développées dans l'écosystème Bitcoin. La concurrence est intense et, bien qu'un nouveau portefeuille soit probablement en cours de développement, plusieurs portefeuilles de l'année dernière ne sont plus activement maintenus. De nombreux portefeuilles se concentrent sur des plates-formes spécifiques ou des utilisations spécifiques et certains sont plus adaptés aux débutants tandis que d'autres sont remplis de fonctionnalités pour les utilisateurs avancés. Le choix d'un portefeuille est très subjectif et dépend de l'utilisation et de l'expertise de l'utilisateur. Par conséquent, il serait inutile de recommander une marque ou un portefeuille spécifique. Cependant, nous pouvons classer les portefeuilles Bitcoin en fonction de leur plate-forme et de leur fonction et fournir des éclaircissements sur tous les différents types de portefeuilles qui existent. Mieux encore, déplacer des clés ou des valeurs d’amorçages (les "seeds") entre les portefeuilles Bitcoin est relativement facile, il vaut donc la peine d'essayer plusieurs portefeuilles différents jusqu'à ce que vous en trouviez un qui corresponde à vos besoins.

Les portefeuilles Bitcoin peuvent être classés comme suit, selon la plateforme :

Portefeuille de bureau

Un portefeuille de bureau a été le premier type de portefeuille Bitcoin créé comme implémentation de référence et de nombreux utilisateurs utilisent des portefeuilles de bureau pour les fonctionnalités, l'autonomie et le contrôle qu'ils offrent. L'exécution sur des systèmes d'exploitation à usage général tels que Windows et Mac OS présente cependant certains inconvénients en matière de sécurité, car ces plates-formes sont souvent non sécurisées et mal configurées.

Portefeuille mobile

Un portefeuille mobile est le type le plus courant de portefeuille Bitcoin. Fonctionnant sur des systèmes d'exploitation de téléphones intelligents tels qu'Apple iOS et Android, ces portefeuilles sont souvent un excellent choix pour les nouveaux utilisateurs. Beaucoup sont conçus pour être simples et faciles à utiliser, mais il existe également des portefeuilles mobiles complets pour les utilisateurs expérimentés.

Portefeuille Web

Les portefeuilles Web sont accessibles via un navigateur Web et stockent le portefeuille de l'utilisateur sur un serveur appartenant à un tiers. Ceci est similaire au webmail en ce sens qu'il repose entièrement sur un serveur tiers. Certains de ces services fonctionnent à l'aide d'un code côté client exécuté dans le navigateur web de l'utilisateur, qui garde le contrôle des clés Bitcoin entre les mains de l'utilisateur. La plupart, cependant, présentent un compromis en prenant le contrôle des clés Bitcoin des utilisateurs en échange d'une facilité d'utilisation. Il est déconseillé de stocker de grandes quantités de bitcoins sur des systèmes tiers.

Portefeuille matériel (hardware)

Les portefeuilles matériels sont des appareils qui exploitent un portefeuille Bitcoin autonome sécurisé sur du matériel à usage spécial. Ils se connectent généralement à un ordinateur de bureau ou à un appareil mobile via un câble USB ou une communication en champ proche (NFC) et fonctionnent avec un navigateur Web ou un logiciel associé. En gérant toutes les opérations liées au Bitcoin sur le matériel spécialisé, ces portefeuilles sont considérés comme très sécurisés et adaptés au stockage de grandes quantités de Bitcoin.

Une autre façon de catégoriser les portefeuilles bitcoin est leur degré d'autonomie et la façon dont ils interagissent avec le réseau Bitcoin :

Client de nœud complet

Un client complet, ou "nœud complet", est un client qui stocke l'historique complet des transactions Bitcoin (chaque transaction par chaque utilisateur, toujours), gère les portefeuilles des utilisateurs et peuvent initier des transactions directement sur le réseau Bitcoin. Un nœud complet gère tous les aspects du protocole et peut valider indépendamment l'ensemble de la chaîne de blocs et toute transaction. Un client à nœud complet consomme des ressources informatiques importantes (par exemple, plus de 125 Go de disque, 2 Go de RAM) mais offre une autonomie complète et une vérification indépendante des transactions.

Client léger

Un client léger, également connu sous le nom de client de vérification de paiement simplifié (SPV ou simplified-payment-verification), se connecte aux nœuds complets Bitcoin (mentionnés précédemment) pour l'accès aux informations de transaction Bitcoin, mais stocke le portefeuille de l'utilisateur localement et crée, valide et transmet indépendamment les transactions. Les clients légers interagissent directement avec le réseau Bitcoin, sans intermédiaire.

Client API tiers

Un client API tiers est un client qui interagit avec Bitcoin via un système tiers d'interfaces de programmation d'applications (API), plutôt qu'en se connectant directement au réseau Bitcoin. Le portefeuille peut être stocké par l'utilisateur ou par des serveurs tiers, mais toutes les transactions passent par un tiers.

En combinant ces catégorisations, de nombreux portefeuilles Bitcoin se répartissent en quelques groupes, les trois plus courants étant le client complet de bureau, le portefeuille léger mobile et le portefeuille Web tiers. Les frontières entre les différentes catégories sont souvent floues, car de nombreux portefeuilles fonctionnent sur plusieurs plates-formes et peuvent interagir avec le réseau de différentes manières.

Pour les besoins de ce livre, nous démontrerons l'utilisation d'une variété de clients Bitcoin téléchargeables, de l'implémentation de référence (Bitcoin Core) aux portefeuilles mobiles et Web. Certains des exemples nécessiteront l'utilisation de Bitcoin Core, qui, en plus d'être un client complet, expose également les API au portefeuille, au réseau et aux services de transaction. Si vous envisagez d'explorer les interfaces de programmation dans le système Bitcoin, vous devrez exécuter Bitcoin Core ou l'un des clients alternatifs.

### Démarrage rapide

Alice, que nous avons présenté dans [Utilisations, utilisateurs et histoires de Bitcoin](#user-stories), n'est pas une utilisatrice technique et n'a entendu parler de Bitcoin que récemment par son ami Joe. Lors d'une fête, Joe explique à nouveau avec enthousiasme Bitcoin à tout le monde et propose une démonstration. Intriguée, Alice demande comment elle peut démarrer avec Bitcoin. Joe dit qu'un portefeuille mobile est ce qu'il y a de mieux pour les nouveaux utilisateurs et il recommande quelques-uns de ses portefeuilles préférés. Alice télécharge "Bluewallet" (disponible pour iOS et Android) et l'installe sur son téléphone.

Quand Alice exécute son application de portefeuille pour la première fois, elle choisit l'option de créer un nouveau portefeuille Bitcoin et prend un moment **loin de Joe et de toutes les autres parties** pour écrire une phrase mnémonique secrète *dans l'ordre* sur un morceau de papier. Comme expliqué par le portefeuille mobile et par Joe plus tôt, la phrase mnémotechnique permet à Alice de restaurer son portefeuille au cas où elle perdrait son appareil mobile et lui donne accès à ses fonds sur un autre appareil. Après avoir créé son portefeuille et sécurisé sa phrase mnémonique, Alice peut appuyer sur son portefeuille pour voir son montant en bitcoins, l'historique des transactions, ainsi que deux boutons qui lui permettent de *recevoir* ou *envoyer* des bitcoins, illustrés dans [figure\_title](#bluewallet-welcome).

### Mots Mnémoniques

Un portefeuille Bitcoin moderne fournira une *phrase mnémonique* (aussi parfois appelée "valeur d’amorçage" ou "phrase de récupération") qu'Alice pourra sauvegarder. La phrase mnémonique se compose de 12 à 24 mots anglais, sélectionnés au hasard par le logiciel, et utilisés comme base pour les clés générées par le portefeuille. La phrase mnémotechnique peut être utilisée par Alice pour restaurer toutes les transactions et tous les fonds de son portefeuille en cas d'événement tel qu'un appareil mobile perdu, un bogue logiciel ou une corruption de la mémoire.

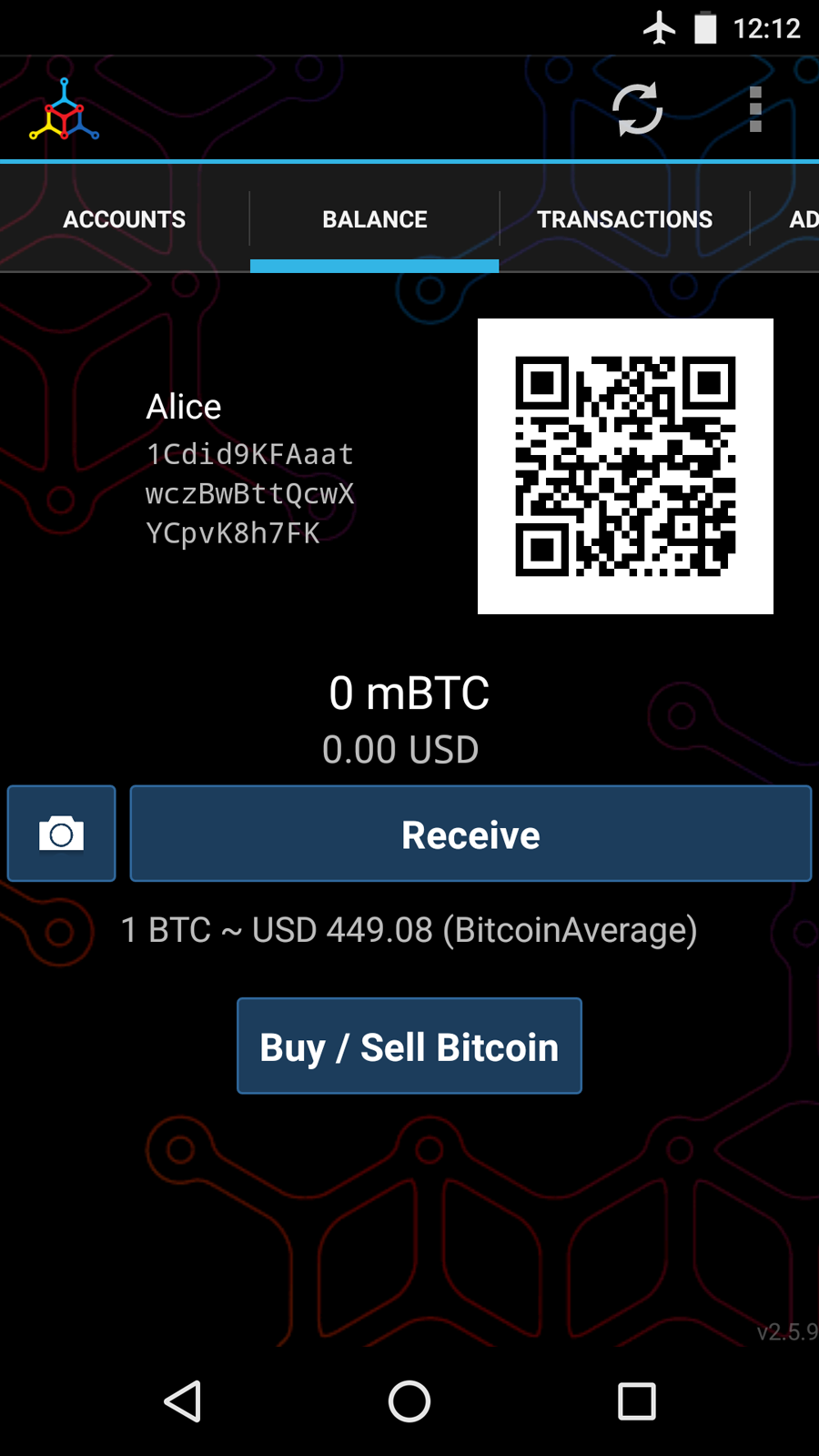
Le terme correct pour ces mots de sauvegarde est "phrase mnémonique". Nous évitons d'utiliser le terme "valeur d’amorçage" pour désigner une phrase mnémotechnique, car même si son utilisation est la même, son usage initial est différent.

### Stocker le mnémonique en toute sécurité

Alice doit faire attention à stocker la phrase mnémonique d'une manière qui équilibre la nécessité d'empêcher le vol et la perte accidentelle. Si elle ne le protège pas suffisamment, son mnémonique risque de se faire voler. Si elle le protège trop, son mnémonique risque d'être définitivement perdu. La méthode recommandée pour équilibrer correctement ces risques est d'écrire deux copies de la phrase mnémonique sur papier, avec chacun des mots numérotés selon l'ordre.

Une fois qu'Alice a enregistré la phrase mnémotechnique, elle doit prévoir de stocker chaque copie dans un endroit sécurisé séparé, tel qu'un tiroir de bureau verrouillé ou un coffre-fort ignifuge.

N'essayez jamais un système de sécurité "bricolage" qui s'écarte de quelque manière que ce soit de la recommandation des meilleures pratiques dans <<mnemonic-storage> >. Ne coupez pas votre mnémonique en deux, ne faites pas de captures d'écran, ne stockez pas sur des clés USB, des e-mails ou des lecteurs cloud, ne le cryptez pas ou n'essayez aucune autre méthode non standard. Vous ferez pencher la balance de manière à risquer une perte permanente ou un vol. De nombreuses personnes ont perdu de l'argent, non pas à cause d'un vol, mais parce qu'elles ont essayé une solution non standard sans avoir l'expertise pour équilibrer les risques encourus. La recommandation des meilleures pratiques est soigneusement équilibrée par des experts et adaptée à la grande majorité des utilisateurs.



Alice utilise l'écran de réception sur son portefeuille Bitcoin mobile Bluewallet et affiche son adresse à Bob au format de code QR

La vue principale du portefeuille affiche le montant en bitcoins, l'historique des transactions et les boutons *Receive* et *Send*. En outre, de nombreux portefeuilles offrent la possibilité d'acheter des Bitcoins directement via un échange ou un service similaire où vous pouvez offrir de l'argent fiduciaire en échange de cryptomonnaie, ce qui est fait par [simpara\_title](#bitcoin_price) et vendre à l'utilisateur du portefeuille à ce prix ou au-dessus. Le bouton *Buy Bitcoin* permettrait à Alice d'acheter des Bitcoins de cette manière.

Alice est maintenant prête à commencer à utiliser son nouveau portefeuille Bitcoin. Son application de portefeuille a généré aléatoirement une clé privée (décrite plus en détail dans [???](#private_keys)) qui sera utilisé pour dériver des adresses Bitcoin qui dirigent vers son portefeuille. À ce stade, ses adresses Bitcoin ne sont pas connues du réseau Bitcoin ou "enregistrées" auprès d'une quelconque partie du système Bitcoin. Ses adresses Bitcoin sont simplement des nombres aléatoires qui correspondent à sa clé privée qu'elle peut utiliser pour contrôler l'accès aux fonds. Les adresses sont générées indépendamment par son portefeuille sans référence ni inscription à aucun service. En fait, dans la plupart des portefeuilles, il n'y a aucune association entre une adresse Bitcoin et toute information d'identification externe, y compris l'identité de l'utilisateur. Jusqu'au moment où une adresse est référencée comme destinataire de la valeur dans une transaction publiée sur le grand livre bitcoin, l'adresse Bitcoin fait simplement partie du grand nombre d'adresses possibles valides en bitcoin. Ce n'est qu'une fois qu'une adresse a été associée à une transaction qu'elle fait partie des adresses connues du réseau.

Alice utilise le bouton *Receive*, qui affiche un code QR avec une adresse Bitcoin. Le code QR est le carré avec un motif de points noirs et blancs, servant de forme de code-barres contenant les mêmes informations dans un format pouvant être scanné par l'appareil photo du smartphone de Joe. À côté du code QR du portefeuille se trouve l'adresse Bitcoin qu'il encode, et Alice peut choisir d'envoyer manuellement son adresse à Joe en la copiant dans son presse-papiers d'un simple toucher. Il convient de noter que lorsque vous recevez des fonds sur un nouveau portefeuille mobile pour la première fois, de nombreux portefeuilles revérifieront souvent que vous avez bien sécurisé votre phrase mnémonique. Cela peut aller d'une simple invitation à demander à l'utilisateur de ressaisir manuellement la phrase.

Les adresses Bitcoin commencent par 1, 3 ou bc1. Comme les adresses e-mail, elles peuvent être partagées avec d'autres utilisateurs de bitcoins qui peuvent les utiliser pour envoyer des bitcoins directement dans votre portefeuille. Il n'y a rien de sensible, du point de vue de la sécurité, à propos de l'adresse Bitcoin. Il peut être affiché n'importe où sans risquer la sécurité du compte. Contrairement aux adresses e-mail, vous pouvez créer de nouvelles adresses aussi souvent que vous le souhaitez, qui dirigeront toutes les fonds vers votre portefeuille. En fait, de nombreux portefeuilles modernes créent automatiquement une nouvelle adresse pour chaque transaction afin de maximiser la confidentialité. Un portefeuille est simplement une collection d'adresses et les clés qui débloquent les fonds à l'intérieur.

==== Obtenir son premier Bitcoin

Il existe plusieurs façons pour Alice d'acquérir des bitcoins :

* Elle peut échanger une partie de sa monnaie nationale (par exemple USD) à un échange de crypto-monnaie
* Elle peut en acheter à un ami ou à une connaissance d'un Meetup Bitcoin, en échange d'argent
* Elle peut trouver un *guichet Bitcoin* dans sa région, qui agit comme un distributeur automatique, vendant des bitcoins contre de l'argent
* Elle peut offrir ses compétences ou un produit qu'elle vend et accepte le paiement en bitcoin
* Elle peut demander à son employeur ou à ses clients de la payer en bitcoin

Toutes ces méthodes présentent des degrés de difficulté variables et nombre d'entre elles impliquent le paiement de frais. Certaines institutions financières exigeront également qu'Alice fournisse des documents d'identification pour se conformer aux réglementations bancaires locales/aux pratiques de lutte contre le blanchiment d'argent (AML), un processus connu sous le nom de Know Your Customer (KYC). Cependant, avec toutes ces méthodes, Alice pourra recevoir des bitcoins.

L'un des avantages du bitcoin par rapport aux autres systèmes de paiement est que, lorsqu'il est utilisé correctement, il offre aux utilisateurs beaucoup plus d'intimité. Acquérir, détenir et dépenser des bitcoins ne vous oblige pas à divulguer des informations sensibles et personnellement identifiables à des tiers. Cependant, lorsque le bitcoin touche les systèmes traditionnels, tels que les échanges de devises, les réglementations nationales et internationales s'appliquent souvent. Afin d'échanger des bitcoins contre votre monnaie nationale, il vous sera souvent demandé de fournir une preuve d'identité et des informations bancaires. Les utilisateurs doivent savoir qu'une fois qu'une adresse Bitcoin est associée à une identité, toutes les transactions Bitcoin associées sont également faciles à identifier et à suivre. C'est l'une des raisons pour lesquelles de nombreux utilisateurs choisissent de maintenir des comptes d'échange dédiés non liés à leurs portefeuilles.

Alice a été initiée au bitcoin par un ami, elle a donc un moyen facile d'acquérir son premier bitcoin. Ensuite, nous verrons comment elle achète des bitcoins à son ami Joe et comment Joe envoie les bitcoins dans son portefeuille.

==== Trouver le prix actuel du Bitcoin

Avant qu'Alice puisse acheter du bitcoin à Joe, ils doivent s'entendre sur le *taux de change* entre le bitcoin et le dollar américain . Cela soulève une question courante pour ceux qui découvrent le bitcoin : "Qui fixe le prix du bitcoin ?" La réponse courte est que le prix est fixé par les marchés.

Le bitcoin, comme la plupart des autres devises, a un *cours du change flottant*. Cela signifie que la valeur du bitcoin vis-à-vis de toute autre devise fluctue en fonction de l'offre et de la demande sur les différents marchés où il est négocié. Par exemple, le « prix » du bitcoin en dollars américains est calculé sur chaque marché en fonction de la transaction la plus récente de bitcoin et de dollars américains. En tant que tel, le prix a tendance à fluctuer minutieusement plusieurs fois par seconde. Un service de tarification regroupera les prix de plusieurs marchés et calculera une moyenne pondérée en fonction du volume représentant le taux de change général du marché d'une paire de devises (par exemple, BTC/USD).

Il existe des centaines d'applications et de sites Web qui peuvent fournir le taux actuel du marché. Voici quelques-uns des plus populaires :

[Bitcoin Average](https://bitcoinaverage.com/)

Un site qui fournit une vue simple de la moyenne pondérée en fonction du volume pour chaque devise.

[CoinCap](https://coincap.io/)

Un service répertoriant la capitalisation boursière et les taux de change de centaines de crypto-monnaies, dont le bitcoin.

[Chicago Mercantile Exchange Bitcoin Reference Rate](https://bit.ly/cmebrr)

Un taux de référence qui peut être utilisé comme référence institutionnelle et contractuelle, fourni dans le cadre des flux de données d'investissement par le CME.

En plus de ces différents sites et applications, la plupart des portefeuilles bitcoin convertiront automatiquement les montants entre le bitcoin et d'autres devises. Joe utilisera son portefeuille pour convertir automatiquement le prix avant d'envoyer des bitcoins à Alice.

==== Envoi et réception de Bitcoin

Alice a décidé d'échanger 10 dollars américains contre des bitcoins, afin de ne pas risquer trop d'argent sur cette nouvelle technologie. Elle donne à Joe 10 $ en espèces, ouvre son application de portefeuille mobile Bluewallet et sélectionne Recevoir. Cela affiche un code QR avec la première adresse Bitcoin d'Alice.

Joe sélectionne ensuite *Envoyer* sur son portefeuille de smartphone Bluewallet et un écran contenant les entrées suivantes s'affiche :

* Le montant à envoyer, en bitcoin (BTC) ou sa devise locale (USD)
* Une adresse Bitcoin de destination
* Une note de transaction (description)
* Des frais de transaction

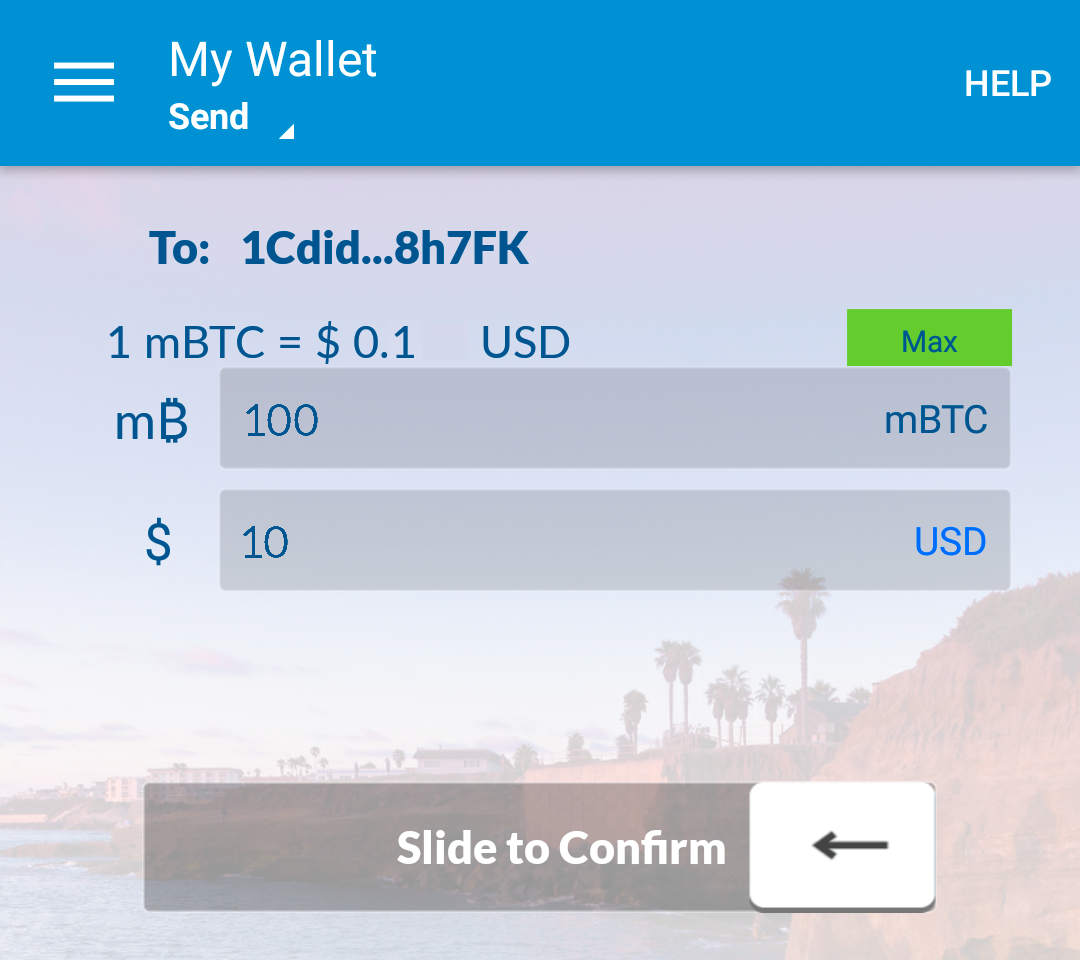
Dans le champ de saisie de l'adresse Bitcoin, il y a un petit bouton *Scan*. Cela permet à Joe de scanner le code QR avec l'appareil photo de son smartphone afin de ne pas avoir à taper l'adresse Bitcoin d'Alice, qui est assez longue et difficile à taper. Joe appuie sur le bouton *Scan* et il active la caméra du smartphone, scannant le code QR affiché sur le smartphone d'Alice.

Joe a maintenant l'adresse Bitcoin d'Alice définie comme destinataire. Joe saisit le montant de 10 dollars américains et son portefeuille le convertit en accédant au taux de change le plus récent à partir d'un service en ligne. Le taux de change à l'époque est de 100 dollars américains par bitcoin, donc 10 dollars américains valent 0,10 bitcoin (BTC) ou 100 millibitcoin (mBTC) comme le montre la capture d'écran du portefeuille de Joe (voir [figure\_title](#bluewallet-mobile-send)).

Dans la saisie de la note/description de la transaction, Joe saisit « Alice ». Il peut utiliser ce champ pour ajouter des informations concernant sa transaction pour référence future. Cette fonction est pour sa tenue de dossiers uniquement. La note de transaction sera stockée dans son portefeuille et seul Joe pourra la voir. Il ne sera pas envoyé à Alice, ni stocké sur la blockchain.

Il sélectionne également des frais de transaction pour sa transaction. Plus les frais de transaction sont élevés, plus vite sa transaction sera confirmée (incluse dans un bloc par un mineur). Il sélectionne les frais de transaction minimum possibles à ce moment-là (0 satoshis/octet).

Le prix du bitcoin a beaucoup changé au fil du temps, et une quantité incroyable depuis la rédaction de la première édition de ce livre. En mars 2021, une personne aurait besoin d'environ 54 000 USD pour acheter un bitcoin entier. De nombreux exemples dans ce livre font référence à des transactions passées réelles, lorsque le prix du bitcoin était beaucoup plus bas et que des transactions sans frais étaient encore possibles. Pensez à quel point Joe aurait été un ami généreux s'il avait conclu le même accord avec Alice aujourd'hui !



Écran d'envoi du portefeuille bitcoin mobile Bluewallet

À l'aide de Bluewallet, Joe vérifie soigneusement qu'il a saisi le bon montant, car il est sur le point de transmettre de l'argent et les erreurs sont irréversibles. Par souci de simplicité, nous supposerons que Joe ne paie aucun frais de transaction. L'objet et la fixation des frais de transaction sont traités dans les chapitres suivants. Après avoir revérifié l'adresse et le montant, il appuie sur *Envoyer* pour transmettre la transaction. Le portefeuille bitcoin mobile de Joe construit une transaction qui attribue 0,10 BTC à l'adresse fournie par Alice, puise les fonds dans le portefeuille de Joe et signe la transaction avec les clés privées de Joe. Cela indique au réseau Bitcoin que Joe a autorisé un transfert de valeur vers la nouvelle adresse d'Alice. Comme la transaction est transmise via le protocole pair à pair, elle se propage rapidement sur le réseau Bitcoin. En moins d'une seconde, la plupart des nœuds bien connectés du réseau reçoivent la transaction et voient l'adresse d'Alice pour la première fois.

Pendant ce temps, le portefeuille d'Alice "écoute" constamment les transactions publiées sur le réseau Bitcoin, à la recherche de celles qui correspondent aux adresses qu'il contient. Quelques secondes après que le portefeuille de Joe ait transmis la transaction, le portefeuille d'Alice indiquera qu'il reçoit 0,10 BTC.

Chaque bitcoin peut être subdivisé en 100 millions d'unités, chacune appelée "satoshi" (singulier) ou "satoshis" (pluriel). Nommé en l'honneur du créateur du bitcoin, le Satoshi est la plus petite unité de bitcoin, équivalente à 0,00000001 BTC.

**Confirmations**

Au début, le portefeuille d'Alice affichera la transaction de Joe comme "Non confirmée". Cela signifie que la transaction a été propagée au réseau mais n'a pas encore été enregistrée dans le registre des transactions bitcoin, connu sous le nom de blockchain ou la chaîne de blocs. Pour être confirmée, une transaction doit être incluse dans un bloc et ajoutée à la chaîne de blocs, ce qui se produit toutes les 10 minutes en moyenne. En termes financiers traditionnels, cela s'appelle *liquidation (ou clearing)*. Ce livre couvrira en détail la propagation, la validation et la liquidation (ou la confirmation) des transactions bitcoin.

Alice est maintenant l'heureuse propriétaire de 0,10 BTC qu'elle peut dépenser. Dans le chapitre suivant, nous examinerons son premier achat avec Bitcoin et examinerons plus en détail les technologies sous-jacentes de transaction et de propagation.

1. "Bitcoin: A Peer-to-Peer Electronic Cash System," Satoshi Nakamoto (<https://bitcoin.org/bitcoin.pdf>). [↑](#footnote-ref-21)