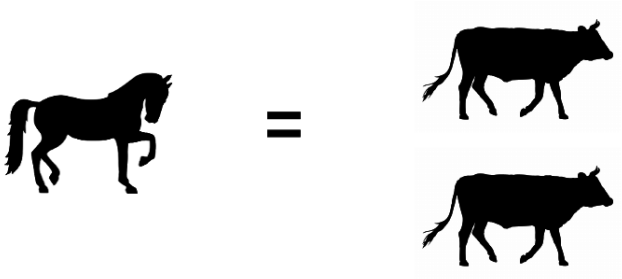
COMPRENDRE LE BITCOIN
et la BlockChain

Pour bien parler du Bitcoin, il faut d'abord savoir ce qu'est une monnaie. En voulant comprendre le fonctionnement du Bitcoin, j'ai dû en apprendre ce qu'est vraiment l'argent. Et ce n'est pas si simple !

Avant la monnaie : le troc

Avant de créer la monnaie, les échanges entre les personnes étaient basés essentiellement sur le troc : on échangeait des produits contre d'autres produits. Ainsi, on pouvait dire par exemple qu'un cheval vaut deux boeufs :



Un cheval vaut deux bœufs

Qui détermine qu'1 cheval vaut 2 boeufs ? Et pourquoi 1 boeuf ne vaudrait pas 2 chevaux ?!
Les gens se mettent tout simplement d'accord, après avoir parfois négocié. Globalement, **plus c'est rare, plus c'est cher**. Si les chevaux sont plus rares que les boeufs, c'est normal qu'il faille plusieurs boeufs pour en acheter un.
Bon, c'est encore simpliste, je le reconnais. Imaginez maintenant que la personne qui possède le cheval souhaite acheter 1 boeuf (et pas 2). Que va-t-elle faire ? Couper le cheval en deux ?
Hum, couper le cheval en deux... Ca va pas le tuer ça ?! Et donc lui faire perdre sa valeur ?

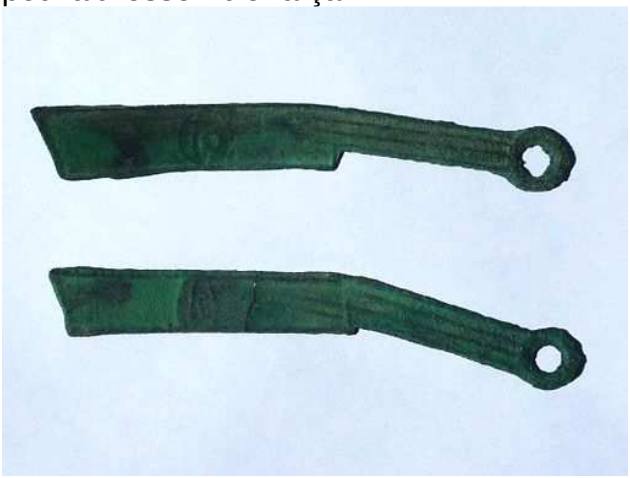
Vous avez bien compris l'absurdité de la chose.

Pour faciliter les échanges, et notamment tenir compte des plus petites divisions, des monnaies ont été créées.

Les monnaies primitives

On retrouve des traces de monnaie assez loin dans le temps, comme des dents d'animaux, couteaux, des barres de cuivre et des colliers en bronze (au deuxième

millénaire avant J.C. !). Au début, la monnaie n'avait donc pas la forme de pièces mais pouvait ressembler à ça :



Des couteaux chinois qui servaient de monnaie, en 600-200 av. J.C. (Michel-Georges Bernard, CC-BY-SA)

A une époque, les légionnaires romains étaient payés en sel. C'est de là que vient le mot "salaire".

De son côté, l'or étant un métal rare, il est devenu précieux et a pris de la valeur. On s'en est aussi servi comme monnaie d'échange et on en a fait des pièces pour visualiser rapidement la valeur.

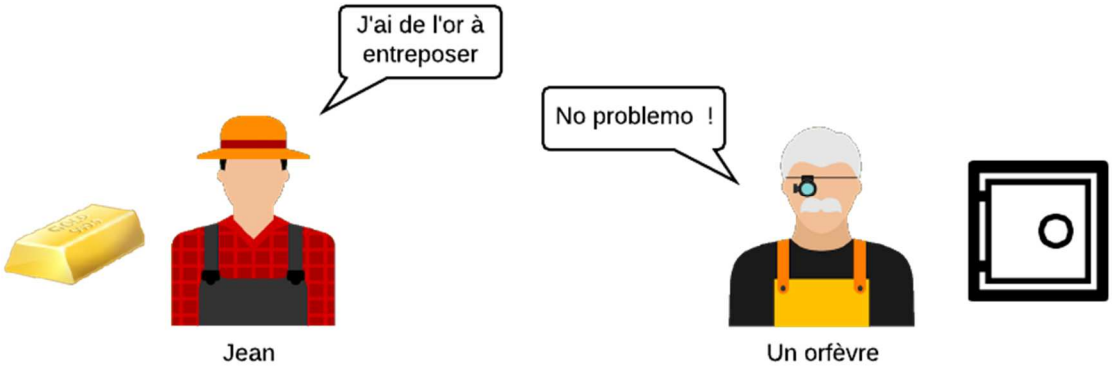
Une monnaie grecque représentant Zeus : le statère

Pour l'anecdote, dans la Grèce antique, on utilisait parfois plus souvent l'argent (le métal) que l'or. L'argent est aussi un métal précieux comme l'or. Aujourd'hui le terme "argent" fait aussi bien référence à la monnaie qu'au métal.

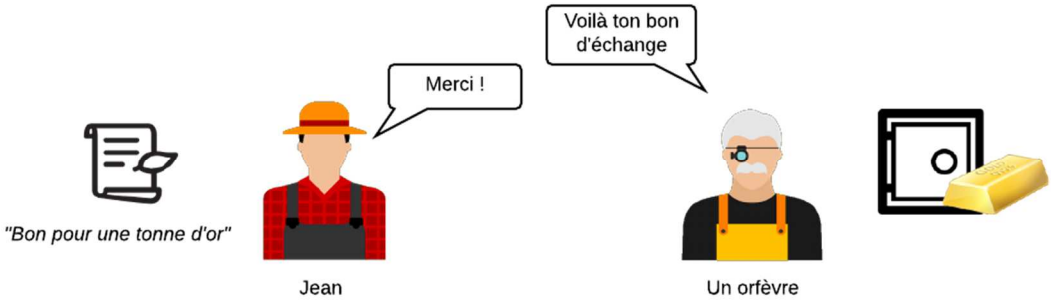
Ces pièces étaient bien plus pratiques à échanger, mais elles avaient un défaut... Elles étaient constituées d'un métal précieux. Que se passait-il si on perdait une pièce ? L'or était perdu.

C'est là qu'il faut que je vous parle de notre ami l'orfèvre :

Un orfèvre dans son atelier (Petrus Christus - 1449)
Son job à la base, c'est de fabriquer des objets en or. Et comme l'or c'était son truc, on a commencé à lui demander s'il ne pouvait pas conserver l'or dans son coffre-fort. Comme ça, l'or était bien au chaud, et on ne risquait pas de le perdre bêtement.



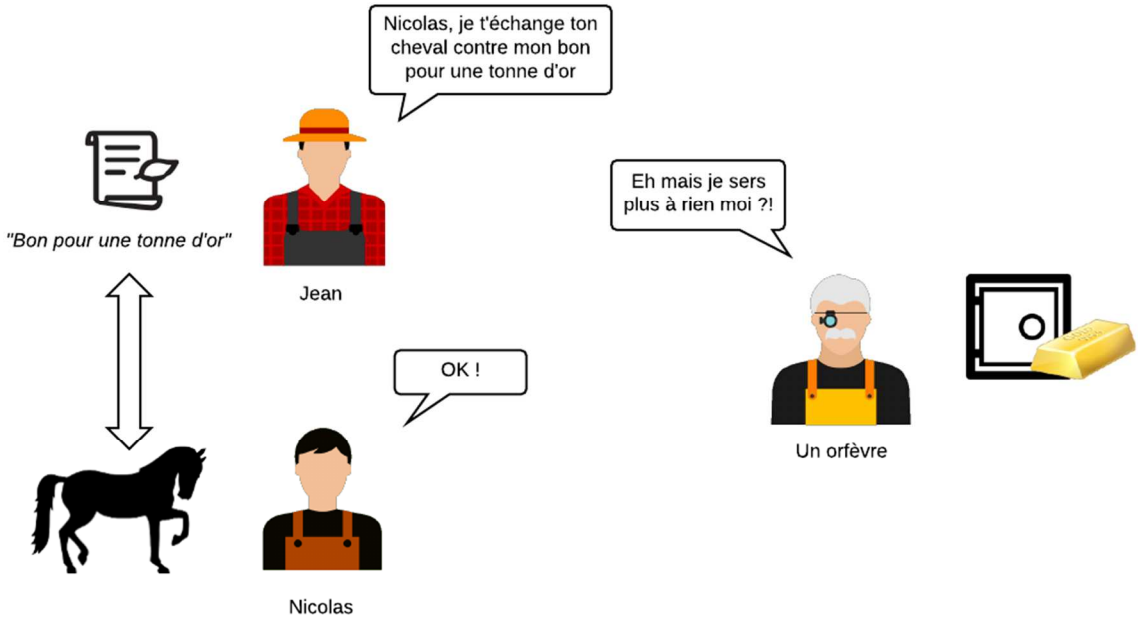
Jean souhaite entreposer de l'or chez l'orfèvre
En échange de l'or entreposé chez eux, les orfèvres donnaient un papier à leurs clients : un certificat de dépôt (du type "Bon pour une tonne d'or"). Ainsi, les clients pouvaient revenir à tout moment récupérer leur or en échange de ce certificat.



Le client reçoit un bon pour pouvoir récupérer son or quand il veut

Les orfèvres deviennent banquiers

Il se trouve que le papier était plus pratique à transporter que l'or. Les clients ont commencé à s'échanger les certificats entre eux pour s'acheter des biens. Après tout, donner un "bon pour une tonne d'or", c'est comme si on donnait une tonne d'or non ? Avec le bon, on peut récupérer l'or correspondant à tout moment.



Les gens commencent à s'échanger les bons entre eux
Ce certificat était en quelque sorte le précurseur du billet de banque qu'on connaît aujourd'hui.
Jusque là, tout va bien, c'est encore assez simple. Mais attendez, ça va commencer à se compliquer un peu.
Malins, les orfèvres ont constaté que les clients venaient rarement récupérer leur or. En même temps, on les sollicitait pour des prêts. **Les orfèvres ont commencé à diffuser plus de certificats de dépôt qu'il n'y avait d'or dans leurs coffres**. Ainsi, il pouvait y avoir "2000 d'or" de certificats de dépôt en circulation, même s'il n'y avait en réalité que "1000 d'or" dans les coffres.

Les orfèvres ont commencé à diffuser plus de bons qu'ils n'avaient d'or dans leurs coffres
Mais heu... ça peut pas marcher ça !
Si, ça peut. Ca fonctionne du temps que tout le monde ne vient pas récupérer son or en même temps. Evidemment, si Louis et Arnaud viennent chacun récupérer une tonne d'or en même temps, la banque ne les aura pas et fera faillite. Et les gens ne seront probablement pas très contents.
C'est comme ça que les orfèvres, devenus banquiers, ont commencé à prêter de l'argent... qu'ils n'avaient pas. C'est un peu fou, mais ça fonctionne comme ça depuis le XVIIème siècle et... **c'est encore le cas aujourd'hui**.
On utilise toujours des pièces de monnaie, mais, vous vous en doutez, elles ne sont plus en or. Elles sont dans un métal qui a très peu de valeur. La pièce représente une certaine quantité d'argent, comme les billets.
Les pièces et les billets ont de la valeur parce qu'on a **confiance** dans le fait qu'on pourra acheter des biens avec. **Tout le système repose sur la confiance**. C'est pour cela qu'on parle de monnaie *fiduciaire*.

De l'étalon-or aux changes flottants

On pourrait encore passer des heures à expliquer comment la monnaie a évolué, mais je ne veux pas tous vous endormir avec mes histoires d'orfèvre. 😔 Surtout que ça devient progressivement plus compliqué. Alors permettez-moi de faire la suite de l'histoire en accéléré.
Jusqu'en 1914, toutes les monnaies sont définies par rapport à l'or. On parle **d'étalon-or**. On peut directement convertir une monnaie en or. C'était le cas avec l'orfèvre : un "bon" correspondait directement à de l'or véritable.
A partir de 1944, avec les accords de Bretton Woods, il est décidé que seul le dollar américain devient directement convertible en or.
En 1971, les Etats-Unis abandonnent cette convertibilité du dollar en or, pour avoir plus de flexibilité sur le nombre de billets qu'ils peuvent imprimer.

A partir de là, toutes les monnaies peuvent s'échanger entre elles, mais ne correspondent plus à de l'or réel. C'est toujours le cas aujourd'hui. On dit qu'on utilise des changes flottants : 1 dollar vaut par exemple 1,20 euros le matin, mais le soir 1 dollar ne vaut plus que 1,15 euros. Tout dépend de l'offre et de la demande : les cours varient librement, il n'y a plus d'or en jeu.
Pfiou.

Chaque monnaie se convertit dans d'autres monnaies à un prix différent

Le cours d'une monnaie change rapidement au sein d'une même journée

Il n'y a pas d'argent sur votre compte en banque

Allez, j'ai presque fini, je vous ai gardé le meilleur pour la fin.
Je reste vraiment le plus simple possible, mais ça va vous donner les bases pour bien comprendre le Bitcoin par la suite.
Il ne reste plus qu'une vérité terrible à vous annoncer : **il n'y a pas vraiment d'argent sur votre compte en banque**.
Vous voyez marqué "+1000€" sur votre compte en banque en ligne, et vous pensez que vous *avez* 1000€. Erreur ! Ce "1000" est juste une ligne dans une base de données

du système informatique de la banque. En réalité, elle ne vous garde pas ces 1000€ en billets au chaud dans un coffre-fort rien que pour vous.
L'argent affiché sur un compte en banque correspond à ce que la banque *vous doit*. Les 1000€ affichés sur votre compte en ligne sont donc une dette de 1000€ de la banque envers vous.
Tu dis que la banque n'a pas les 1000€. Pourtant, si je vais au distributeur de billets, je peux bien récupérer mes 1000€ non ?
Oui. Mais si tout le monde fait ça en même temps, on va très vite découvrir que la banque ne possède pas tous les billets qu'elle dit posséder. Souvenez-vous de ce que faisaient les orfèvres... les banques font toujours pareil ! La loi impose que les banques aient juste une petite partie de l'argent qu'elles disent avoir, mais c'est tout.
Ainsi, sur 1000€ que la banque dit avoir, elle n'en possède peut-être réellement que 100€. Elle peut vous donner 1000€ en billets de banque, mais elle ne pourra pas le faire à tout le monde en même temps.

Seules les pièces et les billets dans votre poche ont aujourd'hui de la valeur (la monnaie *fiduciaire*). En revanche, ce qui est affiché sur un compte en banque n'est qu'une promesse de la banque envers vous qu'elle a cet argent (c'est la monnaie *scripturale*).
Lorsque les individus se ruent vers les distributeurs de billets en même temps, on dit que c'est un "bank run". Et c'est clairement une catastrophe, car ça provoque l'effondrement des banques... et une grosse crise financière ensuite.
C'est arrivé en Grèce récemment : l'Etat a dû limiter les retraits aux distributeurs de billets. Même si vous aviez 50 000€ sur votre compte en banque, vous ne pouviez plus en utiliser qu'une petite partie.

Dernière révélation : l'économie est aujourd'hui en très grande partie basée sur le crédit. Si vous voulez acheter une voiture à 10 000€ et que vous demandez un crédit de 10 000€ à votre banque, que fait-elle ? Elle ajoute simplement "+10 000" dans la base de données. Il n'y a pas plus de billets en circulation. En fait, **les banques créent de l'argent en faisant crédit** (ce n'est pas une blague !).

Pour conclure

Que les économistes m'excusent si j'ai simplifié les choses à l'extrême : il faut dire que le système financier est très compliqué ! Et c'est d'ailleurs ce que je voudrais que vous reteniez : les choses sont tout sauf simples. Je pense cependant vraiment qu'on devrait apprendre une partie de tout cela à l'école (en tout cas moi j'aurais bien aimé !).

J'ai essayé dans ce chapitre de vous donner les grandes idées, en espérant vous avoir donné envie d'en savoir plus. Je me suis aussi efforcé de garder un ton aussi neutre que possible, mais il faut savoir que le fonctionnement actuel du système est très discuté (vous avez forcément entendu parler de "dérégulation des marchés financiers" !).
Les choses "tiennent" actuellement mais rien ne dit que cela puisse fonctionner indéfiniment comme ça. En particulier, il y a des individus qui cherchent depuis des années à se passer des banques, qui jouent le rôle d'intermédiaires. Avec le Bitcoin, on est en passe de trouver un début de réponse à la question !

Nous avons parlé de l'histoire de la monnaie, intéressons-nous maintenant au mouvement *crypto-anarchiste*. Je sais, ça fait un peu peur dit comme ça, mais vous ne pouvez pas parler du Bitcoin et de la Blockchain sans comprendre ce qui a motivé leurs créateurs... les crypto-anarchistes.

Allez, comme dans Matrix, je vous propose de prendre la pilule rouge et de suivre le lapin blanc.

Prenez la pilule rouge et suivez le lapin blanc dans son terrier

Des anarchistes aux crypto-anarchistes

Je suis sûr que vous avez déjà entendu parler des **anarchistes** ? Qu'est-ce que c'est exactement ? Si on regarde le dictionnaire, on apprend que c'est une philosophie. Dans cette philosophie, on souhaite que la société soit autoorganisée, sans hiérarchie... et tout particulièrement sans Etat.
Les anarchistes considèrent que l'Etat n'est pas désirable, qu'il est même dangereux. Ils se méfient donc fortement des institutions, telle que la police, les banques...
En quelque sorte, l'anarchisme est un peu la version à l'extrême opposé du fascisme. Là où les anarchistes imaginent un monde où "chacun fait ce qu'il veut, les choses se régulent entre les gens, il n'y a pas de hiérarchie", les fascistes imaginent un monde où "tout est régulé, sous contrôle de l'Etat, avec une hiérarchie stricte".

Et les crypto-anarchistes dans tout ça ?

C'est un peu la branche "geek" des anarchistes. Il s'agit clairement de personnes qui ont un bon voire très bon niveau technique : ils savent comment Internet fonctionne, comment protéger des informations sur les réseaux, etc.
On emploie aussi le terme de **cypherpunk**. Pour faire simple, un cypherpunk crée les programmes, tandis que le crypto-anarchiste se contente plutôt de les utiliser.
En fait, on pourrait comparer les anarchistes et les crypto-anarchistes comme ceci :

- **Anarchistes** : vivent dans le monde réel
- **Crypto-anarchistes** : vivent dans le monde virtuel, le "cyber-espace"

Ca fait un peu fou dit comme ça, mais le cyber-espace est à bien des égards un nouveau territoire, que la plupart des crypto-anarchistes maîtrisent très bien.
Le cyber-espace est parfois considéré comme un territoire vierge, où les lois ne s'appliquent pas car la notion de territoire géographique n'a plus de sens. En effet, les

données peuvent être partout à la fois, chiffrées et échangées par plusieurs intermédiaires.

Les crypto-anarchistes, rois du chiffrement

Le chiffrement, c'est une façon de coder les données pour que personne d'autre que le destinataire ne puisse les lire (on emploie aussi le mot "cryptage", mais c'est un anglicisme).
Les crypto-anarchistes disent : "Il faut chiffrer toutes ses données, tout le temps, pour que personne d'autre ne puisse les lire".
Mais pourquoi les crypto-anarchistes veulent tout chiffrer ? Ont-ils quelque chose à cacher ?
Pas forcément : ils voient plus ça comme un principe de précaution.
Quand on leur demande pourquoi, ils rétorquent en général : "Et vous, avez-vous quelque chose à cacher ?". Probablement pas. "Pourtant, vous seriez mal à l'aise si quelqu'un venait mettre une caméra de sécurité chez vous et vous surveillait 24h/24, 7j/7". Et c'est précisément ce que se disent les crypto-anarchistes : "Dans le doute, chiffrons et cachons tout, on ne sait jamais ce qui peut se passer à l'avenir".
Mon message ici n'est pas de dire "ces gens-là ont raison", mais plutôt d'expliquer leur raisonnement. Cela va vous permettre de comprendre comment on en est arrivé au Bitcoin.

Pourquoi les crypto-anarchistes ?

Plusieurs évènements ont motivé les crypto-anarchistes à chercher à tout chiffrer et tout cacher. Voici quelques exemples :

Edward Snowden

Ce consultant pour la NSA a dévoilé que les Etats-Unis surveillaient en masse toutes les communications mondiales, y compris celles de leur propre population. C'est un lanceur d'alerte, héros pour les uns, ennemi de la nation pour les autres (tout dépend du point de vue).
Ce qui est sûr, c'est que l'impact de ses révélations a été considérable, à tel point qu'on parle désormais d'"**Ère post-Snowden**", pour désigner la période actuelle où nous *savons* que nous sommes surveillés, car nous en avons eu la preuve.

Edward Snowden, à l'origine des révélations de surveillance massive par les Etats-Unis

Pour ceux qui veulent en savoir plus, il existe un film sur Snowden.

Les Nazis lors de la seconde guerre mondiale

Si on remonte un peu plus loin dans l'Histoire, on se rend compte que les données apparemment anodines ont été utilisées pour de mauvaises intentions.
Avant l'arrivée des Nazis, l'Etat français tenait un registre avec différentes statistiques ethniques et religieuses (par exemple... "qui est juif"). L'Etat n'avait pas forcément de mauvaises intentions en tenant ce registre, mais le jour où les Nazis sont arrivés en France, ils ont pu mettre la main sur ces fichiers et s'en servir pour envoyer directement ces personnes dans les camps de concentration. C'est d'ailleurs pour ça qu'en France il est interdit de tenir des fichiers avec des données ethniques aujourd'hui (oui, on peut dire qu'il y a un certain traumatisme).

Que fait un crypto-anarchiste ?

Comme je vous le disais, un crypto-anarchiste est quelqu'un qui a un bon niveau technique. Il comprend comment fonctionnent les échanges sur Internet, a quelques notions de programmation, utilise Linux, etc. Il chiffre toutes ses communications, même les plus anodines, ce qui peut sembler paranoïaque à première vue.
Ils n'utilisent que des logiciels dans lesquels ils ont confiance et qui leur permettent de naviguer anonymement, pour que personne ne puisse savoir ce qu'ils font :

- **Linux** : le crypto-anarchiste ne jure que par le logiciel libre, dont le code source est lisible par tous et dont on peut s'assurer qu'il ne transmet pas des informations à notre insu. Il n'a aucune confiance dans des logiciels propriétaires. Exit donc Windows et Mac OS X.
  Plus précisément, ils vont utiliser certaines distributions Linux comme Debian ou encore Tails (utilisé par Edward Snowden lui-même).
- Un **VPN** (Virtual Private Network) : permet de chiffrer toutes vos communications sur Internet en passant par un serveur qui fait relais. C'est un outil de base désormais pour éviter que vos communications soient interceptées. Ce cours sur OpenClassrooms vous permettra d'en savoir plus.
- Tor : un réseau qui permet de surfer anonymement, en chiffrant toutes les données.
- Firefox (ou Chromium) : un logiciel libre pour naviguer sur le Web.
- Des extensions comme uBlock Origin, HTTPS Everywhere et Noscript qui limitent la diffusion de nos informations à des tiers
- GPG : pour chiffrer les échanges e-mails
- Signal : pour la communication chiffrée entre mobiles.
- ... et un certain **Bitcoin**, dont on va reparler…

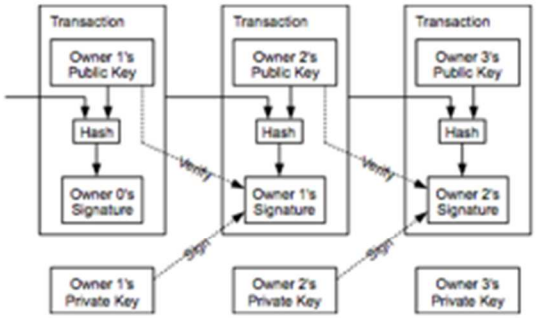
Les crypto-anarchistes ont horreur de tout ce qui est centralisé. Ils préfèrent utiliser des communications « paire à paire » (peer to peer), où les ordinateurs communiquent entre eux sans passer par un serveur central.
Quand on y réfléchit bien, l'argent circule lui aussi de façon très centralisée, puisqu'on le dépose dans des banques. Les banques ont donc un certain pouvoir puisqu'elles voient circuler la plupart des flux financiers. Et c'est justement ce qui dérange les crypto-anarchistes.
Jusqu'à ce qu'un beau jour, un certain Satoshi Nakamoto...

La BLOCKCHAIN

Revenons en 2008. Un certain Satoshi Nakamoto publie en ligne un PDF de moins de 10 pages qui décrit le fonctionnement d'une monnaie qu'il vient d'inventer, le Bitcoin.
Satoshi Nakamoto est un pseudonyme. Personne ne connaît sa véritable identité (même si plusieurs personnes ont dit "C'est moi, c'est moi !"). Actif jusqu'à mi-2010, il a depuis disparu. Qui est-il ? Un marginal, un expert, un alien du FBI ? Sortez le popcorn car on ne sait toujours pas !
Son document est comparable à un papier scientifique : un peu austère dans la forme et évidemment très technique. Vous ne comprendrez probablement pas tout, mais cela vous donnera une idée. Je vous recommande d'y jeter un oeil.
Voici un aperçu du document en question, duquel tout est parti :

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

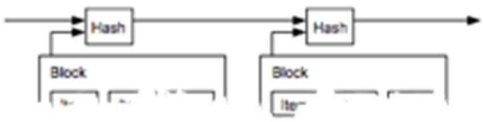


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

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



Aperçu du papier scientifique publié par Satoshi Nakamoto en 2008

Quand j'ai lu ce document, j'ai été étonné que toute l'innovation puisse être résumée en à peine 8 pages. Evidemment, la première fois... je n'ai rien compris.

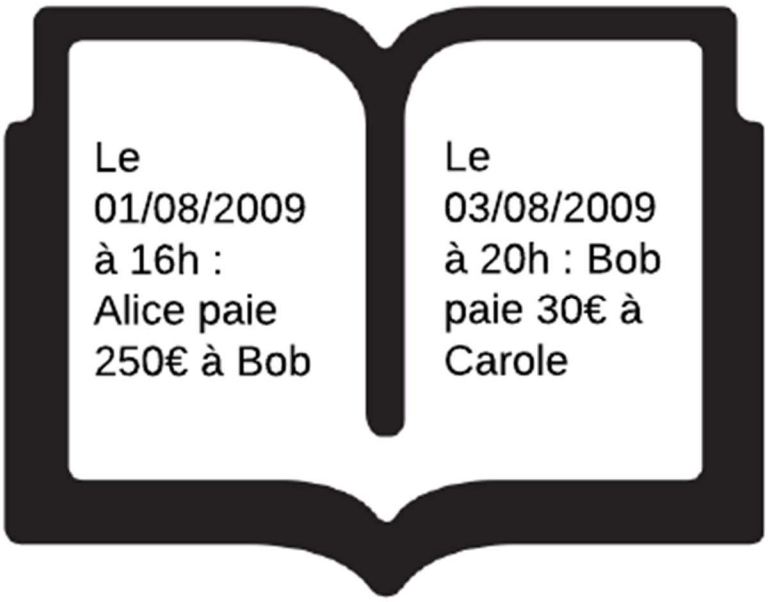
Je relu ce document plusieurs fois, et petit à petit je me suis rendu compte à quel point c'était intelligent. Je ne suis toujours pas un expert du sujet, mais je vais essayer de vous expliquer le concept de façon simple.

Le livre de comptes

Imaginez un livre de comptes. C'est un document dans lequel on écrit tout ce que chacun dépense et achète :

- Le 01/08/2009 à 16h : Alice paie 250€ à Bob
- Le 03/08/2009 à 20h : Bob paie 30€ à Carole
- Le 03/08/2009 à 22h : Alice paie 15€ à Carole
- etc.

En lisant ce document, on voit qui a payé combien à qui.



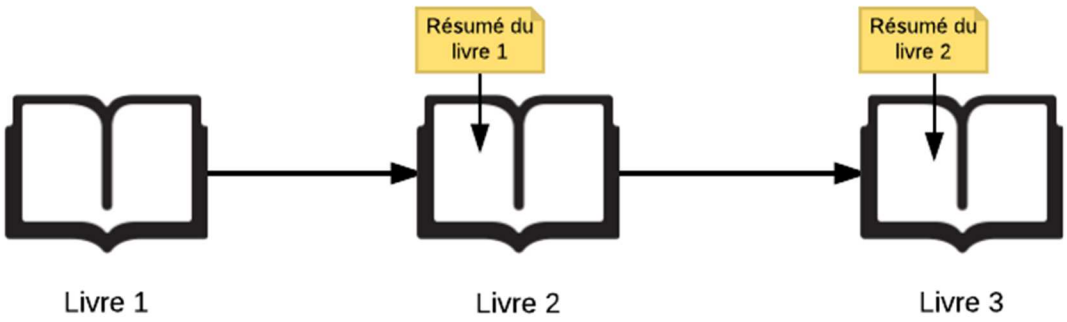
Le livre de compte liste toutes les transactions

Eh bien Bitcoin, c'est ça : un très gros livre de comptes. Je vous le disais, il n'y a pas de "pièces de monnaie" Bitcoin. A la place, il y a ce grand livre de comptes qui dit qui a payé à qui (et quand).
Mais il n'est dit nulle part de combien d'argent chacun dispose ?!
Si ! On sait combien d'argent vous avez car, quelque part dans une des pages du livre, il est écrit que quelqu'un vous a transmis de l'argent. Par exemple, on sait qu'il reste 220€ à Bob puisqu'il a récupéré 250€ d'Alice et donné 30€ à Carole. Simple affaire de déduction !

Une chaîne de livres

La place dans un livre est limitée. Imaginez que notre livre de comptes comporte 1000 pages blanches. Une fois qu'on les a toutes remplies, que fait-on ?

On prend un nouveau livre et on continue ! On va donc avoir des livres numérotés dans l'ordre : Livre 1, Livre 2, Livre 3...
Chaque livre contient un résumé du livre précédent, un peu comme au début des séries télévisés (vous savez, avec la grosse voix qui fait *"Précédemment dans Lost"*). C'est une façon de relier les livres entre eux.

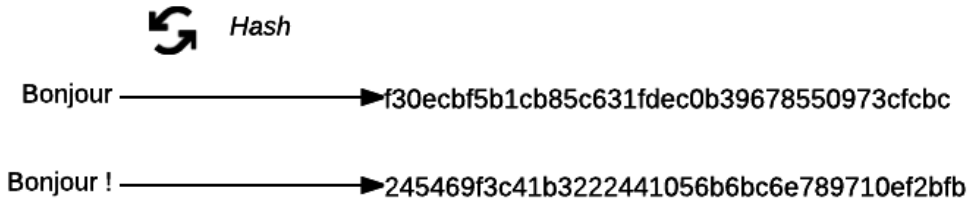


Les livres se suivent et racontent l'histoire. Chaque livre contient un résumé du livre précédent.
Bien entendu, avec Bitcoin, il n'y a pas de vrais livres. A la place, ce sont des fichiers qu'on appelle des "blocs". Les blocs sont les uns à la suite des autres, ils forment une "chaîne de blocs". C'est comme ça que le terme "Blockchain" est apparu.
Le mot Blockchain ne décrit qu'**une petite partie** des concepts du Bitcoin. Ce que je viens de vous montrer là n'est donc qu'une des innovations du Bitcoin : il y en a d'autres dont on va parler plus loin.
Pourquoi tout le monde emploie le mot Blockchain alors ? Principalement parce qu'il y a une "*hype*" très forte actuellement sur ce terme, employé comme un buzzword marketing. Ceux qui l'emploient mélangent parfois beaucoup de concepts, ce qui entretient la confusion. Faites attention donc lorsque vous voyez ce mot : ce n'est pas une formule magique qui va résoudre tous les problèmes de la Terre !
Mais comment faire pour résumer le livre 1 au début du livre 2 ?
C'est là qu'on appelle les Hash à la rescousse.

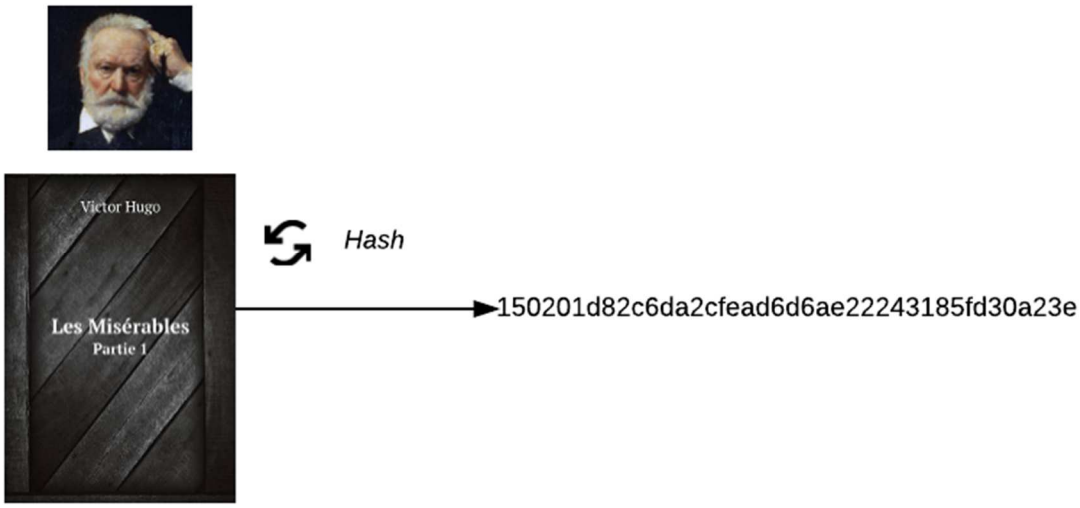
Les Hash

En informatique, et plus particulièrement en cryptographie, on utilise souvent des fonctions de hash. Si vous avez déjà un peu programmé, vous avez dû entendre parler de MD5, SHA1, SHA256... Si ces mots ne vous disent rien, pas de panique : retenez que ce sont des fonctions mathématiques qui transforment n'importe quel contenu sous la forme d'un grand nombre hexadécimal composé de lettres (de "a" à "f") et de chiffres

Ainsi : "**Bonjour**" hashé devient f30ecbf5b1cb85c631fdec0b39678550973cfcbc
Et : "**Bonjour !**" hashé devient 245469f3c41b3222441056b6bc6e789710ef2bfb



Les fonctions de hash transforment un contenu en un nombre qui le représente
Si vous ajoutez ou modifiez une lettre, vous pouvez voir que le résultat est complètement différent (ici, j'ai juste ajouté un point d'exclamation et le hash n'a rien à voir).
Vous pouvez hasher n'importe quoi. Si je hashais par exemple tout le livre "Les Misérables" de Victor Hugo, le nombre produit ne serait pas plus long !



Le résultat si on hashait "Les Misérables" de Victor Hugo
Vous voyez où je veux en venir, non ?

Si on peut hasher les Misérables et obtenir un résultat aussi court, on peut donc hasher notre livre de comptes de la même façon !
Les fonctions de hashage ont une spécificité : elles ne marchent que dans un sens.

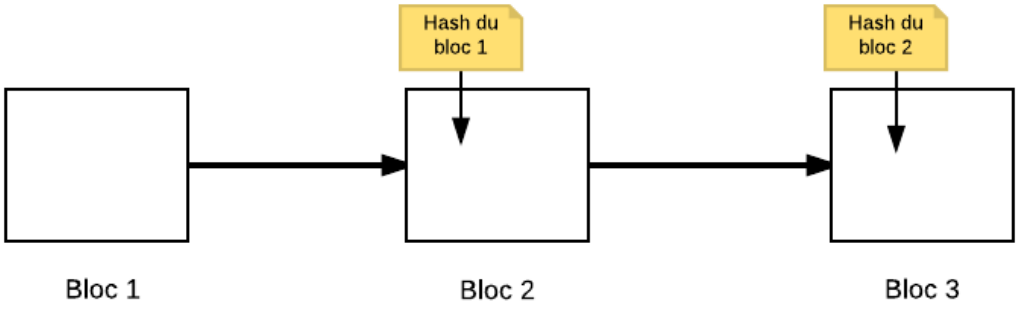
Ainsi, je ne peux rien faire avec le nombre
150201d82c6da2cfead6d6ae22243185fd30a23e
Je ne peux pas l'utiliser pour "retrouver" tout le contenu du livre de Victor Hugo.
Quel intérêt alors ? Ce n'est pas vraiment un résumé du livre du coup ?
150201d82c6da2cfead6d6ae22243185fd30a23e "représente" le livre de Victor Hugo.
C'est une façon de vérifier l'identité du livre, de vérifier qu'il n'a pas été modifié.

Comment peut-on en être sûr ? Eh bien, si vous prenez le livre de Victor Hugo et que vous le passez à la "moulinette" de la fonction de hashage, vous devriez forcément retrouver ce nombre 150201d82c6da2cfead6d6ae22243185fd30a23e (sauf si vous

avez changé une virgule, auquel cas le nombre sera complètement différent comme on l'a vu !). Les hashs nous permettent d'avoir la garantie que le contenu du livre n'a pas été modifié par quelqu'un.

La Blockchain

Voilà qui nous permet donc de représenter notre chaîne de blocs. Mesdames et messieurs, la Blockchain !



La Blockchain est une chaîne de blocs d'informations qui contiennent les hash des blocs précédents
Dans chaque bloc, il y a une ou plusieurs transactions écrites comme "Alice paie 250€ à Bob". En lisant tous les blocs, on peut donc retracer toute l'histoire des échanges en Bitcoin.
Si quelqu'un s'amusait à modifier l'historique (par exemple pour dire dans le bloc 1 "On m'a donné 100 000 Bitcoin", au hasard), cela ne coïnciderait plus avec le hash du bloc 1 contenu dans le bloc 2. Et comme le bloc 3 contient un hash du bloc 2, qui contient lui-même un hash du bloc 1, le bloc 3 serait lui aussi invalide. Un véritable effet de domino !

C'est comme ça (en version simplifiée) que le Bitcoin se protège contre les personnes qui voudraient pirater le système pour s'enrichir.
Dans la pratique, le premier bloc a été créé par Satoshi Nakamoto lui-même le 09/01/2009. Depuis, des nouveaux blocs sont créés toutes les 10 minutes environ. Il y a donc déjà *plusieurs centaines de milliers de blocs dans la blockchain*, et ce nombre ne va faire qu'augmenter dans le futur !

Cela ne va pas faire... trop gros à gérer à la fin ?
Nos ordinateurs ont suffisamment de mémoire. Notre capacité de stockage augmente au fil des années, cela ne devrait donc pas être un vrai problème. Vous allez voir que vous pouvez vous aussi télécharger comme je l'ai fait tout l'historique de la blockchain : il y en a peut-être pour 100 Go environ. C'est beaucoup, mais pas si énorme au final.
Allez, on fait une pause, on respire un grand coup et on passe au chapitre suivant pour en découvrir un peu plus sur le fonctionnement du Bitcoin. Au menu : transferts en réseau, mineurs, preuves de travail et problème de la double dépense.

Le réseau du Bitcoin

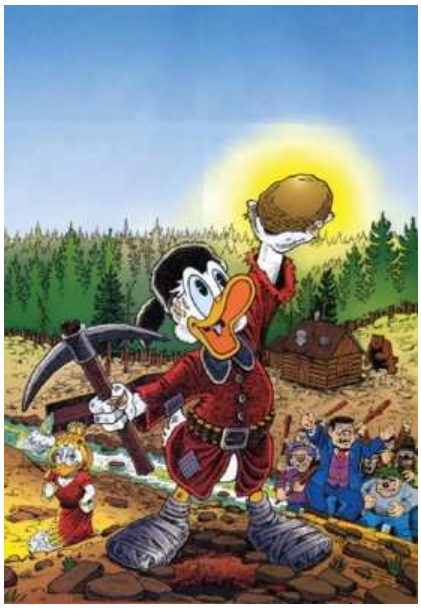
Tout le principe du Bitcoin est de créer un système de monnaie décentralisée. Il ne doit pas y avoir de serveur central. Tout fonctionne donc selon le principe du peer to peer (pair à pair), comme les "*torrents*" qui permettent d'échanger des fichiers entre ordinateurs.
Chaque ordinateur qui possède une copie de la Blockchain est appelé un "noeud" du réseau :

Tous les ordinateurs qui possèdent la Blockchain sont des noeuds du réseau

Vous aussi, vous pouvez ajouter votre ordinateur au réseau ! Il suffit pour cela de faire tourner sur votre machine un logiciel appelé Bitcoin Core. Attention ceci dit : si vous le faites, votre ordinateur va récupérer *toute* la Blockchain depuis les autres ordinateurs, ce qui peut prendre beaucoup de temps et beaucoup d'espace sur votre disque.
C'est toute la force du Bitcoin : il n'y a pas d'autorité centrale, ce sont les ordinateurs qui s'accordent entre eux grâce à l'algorithme complexe du Bitcoin.
Les ordinateurs du réseau vérifient constamment l'historique du Bitcoin. Grâce aux fonctions de hash, ils peuvent prouver tout l'historique des transactions et confirmer que, oui, le 01/08/2009 à 16h, Alice a bien payé 250€ à Bob. Tous les ordinateurs sont donc en quelque sorte les garants de l'intégrité du Bitcoin.
Comment les nouveaux blocs sont-ils créés ?
Par des ordinateurs que l'on appelle les **mineurs**.

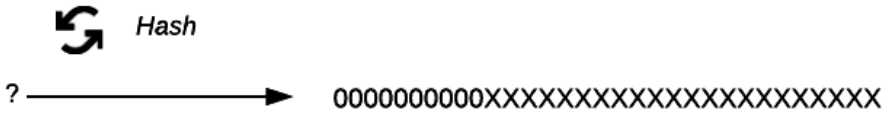
Les mineurs

Lors de la ruée vers l'or au XIXème siècle, les mineurs cherchaient de l'or dans des mines. Comme l'or avait de la valeur, celui qui trouvait de l'or devenait mécaniquement plus riche.



La ruée vers l'or, version Picsou (on a les références qu'on a, hein !)

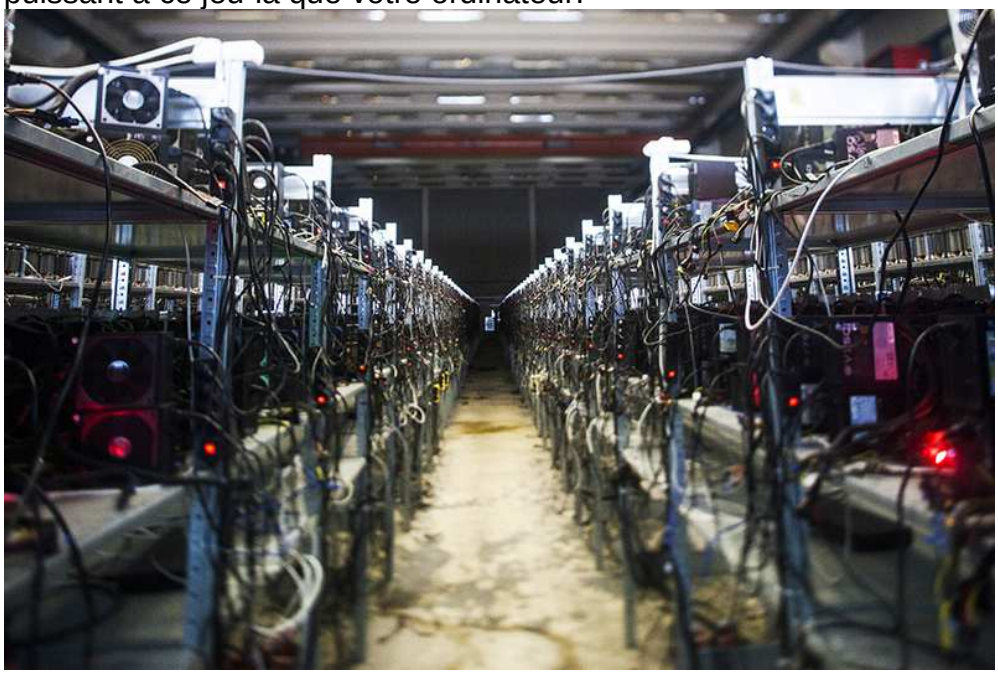
On assiste actuellement à une nouvelle ruée vers l'or... mais virtuelle celle-ci. Pour générer des nouveaux Bitcoin, on fait travailler des ordinateurs inlassablement. Celui qui répond le premier à une question gagne le droit de créer un nouveau bloc dans la Blockchain... et gagne automatiquement de nouveaux Bitcoin.
Que font les ordinateurs qui minent ? Ils essaient de résoudre un problème mathématique. Plus précisément, ils essaient de trouver "le nombre qui, hashé, donne un nombre commençant par une longue série de zéros".



Les mineurs doivent retrouver quel nombre, une fois hashé, commence par une série de zéros

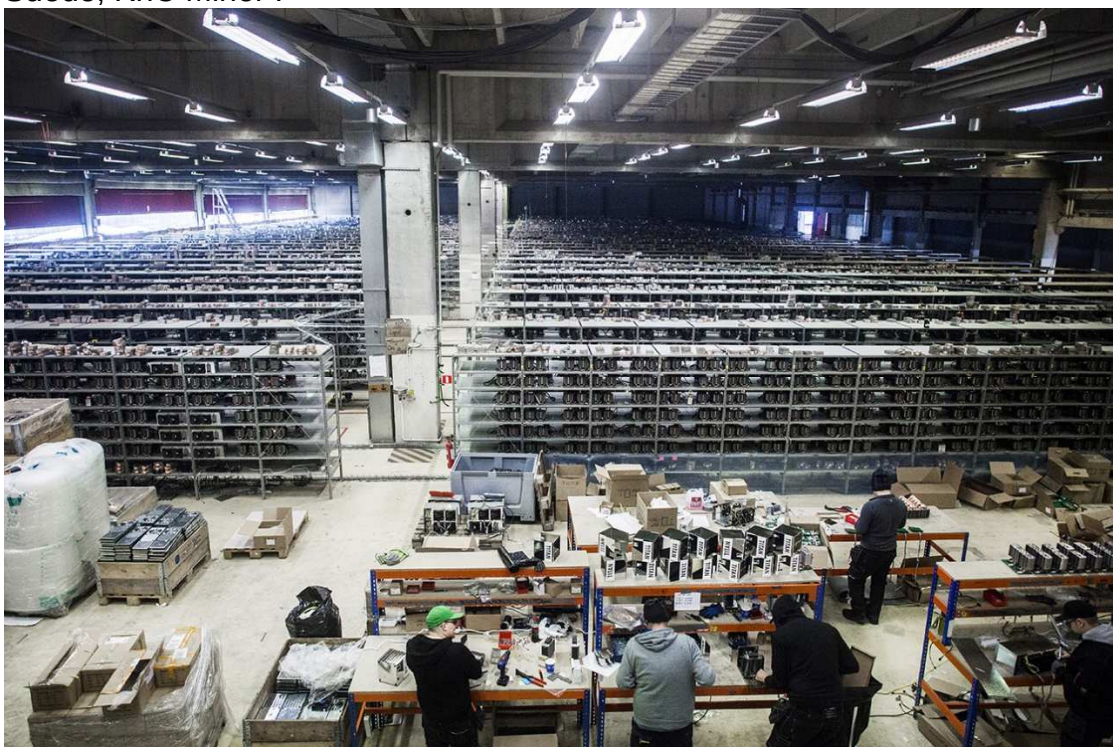
Les fonctions de hashage ne marchent que dans un sens, souvenez-vous. Impossible de partir du hash pour retrouver l'original. Les ordinateurs sont donc condamnés à essayer toutes les possibilités, les hasher, regarder si ça donne un nombre qui commence par beaucoup de zéros... et recommencer si ce n'est pas le cas.
Ca consomme énormément de temps et d'énergie aux ordinateurs ! Mais lorsque tous les ordinateurs du réseau Bitcoin s'y mettent, ils parviennent à trouver une réponse toutes les 10 minutes. La difficulté est automatiquement ajustée en fonction du nombre d'ordinateurs en train de hasher, afin qu'un nouveau bloc soit généré en moyenne toutes les 10 minutes.
A chaque fois, c'est un peu comme gagner à la loterie, puisqu'un nouveau bloc est créé... et surtout quelqu'un est récompensé par des Bitcoin.
Combien gagne le mineur qui trouve la réponse ?
Ca dépend. Actuellement, le mineur "gagnant" récupère 12,5 BTC (Bitcoin), ce qui vaut à l'heure où j'écris ces lignes un peu plus de 7500€. Plus le temps passe, plus il est

difficile de miner des Bitcoin et plus la récompense devient petite. On a même déjà calculé qu'il n'y aurait plus de nouveaux Bitcoin à partir de l'année 2140.
Woaw ?! Je peux gagner 7500€ avec mon ordinateur si je mine des Bitcoin ? Où est-ce que je peux faire ça ? vite !
Alors oui, si en théorie vous pouvez vous aussi miner des Bitcoin avec votre ordinateur, en pratique aujourd'hui vous avez une chance infinitésimale de réussir. Les mineurs sont désormais très organisés et utilisent du matériel spécifique dédié bien plus puissant à ce jeu-là que votre ordinateur.



Les mineurs utilisent du matériel dédié aujourd'hui - Crédits Stefan Bladh

Et les mineurs sont très organisés, dans de très grands entrepôts. Voici l'un d'eux en Suède, KnC Miner :



Les mineurs ont plus de moyens que vous on dirait (ici KnC Miner) - Crédits Stefan Bladh

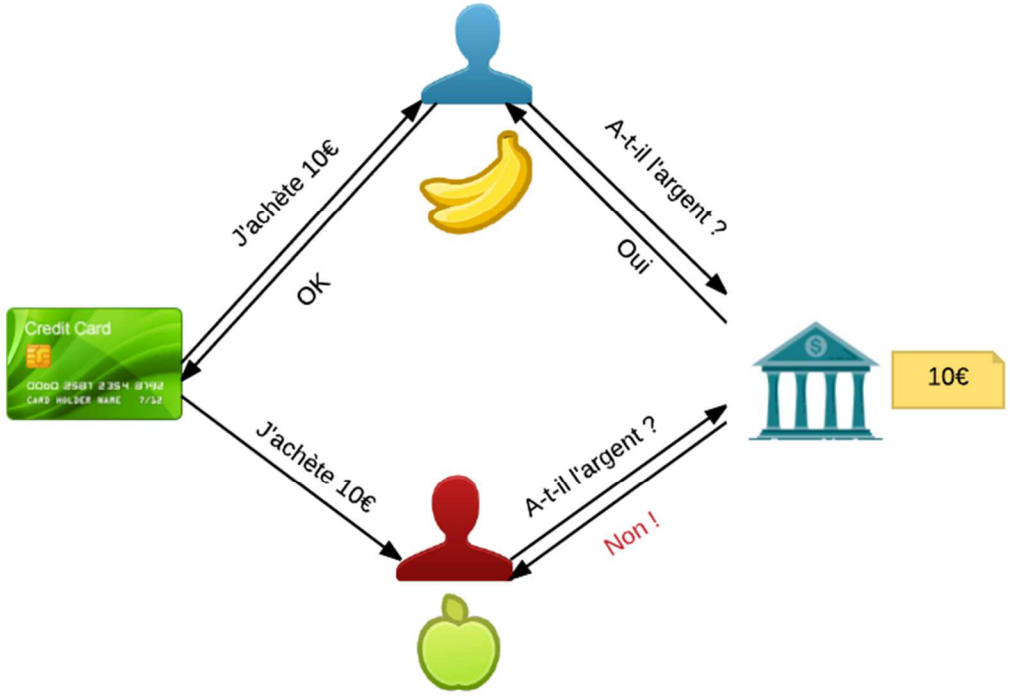
Et ça, c'est juste *un* entrepôt dédié au minage des Bitcoin au nord de l'Europe. Il y en a d'autres. En pratique, de très nombreux mineurs sont situés en Chine où l'électricité est moins chère (et ils sont beaucoup plus nombreux). Bref, la compétition est rude, compris ?

Des mineurs de Bitcoin en Chine (ici HaoBTC) - Crédits Eric Mu

S'il y a autant d'ordinateurs qui travaillent, c'est parce qu'ils sécurisent le système avec leurs calculs. Ils fournissent des *proofs of work* (preuves de travail) : les calculs permettent de rendre quasi-impossible de falsifier l'historique de la blockchain pour faire croire que vous avez plus d'argent qu'en réalité. Le système est fait de telle sorte que, si vous vouliez pirater la blockchain, il vous faudrait contrôler plus de 50% de la puissance de calcul de tous les ordinateurs qui minent sur la planète !

Le dilemme de la double dépense

L'un des plus gros défis du Bitcoin (et de toute monnaie d'ailleurs), c'est celui de la **double dépense**. On veut éviter qu'une personne puisse faire croire qu'elle a plus d'argent qu'en réalité. Dans la pratique, ça veut dire qu'on veut éviter qu'on puisse dépenser 2 fois une même quantité d'argent.
Imaginez. Vous avez 10€ en tout sur votre compte en banque (c'est pas beaucoup, je sais). Vous allez acheter 10€ de bananes chez un vendeur avec votre carte bancaire, et en même temps un complice tente d'acheter 10€ de pommes au magasin d'en face avec une de vos autres cartes bancaires. Il y aurait un vrai problème si vous pouviez acheter les bananes et les pommes, car vous ne disposez que de 10€.
Que se passe-t-il en réalité ? C'est la banque qui joue ici le rôle d'intermédiaire de confiance pour éviter cette situation. Elle va accepter la première transaction (vous allez pouvoir acheter des bananes), mais elle va refuser la seconde. Le vendeur de pommes refusera donc de vous les vendre en voyant que la transaction a été refusée par la banque.



Comment la banque joue le rôle d'intermédiaire de confiance

Voici donc ce qui se passe :
- (Vous) "Eh, j'achète 10€ de bananes"

- (Vendeur 1) "Je vérifie que vous avez l'argent en demandant à votre banque... Ok c'est bon, voici vos bananes !"
Et en même temps :
- (Complice) "Eh, j'achète 10€ de pommes"

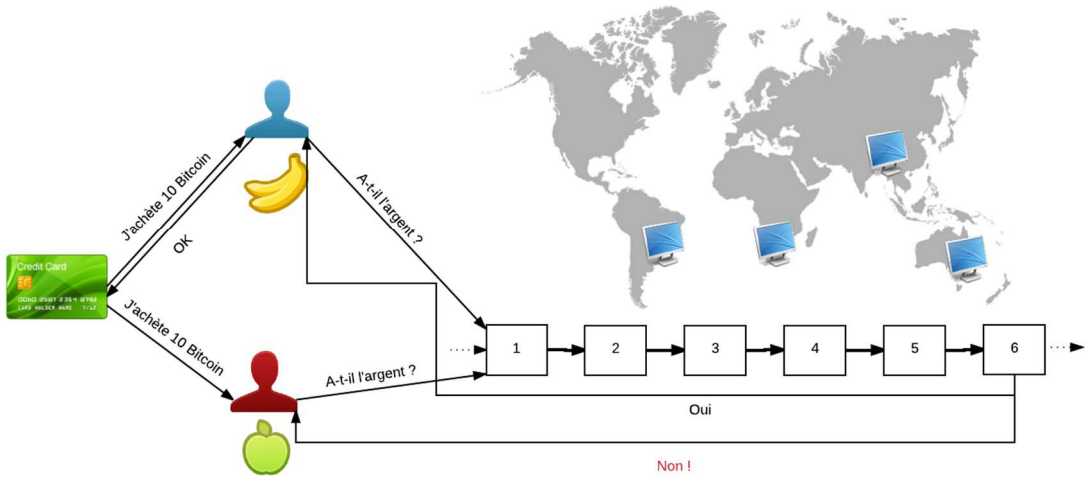
- (Vendeur 1) "Je vérifie que vous avez l'argent en demandant à votre banque... Ah non, désolé vous n'avez pas cet argent."
C'est donc à ça que servent les banques ? Confirmer combien il y a d'argent à tout instant et éviter qu'un vendeur se fasse avoir ?
Entre autres, oui. Ici, comme la banque est le "nœud" central, elle n'autorise qu'une transaction à la fois, dans un *ordre* précis. Ainsi, elle va accepter la première demande qu'elle reçoit, mais pas la seconde (même si les deux lui arrivent à quelques millisecondes d'écart ou pile en même temps).
Et comment peut fonctionner le Bitcoin alors, vu qu'il n'y a pas de banque impliquée?

Ca paraît un peu fou, mais le Bitcoin laisse le réseau des ordinateurs décider entre eux. C'est la majorité qui l'emporte. Si une majorité d'ordinateurs décide que vous avez acheté les bananes en premier, alors le vendeur de pommes verra que vous n'avez plus l'argent et refusera la transaction.

En pratique avec le Bitcoin, on doit attendre qu'une transaction soit *validée*. La validation d'une transaction n'est pas instantanée avec le Bitcoin. On considère qu'il faut attendre que plusieurs blocs aient été ajoutés à la blockchain pour confirmer la transaction (ce qui peut prendre quelques dizaines de minutes !). Ca veut dire qu'à

partir du moment où vous payez, le vendeur va attendre l'arrivée de nouveaux blocs pour être sûr que vous n'avez pas essayé de tromper le système.
Plus il y a eu de nouveaux blocs, plus on est sûr que vous aviez bien l'argent. Si le vendeur choisit de ne pas attendre, il prend un risque que vous l'ayez trompé.
Bien sûr, vous pourriez faire dire à votre ordinateur que vous aviez plus d'argent, mais personne sur le réseau ne vous croira. A moins de contrôler au moins 51% des ordinateurs du réseau et refaire tous les calculs des hashs (ce qui demanderait une puissance *énormissime*), vous ne pourrez pas rétroactivement influencer le cours de l'histoire.
Tous ces ordinateurs qui minent sont donc un rempart contre le piratage de la blockchain. Ils évitent que quelqu'un puisse réécrire le "livre de comptes" (la blockchain) à son avantage.

J'ai essayé à ma manière de résumer le concept dans ce schéma (qui simplifie beaucoup les choses, mais ça vous donnera une idée du principe !) :



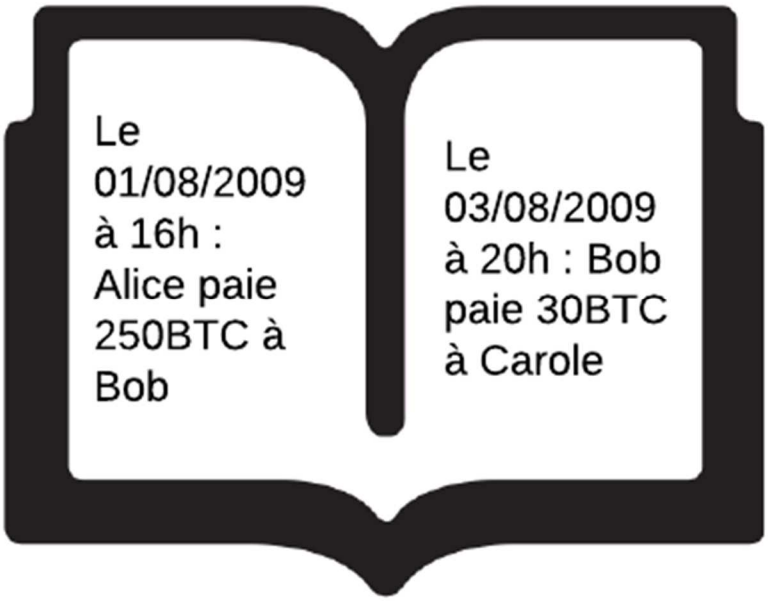
Validation d'une transaction sur le réseau Bitcoin

Chaque vendeur va voir qu'on lui offre de l'argent, mais il va attendre que de nouveaux blocs aient été ajoutés à la blockchain (ici 6 blocs) pour être sûr que le réseau d'ordinateurs a accepté la transaction. C'est comme ça que le réseau d'ordinateurs peut remplacer la banque !

Vous le savez maintenant : il n'y a pas de pièces "physiques" de Bitcoins. Alors, comment s'échange-t-on des Bitcoins d'un compte à un autre ?

La Blockchain et le livre de comptes

En son coeur, Bitcoin stocke les transactions dans un grand livre de comptes qu'on appelle la Blockchain. Toutes les transactions depuis le premier jour sont visibles par tout le monde.



Dans la Blockchain, on retrouve qui a payé combien à qui en Bitcoins (BTC)

Si vous vous appelez Bob, tout le monde sait donc que vous avez maintenant 220 BTC (250 BTC donnés par Alice, et 30 BTC que vous avez donnés à Carole). Pas besoin de pièces de monnaie, c'est écrit dans la Blockchain.
En fait, dans la Blockchain, il n'y a pas nos vrais noms. A la place il y a des adresses qui ressemblent à ça : 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

On y reviendra un peu plus loin

La Blockchain est publique non ? Elle est partagée entre tous les ordinateurs du réseau. Donc, si je m'appelle Bob, qu'est-ce qui m'empêche d'y écrire "Alice me donne 500 BTC" ?
Satoshi Nakamoto, le créateur du Bitcoin, y a bien entendu pensé le premier. Pour empêcher ça, il a stipulé que toutes les transactions devaient être **signées** dans la Blockchain. Donc si vous essayez d'écrire "Alice donne 500 BTC à Bob", les autres ordinateurs ne vous croiront pas tant qu'ils n'auront pas vu la signature d'Alice.
Evidemment, vous vous en doutez, les signatures ne se font pas sur un bout de papier ici. Je vous présente donc... la signature électronique grâce à la cryptographie asymétrique !

La signature électronique avec la cryptographie asymétrique

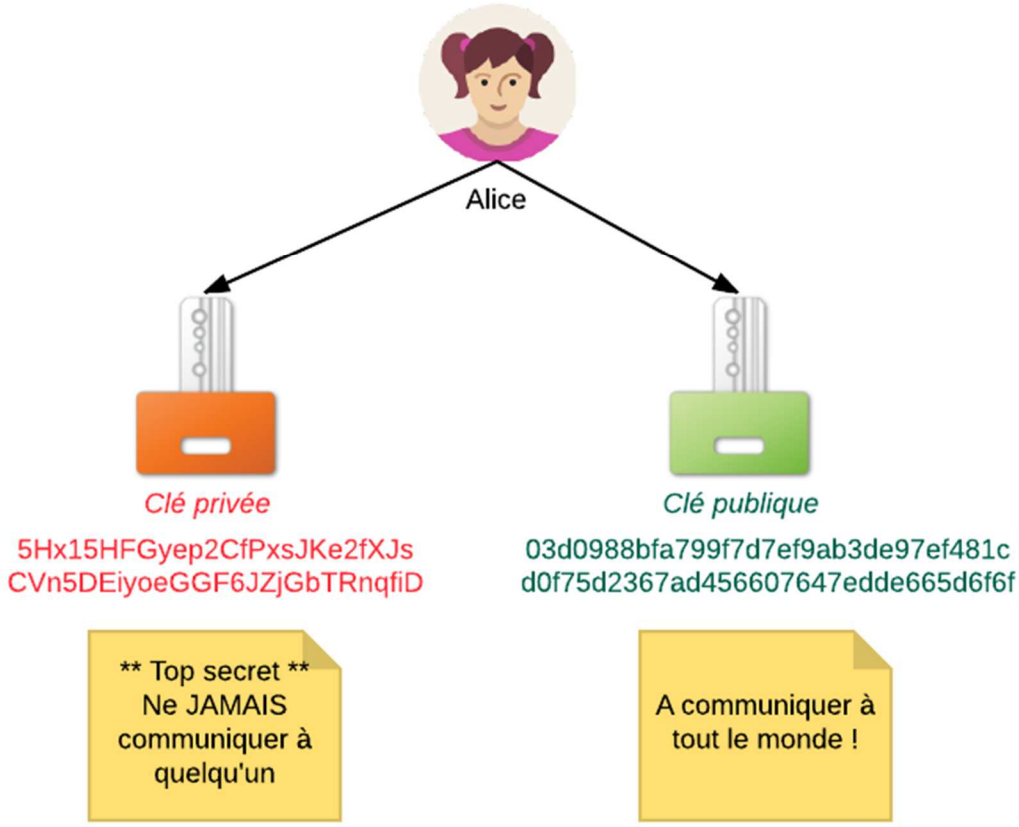
La cryptographie asymétrique n'a rien de nouveau : c'est ce qui permet de sécuriser les échanges sur Internet. Par exemple, c'est ce qui permet d'éviter que quelqu'un intercepte votre numéro de carte bancaire quand vous payez sur un site. Tous les sites qui commencent par HTTPS utilisent ce procédé.
La cryptographie asymétrique peut servir à deux choses :

- **Chiffrer des informations** : permet de cacher ces informations aux yeux d'autres personnes. C'est ce qu'on fait sur les sites HTTPS.
- **Signer des messages** : permet de s'assurer qui est à l'origine du message.

Ah ! On y vient, vous voyez. On peut utiliser ce truc pour signer, donc authentifier l'expéditeur d'un message.
Alors comment ça marche ? Chaque personne génère un couple de clés à l'aide d'un algorithme mathématique :

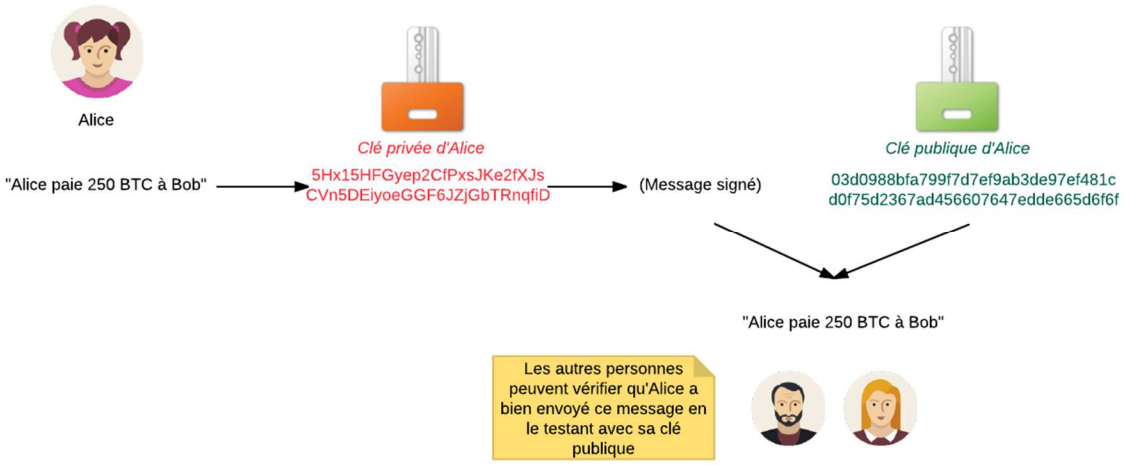
- **Une clé privée**, qui ne doit être communiquée à *personne*
- **Une clé publique**, qui peut et doit être communiquée à *tout le monde*

Par exemple, si Alice veut pouvoir signer ses échanges, elle va avoir besoin de se créer sa propre paire de clés :



Alice génère une paire de clés : une publique et une privée

Les clés vont ensemble, elles sont liées l'une à l'autre.
Si Alice veut signer un message (ex :"Je donne 500 BTC à Bob"), elle le passe dans une moulinette mathématique qui chiffre ce message à l'aide de sa clé privée.
Pour le déchiffrer, et donc obtenir la preuve qu'elle est bien bien l'auteur du message, les autres personnes du réseau vont utiliser sa clé publique. Si on arrive à déchiffrer son message à l'aide de sa clé publique, alors on sait que c'était bien elle.

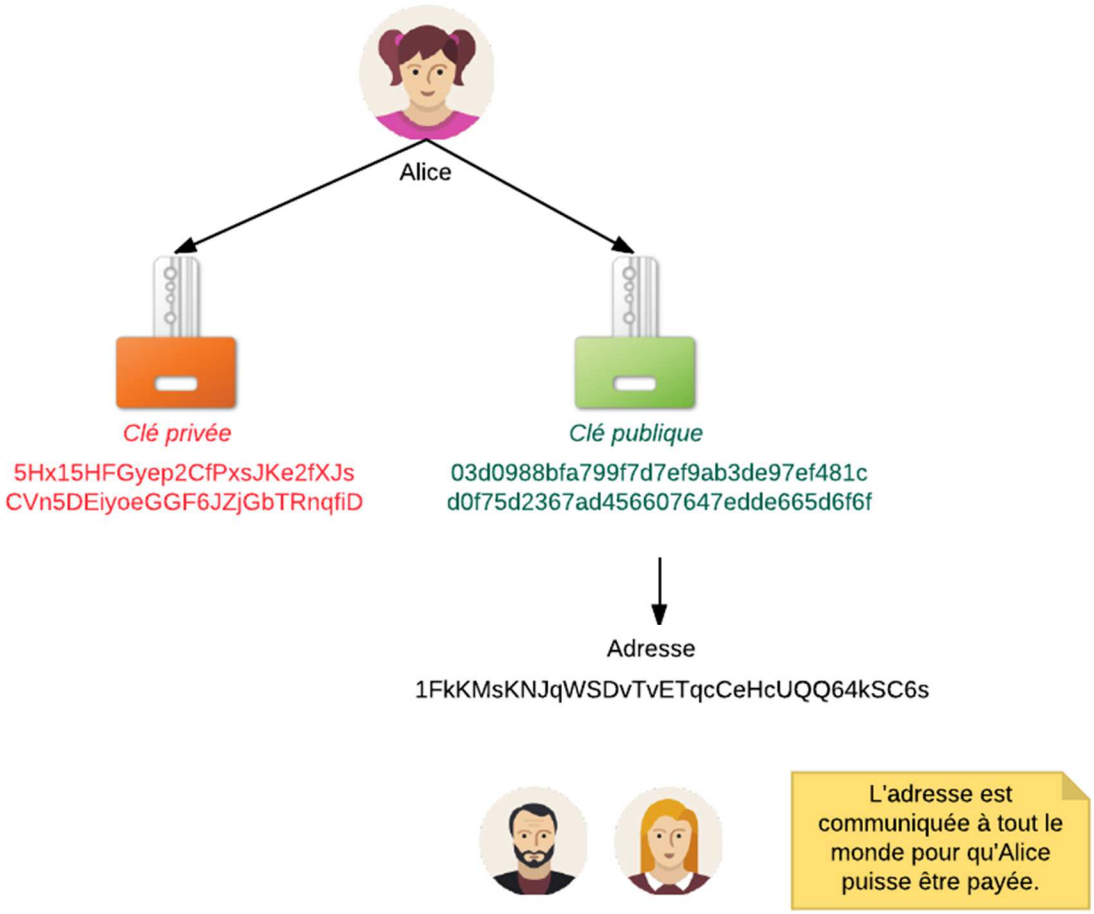


Si Alice envoie un message, elle le signe avec sa clé privée et tout le monde peut vérifier que c'était elle grâce à sa clé publique !

Voilà pour ce petit aparté sur la cryptographie asymétrique. Si vous connaissiez déjà le principe, un petit rappel ne fait jamais de mal. Si vous ne connaissiez pas... je me doute que ça fait beaucoup d'informations à la fois. Faites-moi confiance pour le moment, retenez les grandes lignes, vous aurez tout le temps de vous renseigner plus en détail sur cet univers passionnant après si vous voulez.

Votre adresse dans le monde des Bitcoins

Revenons à nos moutons.
Vous avez compris que seule Alice peut dépenser son argent parce qu'elle est la seule à posséder sa clé privée. C'est ce qui lui permet de signer ses messages.
Si quelqu'un d'autre mettait la main sur la clé privée d'Alice, il pourrait hurler à la planète entière qu'Alice vient de lui donner tout son argent, et ce serait trop tard. Il n'est pas possible d'annuler une transaction en Bitcoin. Vous pourrez faire `Ctrl` + `Z` autant de fois que vous voudrez, quand l'argent est parti il est parti.
Voilà pourquoi il faut impérativement protéger sa clé privée. Si quelqu'un vous la vole, parce que votre ordinateur est infecté par un virus par exemple, bye bye les Bitcoins !
Dans la pratique, il n'y a pas les noms des personnes sur la Blockchain. On se transfère l'argent d'une adresse à une autre.
L'adresse est tout simplement une version condensée de la clé publique. Quand Alice génère une paire de clés, elle génère donc automatiquement une adresse à partir de sa clé publique. C'est ce qu'elle communique au monde entier pour dire "*Si vous voulez me payer, c'est à cette adresse !*".

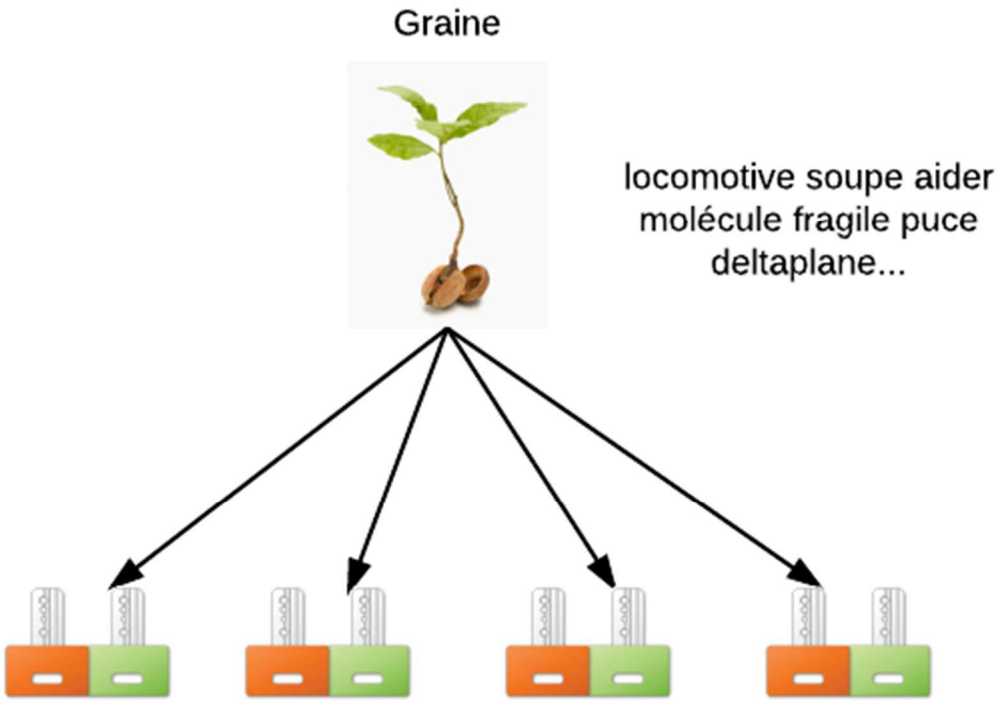


L'adresse est communiquée par Alice à tout le monde pour qu'elle puisse être payée

Vous verrez qu'il existe des logiciels de portefeuilles de Bitcoins... mais ils ne stockent pas d'argent (puisque l'argent en circulation est écrit dans la Blockchain). Ce que les portefeuilles stockent, ce sont des paires de clés comme celle-ci. En résumé, quand vous vous baladez avec vos clés, vous vous baladez avec votre argent.

Vous n'aurez pas une adresse mais plusieurs

Allez, une dernière info et on va arrêter là sinon j'ai peur de vous saturer l'esprit.
En réalité, vous n'aurez pas une adresse mais plusieurs. En effet, il est dangereux de n'utiliser qu'une seule adresse. Pourquoi ? Parce que, vu que la Blockchain est publique, tout le monde pourrait savoir combien d'argent vous avez. Je suis sûr que vous ne seriez pas très à l'aise si l'univers entier savait tout de vos finances !
Généralement, on conseille d'utiliser une seule fois une adresse pour recevoir un paiement. Ensuite, vous devriez utiliser une autre adresse.
Pour avoir plusieurs adresses, il va falloir générer plusieurs paires de clés. Les logiciels portefeuilles de Bitcoins savent faire ça très bien pour nous. Ils utilisent même un procédé très malin pour générer une infinité de paires de clés : ils partent d'une série de mots aléatoires. Cette série de mots est appelée **graine** (*seed*). Elle est unique et facile à mémoriser. Par exemple :
locomotive soupe aider molécule fragile puce deltaplane...
Cette liste de mots nous permet de générer autant de paires de clés qu'on veut, donc autant d'adresses pour se faire payer. Et comme cela inclut les clés privées, cela veut aussi dire que la liste de mots nous donne la possibilité de payer avec notre argent.



La graine (liste de mots) nous permet de générer nos paires de clés

La graine (liste de mots) est donc ce qu'il y a de plus précieux ! Toutes les paires de clés en dérivent.
Quiconque possède la liste de mots possède l'argent. Autant vous dire qu'il va falloir la stocker en lieu sûr !

Voilà, vous en savez *un peu plus* sur le monde du Bitcoin et de la Blockchain. Passionnant non ? Et encore, on ne fait que couvrir les choses en surface. Comme je vous le disais, je trouve ça à la fois extraordinairement complexe et intelligent.

Dans la prochaine partie, on va rentrer dans le concret : on va acheter nos premiers Bitcoins, les stocker dans un portefeuille (avec une graine, des clés, des adresses et tout !) et bien sûr... on va les dépenser.

On va faire un peu d'exploration : on va parcourir la Blockchain en temps réel pour voir ce qui est écrit dedans !

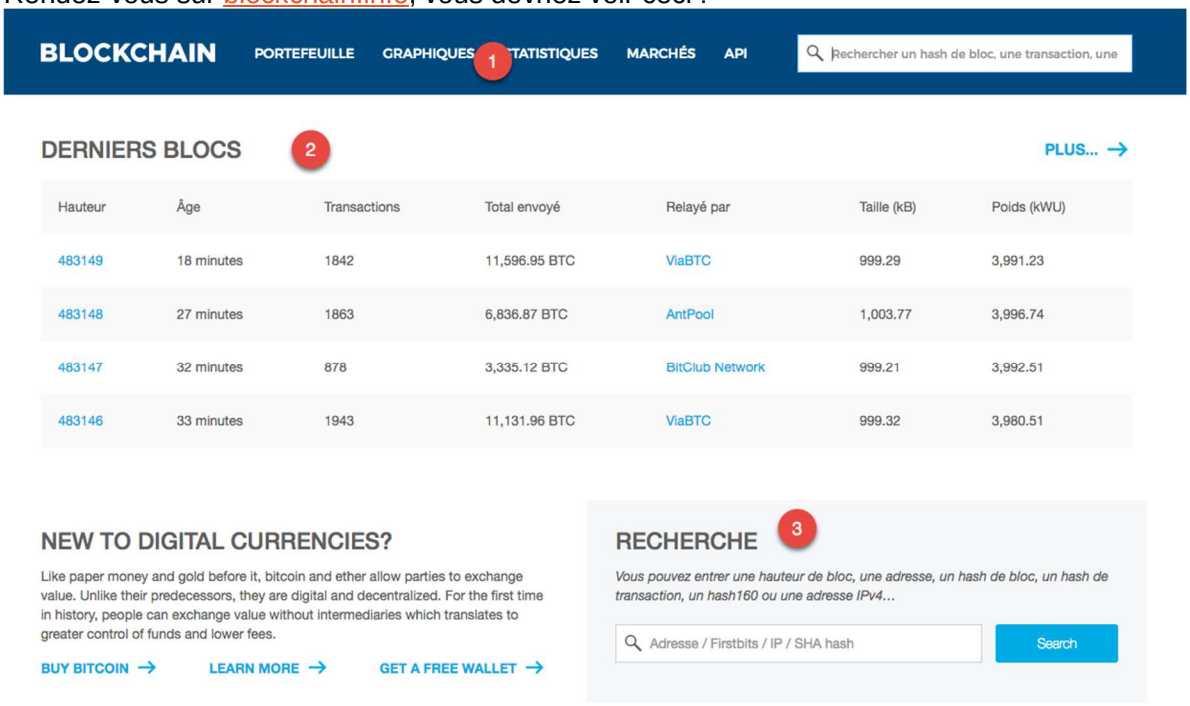
Tout le monde peut accéder à la Blockchain du Bitcoin car elle est publique : c'est une information partagée par tous les ordinateurs du réseau.

Vous pouvez même télécharger votre propre copie de la Blockchain en téléchargeant par exemple le logiciel officiel Bitcoin Core. Cependant, la Blockchain est maintenant très grosse et peut prendre des dizaines de Go (et donc des semaines) à télécharger.

Heureusement, des sites nous permettent de parcourir la Blockchain de façon plus visuelle et plus rapide.

Accueil de Blockchain.info

Rendez-vous sur blockchain.info, vous devriez voir ceci :



Accueil du site Blockchain.info

Sur la page d'accueil, 3 sections peuvent vous intéresser :

1. Une section "Graphiques" qui vous donne des informations visuelles sur la Blockchain
2. La liste des derniers blocs de la Blockchain
3. Un module de recherche pour retrouver une transaction, via une adresse par exemple

Les graphiques

Le site nous propose plus de graphiques qu'il ne nous en faut. Arrêtez-vous notamment sur le graphique de la capitalisation boursière en sélectionnant l'échelle "de tous les temps" en bas :

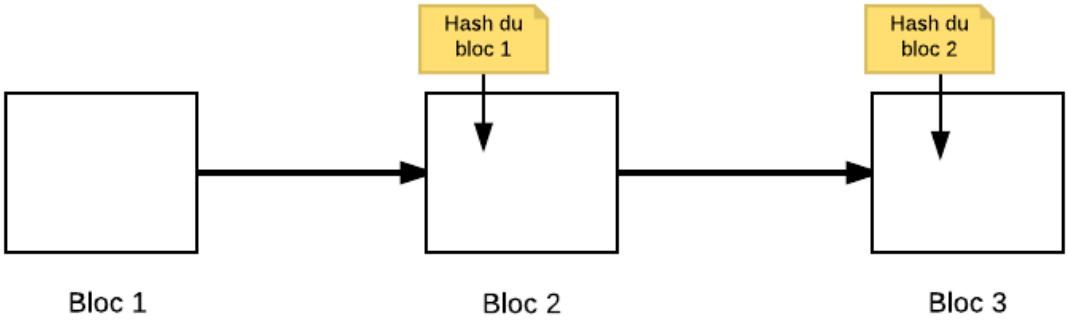
Capitalisation boursière des Bitcoins au fil du temps (valeur totale des Bitcoins)

Ce graphique est, je trouve, assez passionnant. Il indique combien valent l'ensemble des Bitcoins au fil du temps. Ici, on y voit donc les tous premiers Bitcoins échangés en Janvier 2009 jusqu'à nos jours.
Pour obtenir ce graphe, il suffit de multiplier le prix moyen du Bitcoin par le nombre de Bitcoins en circulation. Vous voyez donc que, tout à droite du graphe, il y a l'équivalent des **dizaines de milliards de dollars de Bitcoins en circulation**.

Ce nombre va augmenter ou diminuer au fil du temps. Comme vous pouvez le voir, jusqu'en 2013 la valeur était tellement faible qu'elle a ici l'air à zéro. Puis, la valeur a fortement augmenté.
Un autre graphe très intéressant est le prix du marché (en dollars). Il vous indique combien valait un Bitcoin à chaque date. A une époque, on pouvait acheter 1 BTC pour environ 10$! Ce temps paraît lointain.

Les blocs

L'accueil de blockchain.info met principalement en avant les derniers blocs du réseau. Vous vous souvenez de quoi il s'agit ? C'est cette liste de "livres de comptes" qui se suivent les uns les autres. Dans chaque livre (bloc) on a écrit qui a payé combien à qui.



Rappel : la blockchain est une... chaîne de blocs. Les transactions sont écrites dedans.

Tous les blocs sont numérotés. Au moment où j'ai pris ma capture d'écran au début de ce chapitre, on en était au bloc n° 439800, généré il y a moins d'une minute. Dedans, il y avait 1914 transactions pour un total de plus de 7000 BTC échangés.

Hauteur	Âge	Transactions	Total envoyé	Relayé par	Taille (kB)
439800	1 minute	1914	7,050.55 BTC	ViaBTC	999.21

Les infos sur le dernier bloc

Vous noterez que le bloc fait une taille de 999 Ko (soit 1 Mo). Par définition, les blocs ne peuvent pas faire plus de 1 Mo : cela veut dire qu'il est plein et qu'on ne peut plus y ajouter de transactions. C'est un *gros* sujet de débat dans le monde du Bitcoin : tous les blocs sont plein à craquer, les transactions mettent donc du temps à être propagées car elles attendent qu'un nouveau bloc soient libre. Faut-il étendre la taille de base d'un bloc ? Certains pensent que oui, d'autres que non, surtout pas, car ça rendrait le réseau plus centralisé. On y reviendra !

Bloc #439800

Sommaire	
Nombre de transactions	1914
Somme des outputs	7,050.55066094 BTC
Volume estimé des transactions	2,310.02515733 BTC
Frais des transactions	0.62680049 BTC
Hauteur	439800 (Chaîne principale)
Date (timestamp)	2016-11-20 14:34:07
Date de réception	2016-11-20 14:34:07
Relayé par	ViaBTC
Difficulté	281,800,917,193.2
Morceaux	402908884
Taille	999.208 KB
Version	0x20000000

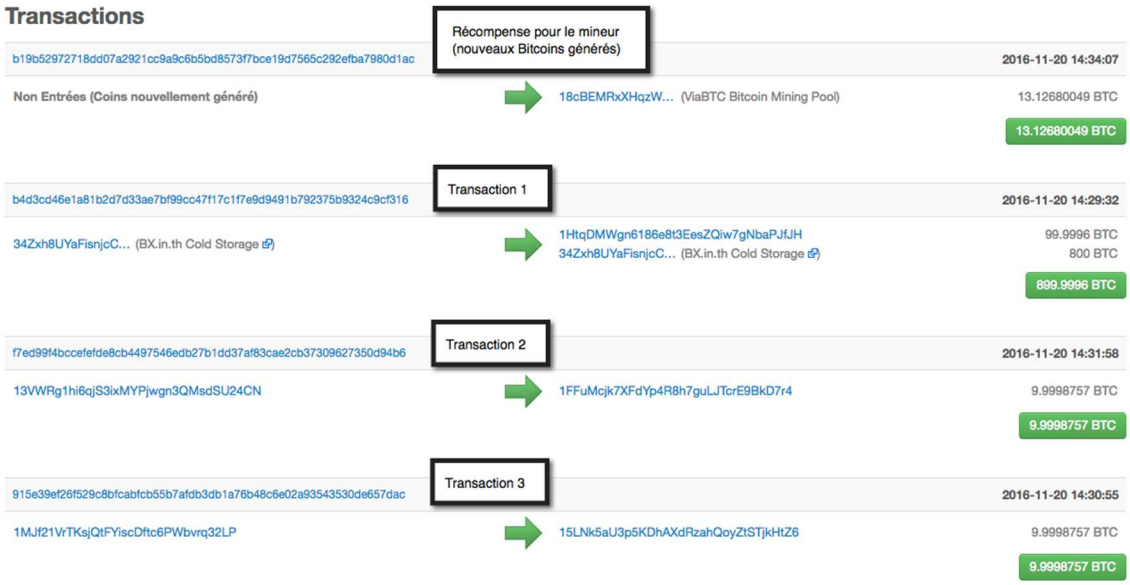
Hashes	
Hash	00000000000000001c6368aeaf99003708c2a941521959cbc23a92fc2ca7b13
Bloc précédent	0000000000000000001639e49acf658f2ee2fbc38be554d6d3efd237a5c6584ee
Bloc(s) suivant(s)	000000000000000003267f54632a7c547e119bd7767dcabbb951e87340324624
Merkle racine	a5ccb2d54dc0cbed28d0bc4595cd4add7970aa3a60e6874d07473869bd17b1d7

Propagation sur le réseau (Cliquez pour voir)

Informations détaillées sur le bloc 439800

Vous pouvez voir où le bloc a été généré (ici, il semble que l'adresse précise ne soit pas connue car ça tombe au beau milieu de l'océan !). Vous avez la date du bloc et aussi le hash qui le représente en haut à droite.
Vous vous souvenez quand je vous disais que les mineurs cherchaient des hash commençant par un certain nombre de zéros ? C'est pour cela que le hash ressemble à ceci :
00000000000000001c6368aeaf99003708c2a941521959cbc23a92fc2ca7b13
Vous avez aussi l'identifiant du mineur qui a créé ce bloc (en ayant trouvé ce hash). Ici, il s'appelle "ViaBTC".

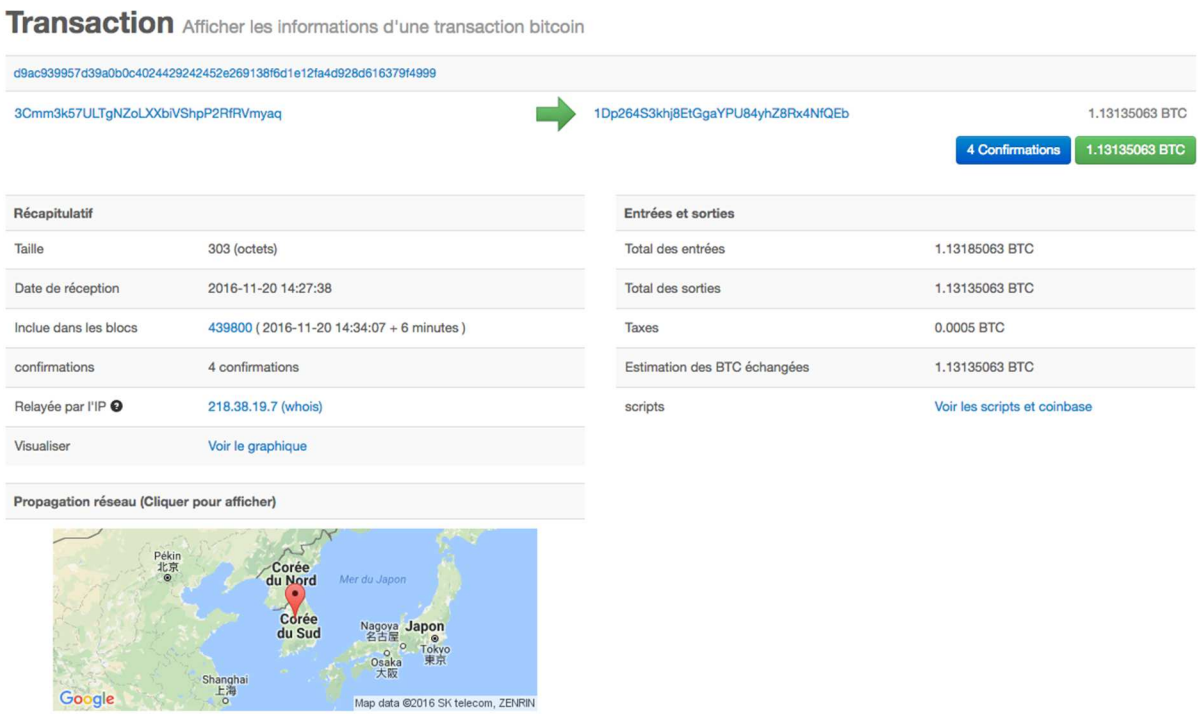
Descendez plus bas sur la page pour voir... tous les échanges de Bitcoins au sein de ce bloc ! C'est là qu'on voit notamment "Alice a donné 250 BTC à Bob" par exemple (sauf qu'on voit des adresses et pas des noms). Vous verrez la quantité d'argent qui s'échangent d'une main à une autre, c'est impressionnant ! 😲



Aperçu des transactions dans le bloc

La première transaction est, par définition, une récompense donnée au mineur qui a trouvé le hash magique qui commence par une série de zéros. Ici, le mineur a gagné 13 BTC, soit environ 9000 € au cours du moment. Pas mal !
A gauche, vous avez l'adresse qui émet des Bitcoins et à droite l'adresse qui en reçoit. On peut voir par exemple sur la transaction 3 qu'une adresse a envoyé à une autre près de 10 BTC. Il n'y a pas les noms des personnes, mais par contre tout le monde sait maintenant qu'une adresse vient de recevoir 10 BTC. Si vous cliquez sur cette adresse, vous pouvez ensuite voir à qui elle a envoyé de l'argent à son tour.

Les transactions

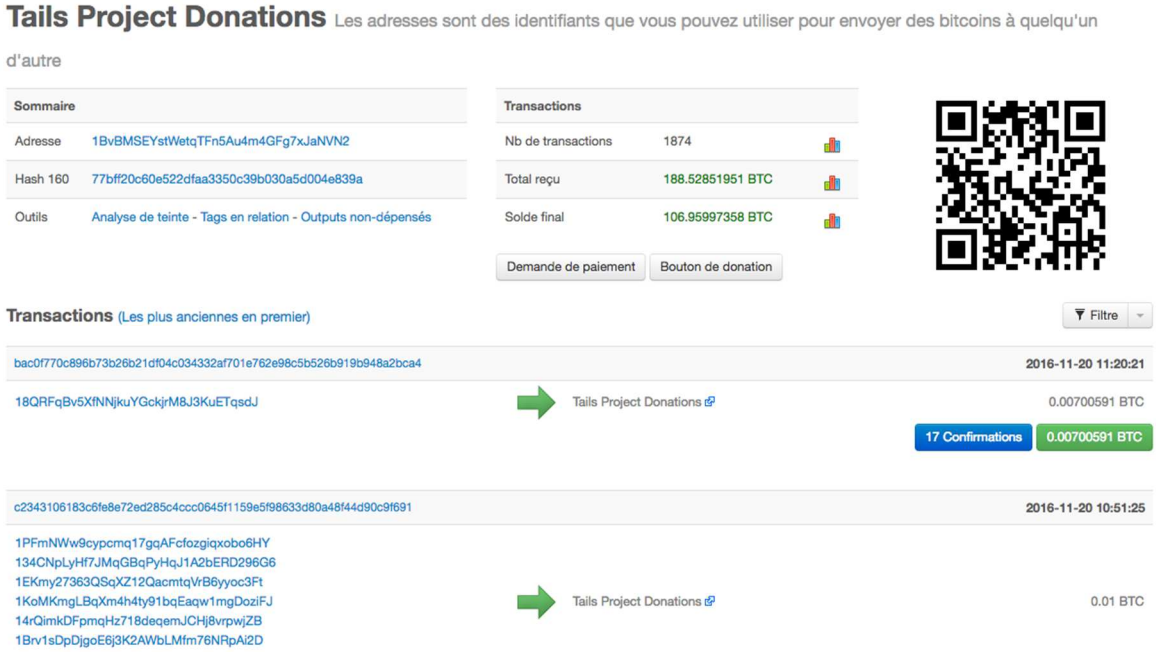


Détails d'une transaction

Ici, on voit que cette transaction a eu lieu en Corée du Sud par exemple. On sait que 1,13 BTC ont changé de mains.
On voit enfin combien de fois la transaction a été confirmée (ici 4 fois au moment de ma capture d'écran). Plus il y a eu de confirmations, plus on est sûr que l'argent a bien changé de mains. Cela nous permet d'éviter que la personne puisse tricher en dépensant plusieurs fois cet argent, souvenez-vous.

Recherche

Enfin, vous pouvez rechercher une adresse ou un numéro de transaction dans le moteur de recherche de blockchain.info. Essayez par exemple de rechercher l'adresse `1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2` et vous allez tomber sur cette page :



Détails d'une adresse sur le réseau Bitcoin

Cette adresse correspond à "quelqu'un". D'habitude on ne sait pas qui, mais celle-ci est un peu particulière car elle indique clairement qui elle est : "Tails Project Donations". Il s'agit donc probablement d'une adresse qui reçoit des dons pour le projet Tails (une distribution Linux dont je vous ai déjà un peu parlé, que les crypto-anarchistes adorent car elle les rend anonymes sans laisser de traces).

Vu que tout est public sur la Blockchain, c'est fou tout ce qu'on y apprend ! On voit notamment que :

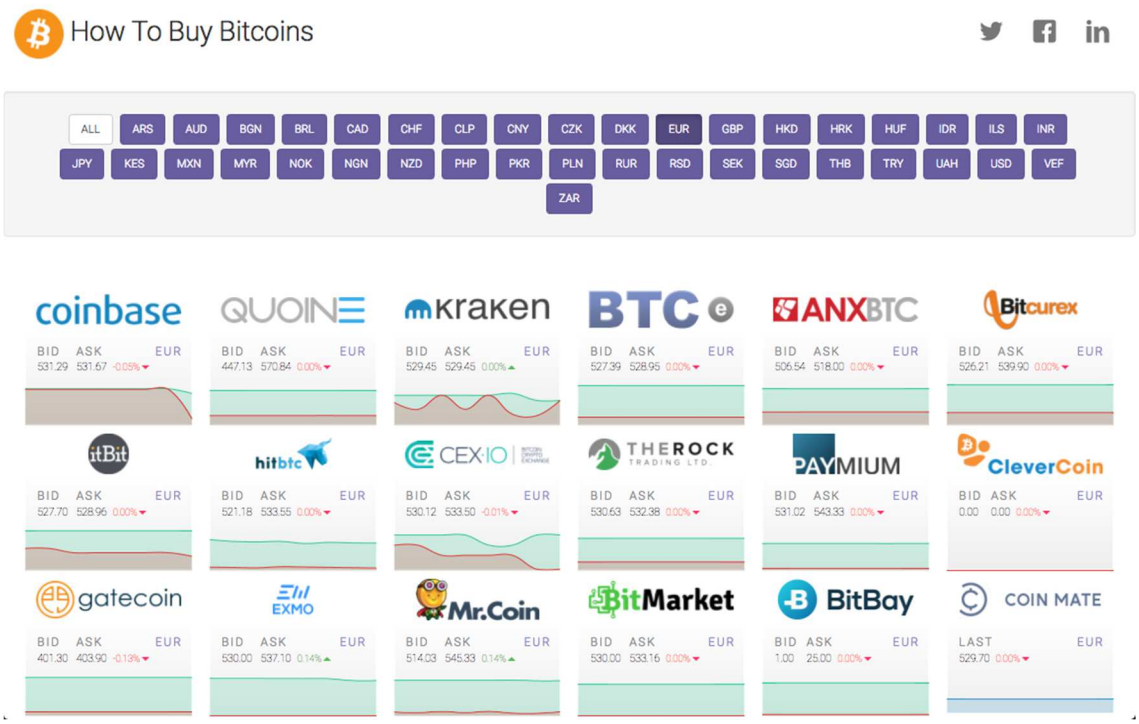
- **1874 transactions** ont eu lieu avec cette adresse
- **Cette adresse a reçu en tout 188 BTC**
- Actuellement, **il reste 106 BTC sur cette adresse** (une belle somme au cours du moment !), le reste ayant probablement été dépensé ailleurs
- Un QR Code a été généré pour vous permettre d'y envoyer de l'argent plus facilement (on verra comment faire plus tard)
- Et enfin vous avez tout le détail des transactions qui ont eu lieu avec cette adresse. Qui a donné à qui, quand, vous pouvez tout savoir !

Bref, vous l'aurez compris, sur la Blockchain tout est écrit, tout se sait ! C'est important de bien l'avoir en tête.

Où acheter des Bitcoins ?

Une simple recherche de "buy bitcoins" vous donnera largement assez de réponses... au point que vous ne saurez pas où aller.

Si vous voulez avoir une vue globale, le site How To Buy Bitcoins référence de nombreux sites qui permettent d'acheter des Bitcoins :



How To Buy Bitcoins référence de nombreux sites permettant d'acheter des Bitcoins

Conseil : sélectionnez votre devise habituelle (EUR pour les Euros) pour repérer les sites qui vous permettent d'acheter dans cette monnaie. Cela vous permettra aussi de connaître à quel prix ils vendent 1 BTC (Bitcoin). Par exemple, sur cette capture, on voit que Coinbase vend 1 BTC pour 531 EUR. Donc si vous payez 531€, vous obtiendrez 1 Bitcoin.
Ces sites sont des places de marché. Il y a des gens qui y vendent leurs Bitcoins et d'autres comme vous qui en achètent. C'est exactement comme dans les films sur Wall Street où vous voyez des traders hurler "*J'achète ! Je vends !*", sauf que tout se passe ici en ligne.

Les places de marché sont une sorte de Wall Street virtuel, où chacun achète et vend des Bitcoins

Sur ces places de marché, certains achètent des Bitcoins juste pour les revendre. Jouer au trader n'est pas sans risque. Certains achètent des Bitcoins (ex : à 600€) et les revendent quand ils valent plus cher (ex : à 630€), et empochent ainsi la différence. C'est un **jeu dangereux,** car on peut y perdre beaucoup d'argent.
Si en revanche vous avez toujours rêvé d'être Leonardo Di Caprio dans le Loup de Wall Street sans bouger de votre chaise, alors c'est fait pour vous. Bravo, vous êtes devenu le spéculateur financier qui "*gagne 10 000€ par semaine sans bouger de chez lui*", comme dans les pubs pour le Forex (marché des devises) qu'on voit circuler sur Internet.
Comment choisir parmi toutes ces places de marché ?
Pas évident, je le reconnais ! Il y a plusieurs critères à prendre en compte :

- Par quels moyens permettent-ils d'acheter des Bitcoins ? Virement, carte de crédit, cash ? Le virement coûte moins cher en frais, mais est plus long que la carte de crédit. Le cash, lui, est plus anonyme mais pas toujours le plus pratique.
- A quel prix vendent-ils actuellement des Bitcoins ? Certains sont plus chers que d'autres, même si globalement les prix tendent à s'équilibrer.
- A quel prix vous font-ils payer leur service ? Quels sont les frais ?

En ce qui me concerne, je connais notamment :

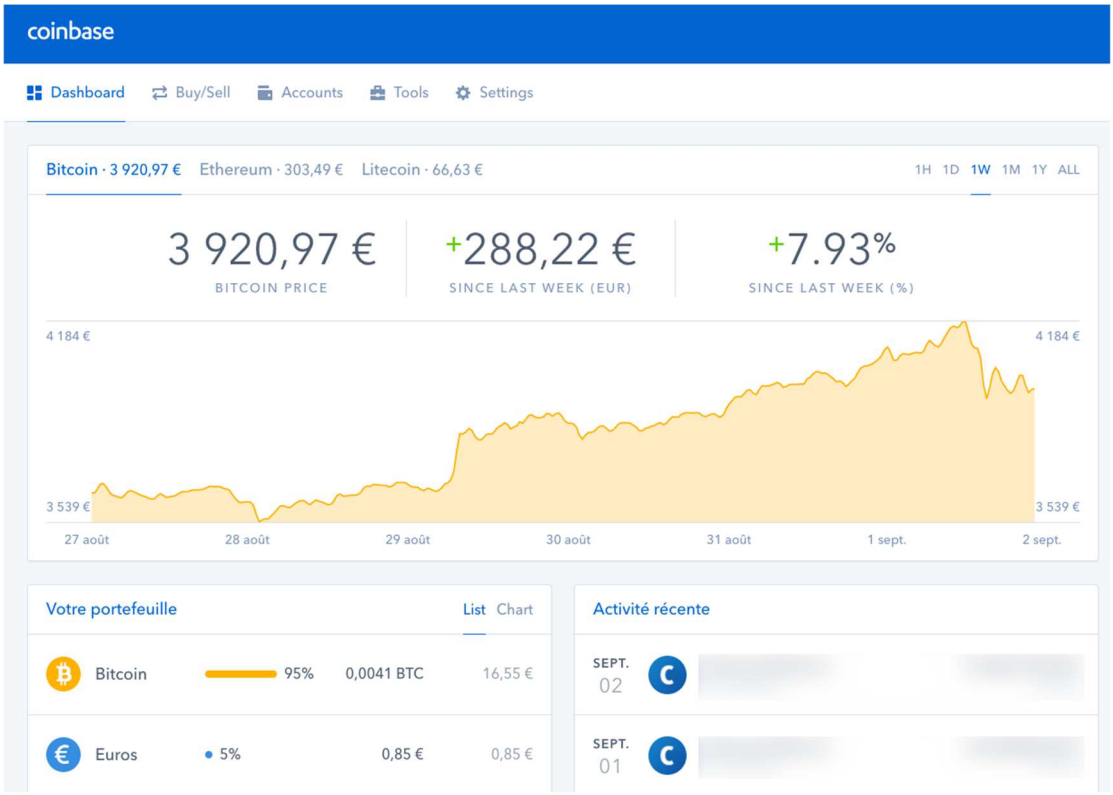
- Coinbase : qui a l'avantage de permettre d'acheter en carte de crédit.
- Kraken : une des références les plus connues.
- Paymium : une place de marché française.
- ... mais il en existe beaucoup d'autres et je ne les ai pas toutes testées évidemment.

Acheter sur Coinbase

Puisqu'il faut bien montrer un exemple, je vais vous présenter Coinbase qui est celui que j'utilise pour acheter des Bitcoins. Il est surtout pratique parce qu'il permet d'acheter instantanément des Bitcoins par carte bancaire (même si ça implique un peu plus de frais).
Commencez par créer un compte. Je vous propose 2 méthodes, en toute transparence :

- Coinbase (lien normal) : vous permet de créer un compte classique, sans bonus.
- Coinbase (lien affilié) : vous permet de créer un compte dans lequel on offrira à vous et moi 10$ à partir de 100$ de Bitcoins achetés.

Créez votre compte comme sur n'importe quel site, il n'y a rien de spécial à savoir. En revanche, je vous invite à utiliser un mot de passe long, solide, que vous n'avez jamais utilisé ailleurs. Il y a de l'argent en jeu et vous ne voudriez pas vous le faire voler !
Je vous recommande par ailleurs fortement d'activer la double authentification pour sécuriser votre compte, en utilisant une application comme Google Authenticator. Cela réduit grandement les risques que quelqu'un s'introduise dans votre compte pour vous voler des Bitcoins.
Une fois connecté, vous arrivez sur le tableau de bord :



Le tableau de bord de Coinbase

Vous pouvez y voir le prix actuel d'1 Bitcoin (BTC). Comme vous pouvez le constater, ça peut varier grandement d'un jour à l'autre !

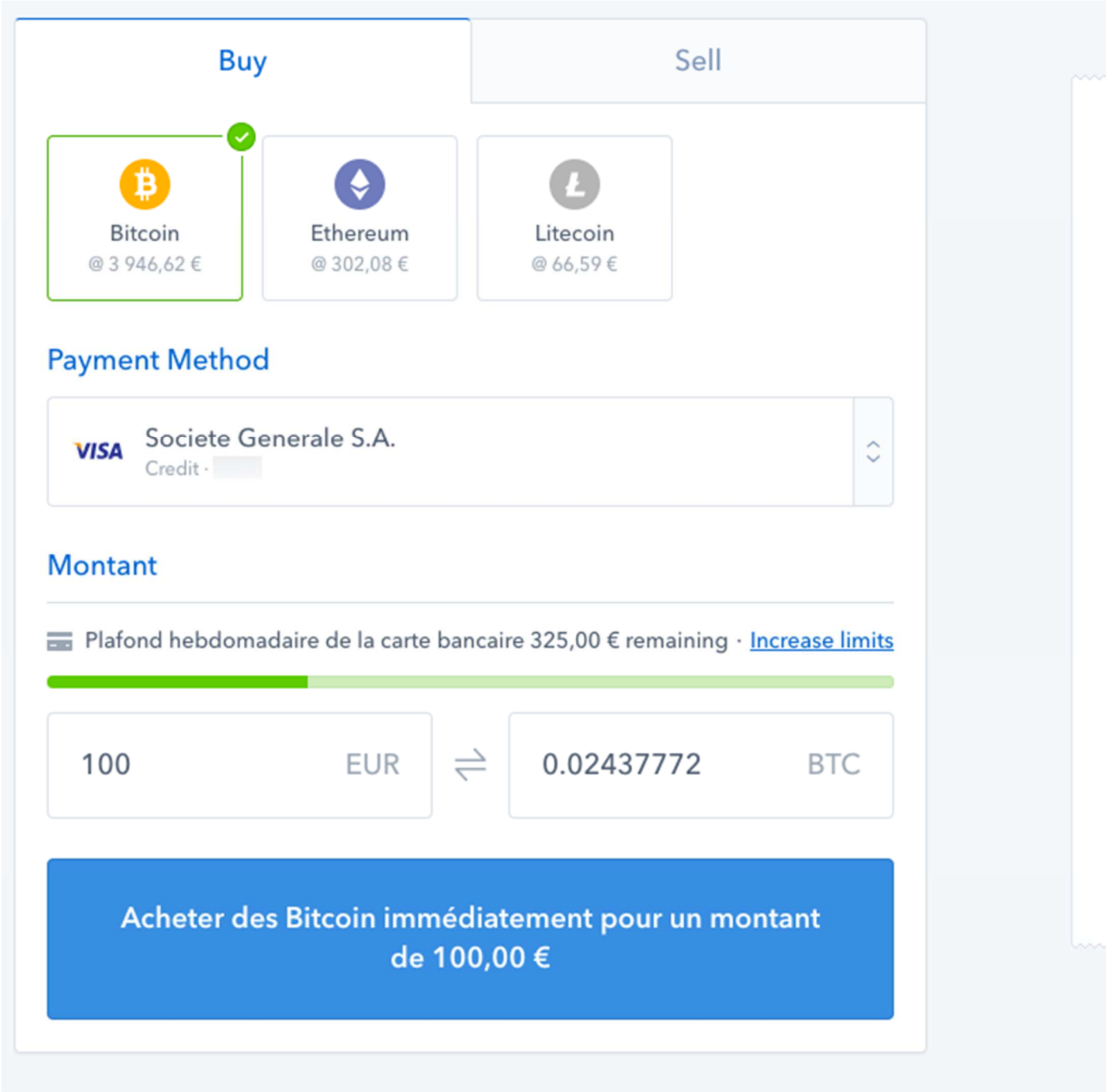
On vous propose aussi de télécharger l'application Coinbase pour téléphone mobile, que je trouve bien faite.
Pour acheter des Bitcoins, vous devez commencer par ajouter une méthode de paiement. Rendez-vous sur la page "Paramètres/Méthodes de paiement", puis cliquez sur "Ajouter une méthode de paiement" :

Choix de la méthode de paiement

Vous pouvez acheter vos Bitcoins soit par :

- **Virement bancaire** (SEPA) : les virements ont le défaut d'être longs (4-5 jours !) mais vous pouvez acheter plus de Bitcoins par ce biais.
- **Carte bancaire** (si celle-ci supporte 3D Secure) : l'achat est immédiat, c'est très pratique ! En revanche, il y a une limite plus forte au nombre de Bitcoins que vous pouvez acheter et un peu plus de frais.

Je trouve que le plus intuitif pour commencer est de faire un achat par carte bancaire. A moins que vous n'ayez l'intention d'acheter immédiatement des dizaines de milliers d'euros en Bitcoin, la carte bancaire est largement suffisante.
Une fois la carte bancaire ajoutée, vous pouvez vous rendre sur la page "Achat/vente" (Buy/Sell) :



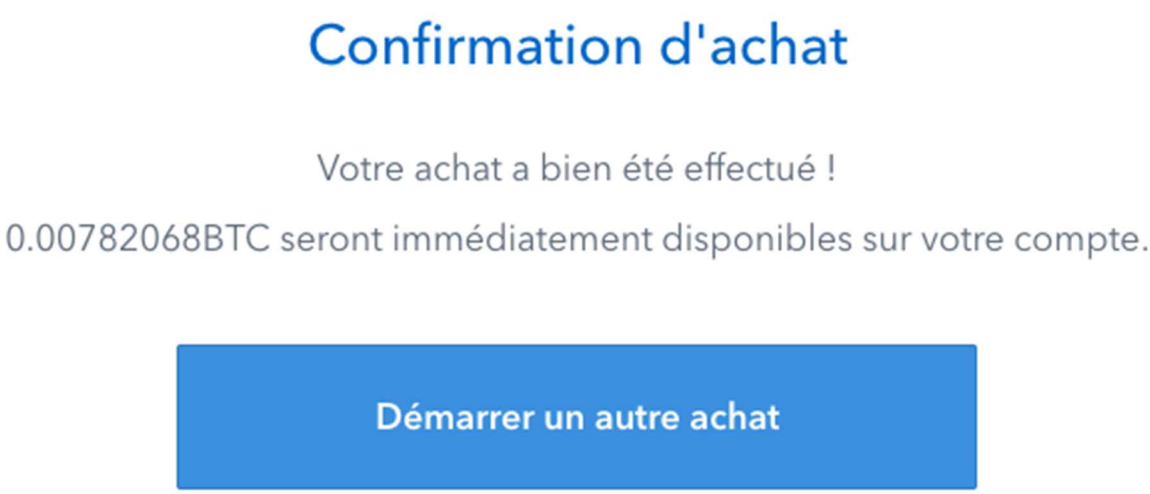
Achats de Bitcoins sur Coinbase

Vérifiez en haut que vous achetez ("Buy"). Sélectionnez votre devise, ici le Bitcoin (on vous propose d'autres cryptomonnaies, dont on ne parlera pas pour le moment). Sélectionnez votre méthode de paiement : vous devriez trouver dans la liste la carte de crédit que vous venez d'ajouter.
Ensuite, indiquez combien de Bitcoins vous voulez acheter. Comme vous ne connaissez pas bien la valeur d'un Bitcoin, je vous recommande de remplir le champ en Euros et Coinbase fera automatiquement la conversion.

Combien devrais-je acheter de Bitcoins ?

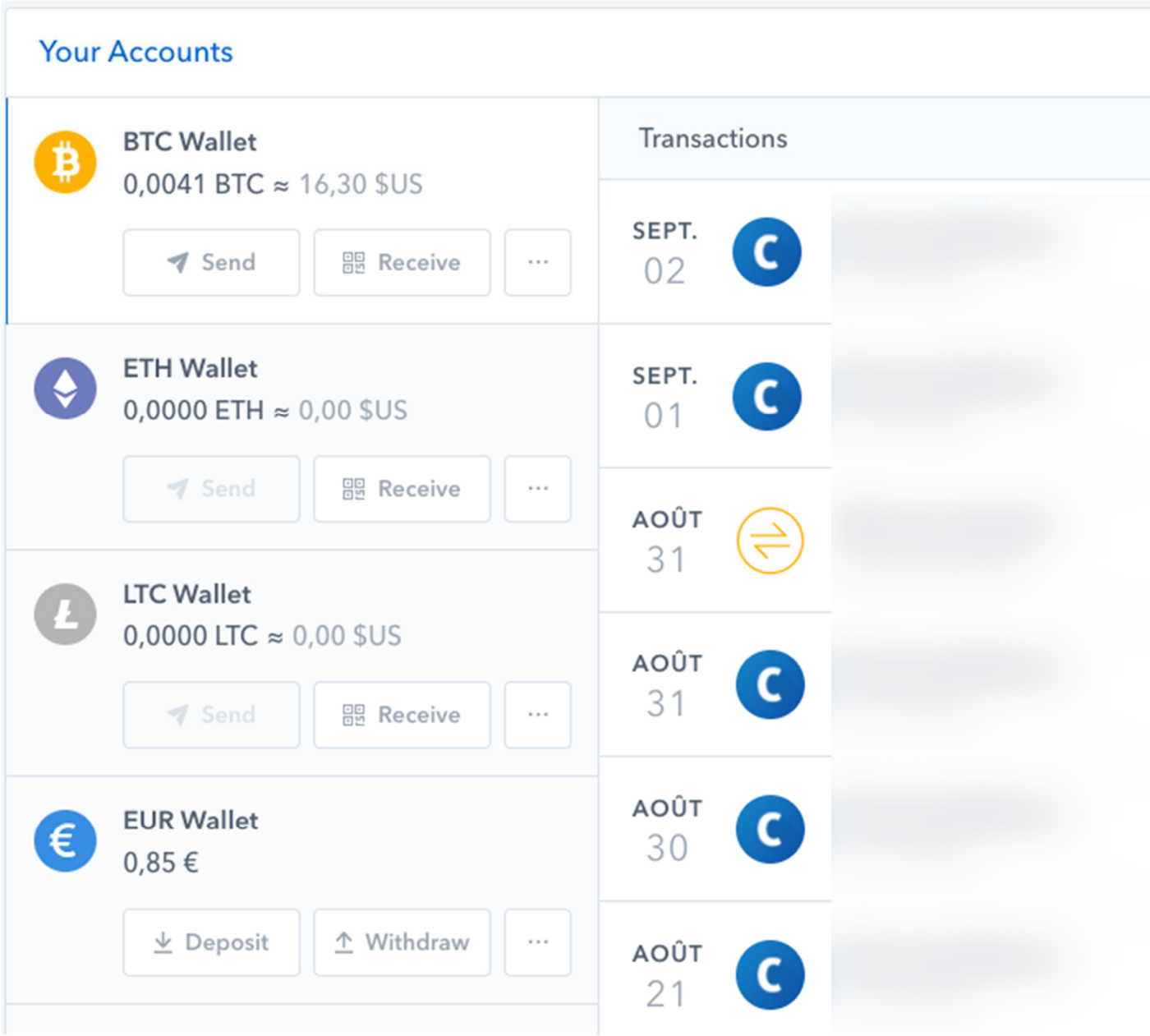
A ce stade, si c'est la première fois et que vous hésitez, je dirais "le minimum" : 5€ ? 10 € ?
Par la suite, si vous avez pris confiance, vous pourrez alors commander plus (à partir de 92€, si vous avez créé le compte via le lien affilié, on vous offrira 9€).
Comme vous le voyez, il y a aussi des frais prélevés par Coinbase pour l'opération d'achat.
Si vous êtes plus patient, vous pouvez aussi choisir de faire un virement depuis votre banque en utilisant le portefeuille en Euros (EUR Wallet). C'est un peu plus compliqué, ça prend plusieurs

jours, il faut bien penser à indiquer le numéro de référence dans le virement, mais l'avantage est que ça vous revient moins cher !
Le paiement est instantané. Vous devriez avoir la confirmation comme ceci :



Bravo, vous avez acheté des Bitcoins !

J'ai ici acheté... 0,00782068 Bitcoin !
Il faut savoir qu'1 Bitcoin peut être divisé en "bits", un peu comme les Euros sont divisés en centimes.
1 Bit = 0,000001 BTC
Vous pouvez retrouver votre argent dans la section "Comptes" (Accounts) sur Coinbase :



Vos comptes sur Coinbase

Coinbase permet d'héberger plusieurs portefeuilles virtuels :

- **BTC Wallet** : votre portefeuille de Bitcoins. C'est lui qui vient d'être crédité de 7820 bits (environ 5€) suite à l'achat que je viens de faire.
- **ETH Wallet et LTC Wallet** : d'autres cryptomonnaies qu'on peut acheter sur Coinbase.
- **EUR Wallet** : votre portefeuille d'Euros, que vous pouvez utiliser pour y faire des virements en Euros depuis votre banque. Une fois ce portefeuille rempli, vous pouvez l'utiliser pour acheter des Bitcoins.
- **BTC Vault** : un portefeuille sécurisé de Bitcoins, qui demande des protections supplémentaires. C'est une fonctionnalité de Coinbase dont on ne parlera pas ici.

OK, donc si je comprends bien, je viens d'acheter des Bitcoins... et il y a maintenant une belle page qui dit que j'ai des Bitcoins... super. Je ne vois pas bien ce qu'il vient de se passer, où sont mes pièces en Bitcoins ? Je veux mon argent, AU VOLEUR AU VOLEUR !

Je vous ai déjà dit qu'il n'y avait pas de pièces en Bitcoins : il s'agit d'une monnaie virtuelle.

Pour l'instant, nous avons effectivement récupéré des Bitcoins et le seul endroit où nous les voyons c'est sur cette page de Coinbase. Cependant, il n'est pas recommandé de laisser de l'argent là-dessus. En effet, si le site Coinbase se fait pirater, des personnes pourraient voler vos Bitcoins. C'est d'ailleurs ce qui est arrivé à la plateforme Mt. Gox, fermée depuis.

C'est un peu comme laisser de l'argent dans un casier au milieu d'une gare. Certes, il y a un code qui protège l'ouverture, mais il y a aussi du monde qui passe devant.

Que faire alors ? Il est **recommandé de rapatrier ces Bitcoins sur un portefeuille situé chez vous.** Ce portefeuille peut être sur votre ordinateur, votre téléphone portable ou un matériel spécialisé.

Stocker des bitcoins

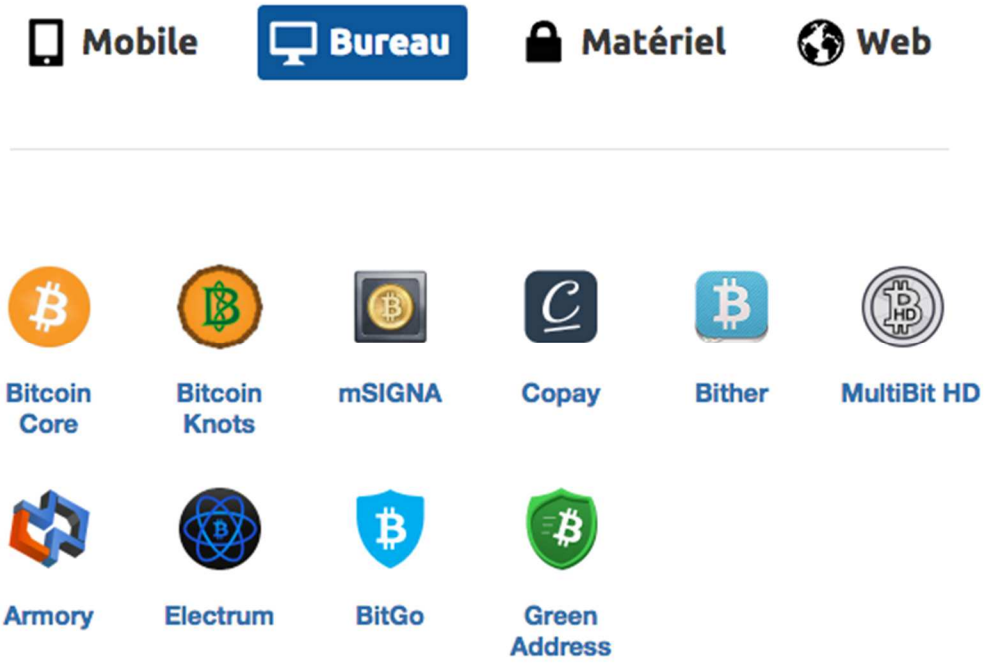
Avoir des Bitcoins, c'est bien, les conserver en lieu sûr, c'est mieux. Nous allons dans ce chapitre nous procurer l'équivalent d'un portefeuille... mais au format électronique. Nous allons passer par un logiciel spécial.

Nous allons nous créer un portefeuille... électronique.

Les portefeuilles de Bitcoins ne stockent pas vraiment l'argent (pour la millième fois : il n'y a pas de pièces dans le monde du Bitcoin !). Ils stockent en revanche des paires de clés qui vous permettent d'accéder à votre argent.
Si vous voulez en savoir plus sur les paires de clés, retournez lire le chapitre sur les paiements en Bitcoins dans la première partie de ce cours !

Les différents types de portefeuille

Le site officiel de Bitcoin résume je trouve très bien les différents portefeuilles disponibles sur le marché :



Les différents types de portefeuille selon Bitcoin.org

Vous avez 4 catégories :

- **Mobile** : ce sont des portefeuilles sous forme d'application mobile. Tant que vous avez votre smartphone sur vous avec l'application, vous avez donc votre argent sur vous.
- **Bureau** : ce sont des portefeuilles pour des ordinateurs de bureau.
- **Matériel** : il s'agit de matériel dédié au Bitcoin qui vous permet de stocker vos Bitcoins de manière sécurisée (le plus souvent sur une sorte de clé USB).
- **Web** : ce sont des portefeuilles en ligne, stockés sur un site. Coinbase fait partie de la liste, car les Bitcoins que nous avons achetés peuvent rester là-bas.

Quel type de stockage choisir ?

Si je devais classer ces outils, **du plus sécurisé au moins sécurisé** à mes yeux :

1. Matériel : il n'y a rien de mieux qu'un matériel dédié au Bitcoin, vos Bitcoins sont inaccessibles sans la clé. Personne ne peut se "connecter" à la clé pour récupérer ses secrets.
2. Mobile : la sécurité sur smartphone est en général bonne, car les applications sont isolées les unes des autres. Bien sûr, cela suppose que vous faites toutes les mises à jour iOS ou Android.
3. Bureau : un ordinateur de bureau peut être vulnérable s'il est connecté à Internet. C'est souvent mieux que de laisser traîner ses Bitcoins sur un site web, mais on prend quand même le risque d'avoir un virus qui pourrait récupérer nos Bitcoins. Certains, pour se protéger, stockent leur Bitcoins sur un ordinateur qui n'est jamais connecté à Internet !
4. Web : ce n'est clairement pas l'idéal, même si c'est la solution qui semble la plus pratique au premier abord. Si le site web que vous utilisez pour stocker vos Bitcoins se fait pirater, vous risquez fort de ne plus jamais revoir vos Bitcoins. Bien entendu, certains font de vrais efforts en termes de sécurité pour ne jamais voir votre clé privée, mais si vous êtes un bon parano vous ne devriez pas leur faire confiance.

Bien entendu, tous ces logiciels ne se valent pas. Si vous cliquez sur l'un d'eux sur la page des portefeuilles, vous aurez plus de détails sur ce que vaut leur sécurité :

Plus de détails sur la sécurité des portefeuilles

A vous de faire un choix éclairé ! Les possibilités ne manquent pas.

... quoi, vous ne savez pas choisir et vous avez besoin d'aide ? Allons allons, vous devriez vraiment essayer vous-mêmes les logiciels !
Ceci étant, il faut bien que je vous montre comment fonctionne un portefeuille, donc je vais en prendre en exemple.
Sur ordinateur de bureau, le choix le plus logique serait **Bitcoin Core**, le logiciel officiel (il est open source, comme la plupart de ces logiciels, c'est un minimum si on veut avoir confiance). Le problème de Bitcoin Core, c'est qu'il vous fait télécharger touuuuute la blockchain. Votre ordinateur devient donc un noeud officiel du réseau, qui enregistre et valide la blockchain, mais le téléchargement de la blockchain peut prendre des jours voire des semaines... et occuper une grosse partie de votre espace disque.
Je vous présenterai dans ce cours 3 solutions, de catégories différentes :

- **Bureau** : Electrum
- **Mobile** : breadwallet
- **Matériel** : Ledger

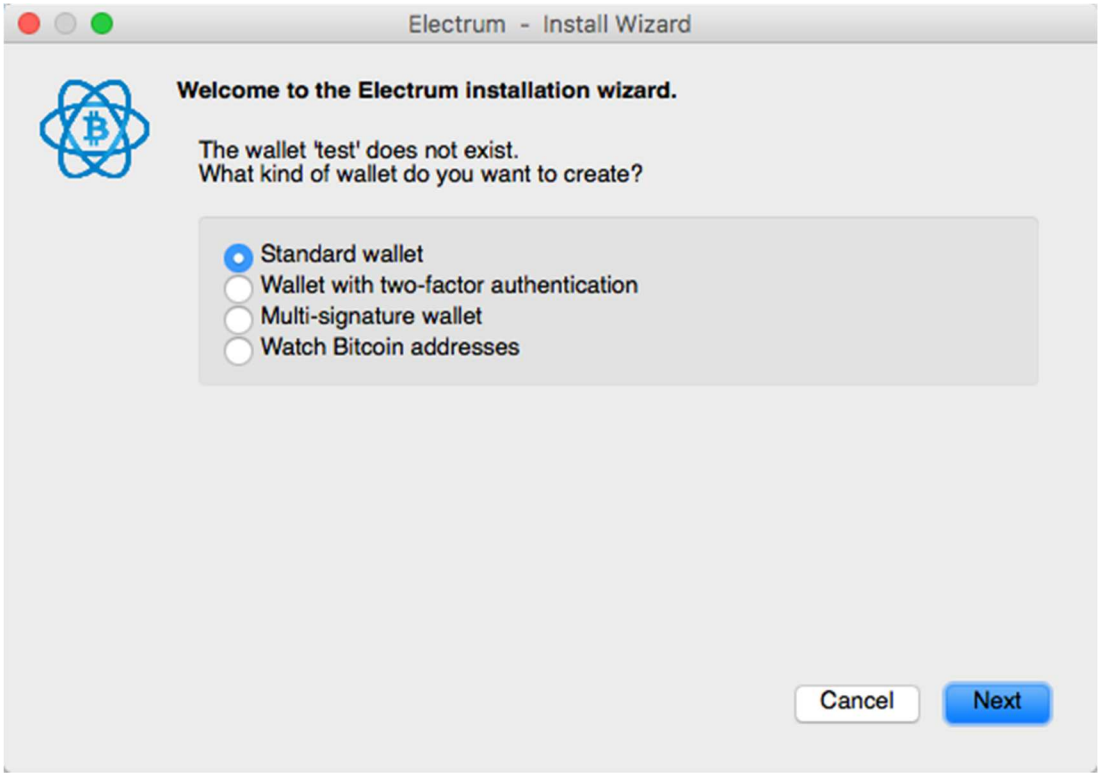
Configuration d'Electrum

Electrum a l'avantage d'être simple et léger, tout en offrant une sécurité correcte.
Quand je dis "sécurité correcte", si votre ordinateur est infecté par un virus, vous prenez quand même le risque de perdre vos Bitcoins. L'idéal est de l'installer sur un ordinateur qu'on ne connecte jamais à Internet, mais est-ce que ça existe encore de nos jours ?

Si vous avez une vieille machine sans wifi dans une cave, vous savez quoi en faire maintenant !

Vous pouvez télécharger Electrum sur le site officiel.

La première fois que vous lancez Electrum, on vous indique que vous n'avez pas de portefeuille sur cet ordinateur :

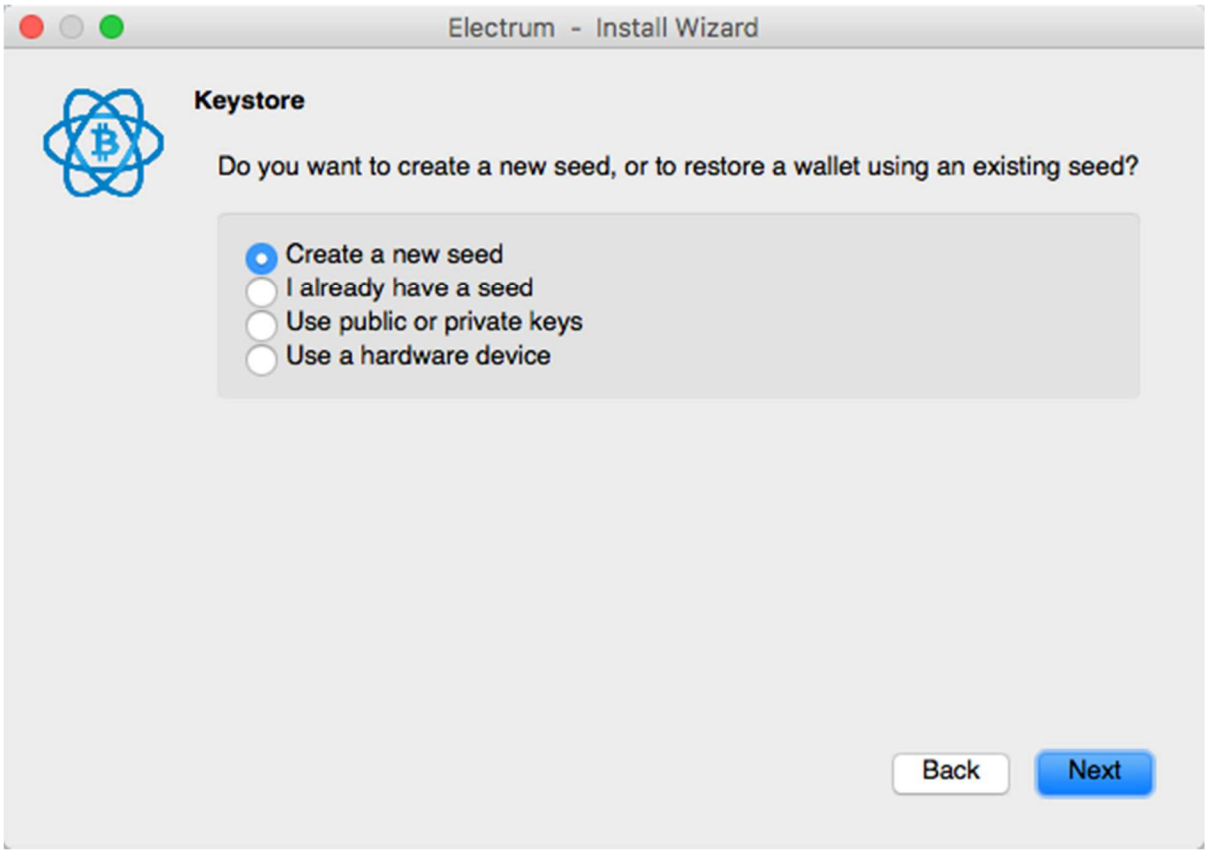


Electrum vous demande de créer un portefeuille

On vous demande le type de portefeuille. Le choix peut avoir une incidence sur la sécurité :

- **Standard wallet** : portefeuille normal, sans fioritures, stocké sur votre ordinateur. C'est le choix le plus simple, mais probablement le moins sécurisé du lot.
- **Wallet with two-factor authentication** : ce type de portefeuille vous permet d'activer une double authentification pour déverrouiller l'accès au portefeuille. Plutôt une bonne idée, mais ça oblige ici à utiliser un service externe (Trustedcoin) qui prendra quelques frais au passage.
- **Multi-signature wallet** : le portefeuille est verrouillé par plusieurs clés au lieu d'une seule. Un peu comme dans les films de James Bond, où il faut 3 clés détenues par 3 personnes différentes pour ouvrir la porte d'un sas sécurisé.
- **Watch Bitcoin addresses** : si vous voulez juste suivre des mouvements financiers sur le réseau. Ca correspond à créer un portefeuille en lecture seule, depuis lequel vous ne pouvez pas envoyer d'argent.

Nous allons rester simple pour le moment et créer une standard wallet. On vous demande ensuite d'autres informations :



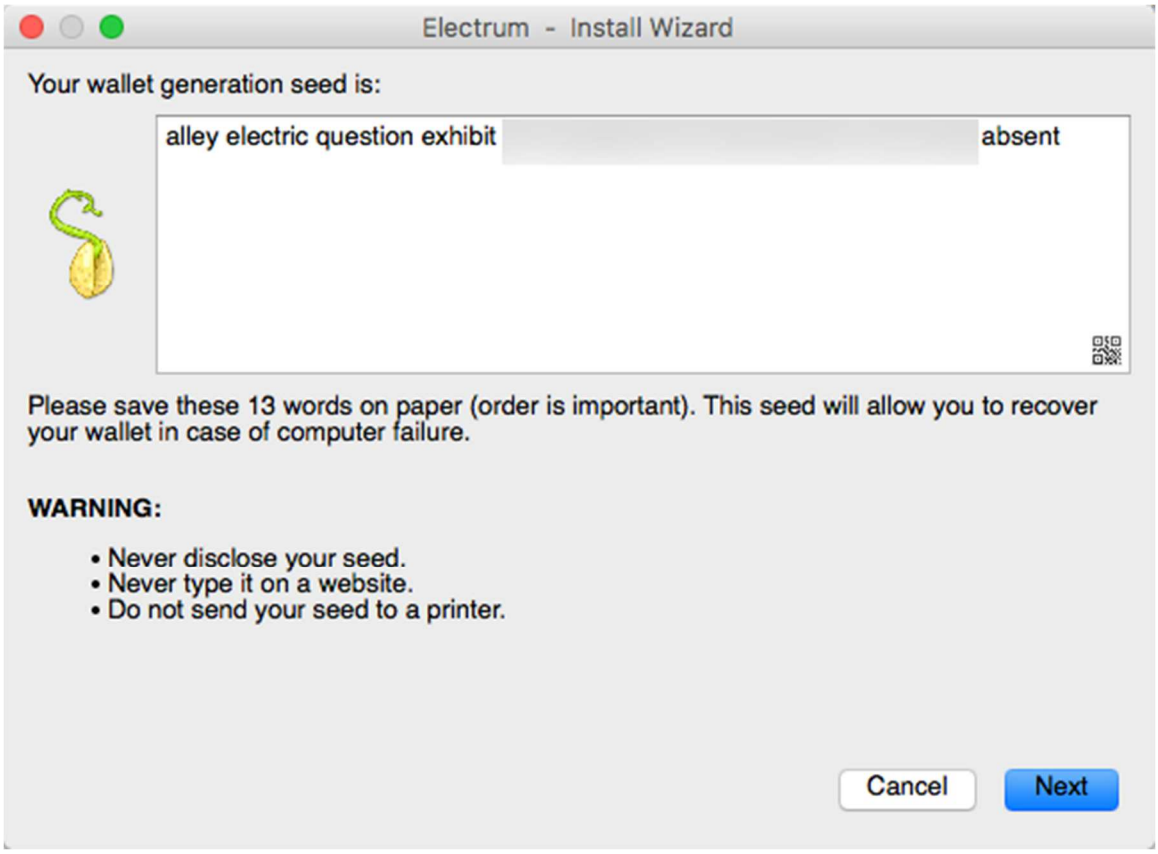
Configuration du portefeuille

Vous allez sélectionner "**Create a new seed**" (créer une nouvelle graine). Les autres options servent à restaurer un portefeuille que vous auriez perdu, ou à configurer Electrum avec un matériel spécifique pour le sécuriser (nous en reparlerons dans un prochain chapitre).

Nous ne choisissons pas la méthode la plus sûre : la clé qui sécurise votre argent sera stockée sur notre ordinateur et pourrait être volée si nous avons un virus. Cependant, comme on ne va pas mettre des milliers d'euros dessus non plus pour le moment, ça fera l'affaire.
Electrum doit générer une paire de clés :

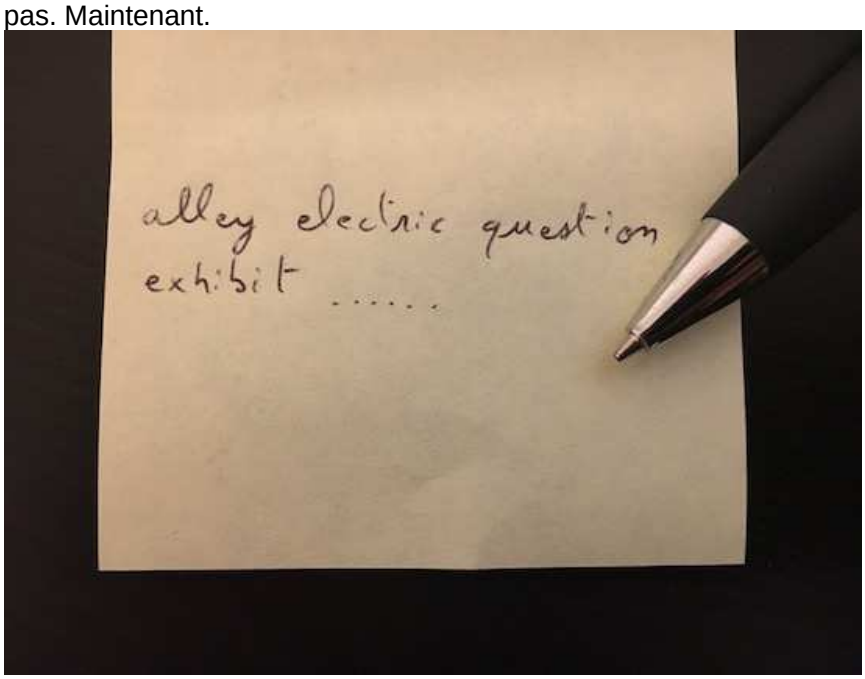
- **Clé publique** : qui peut être communiquée à tout le monde
- **Clé privée** : sert à signer les transactions, à prouver que vous êtes bien le propriétaire. *Quiconque possède la clé privée possède l'argent*.

Electrum utilise un algorithme assez malin qui permet, à partir d'une liste de mots aléatoires, de générer la paire de clés. Electrum vous communique donc cette liste de mots, qui est **ultra-confidentielle** :



Génération de la graine (seed)

On dit que cette liste de mots est une graine (seed). A partir de cette graine, on peut reconstruire votre paire de clés qui sert à transférer l'argent.
Vous devez **noter ces mots sur une feuille de papier**. Sérieusement. Faites-le. Je ne plaisante pas. Maintenant.

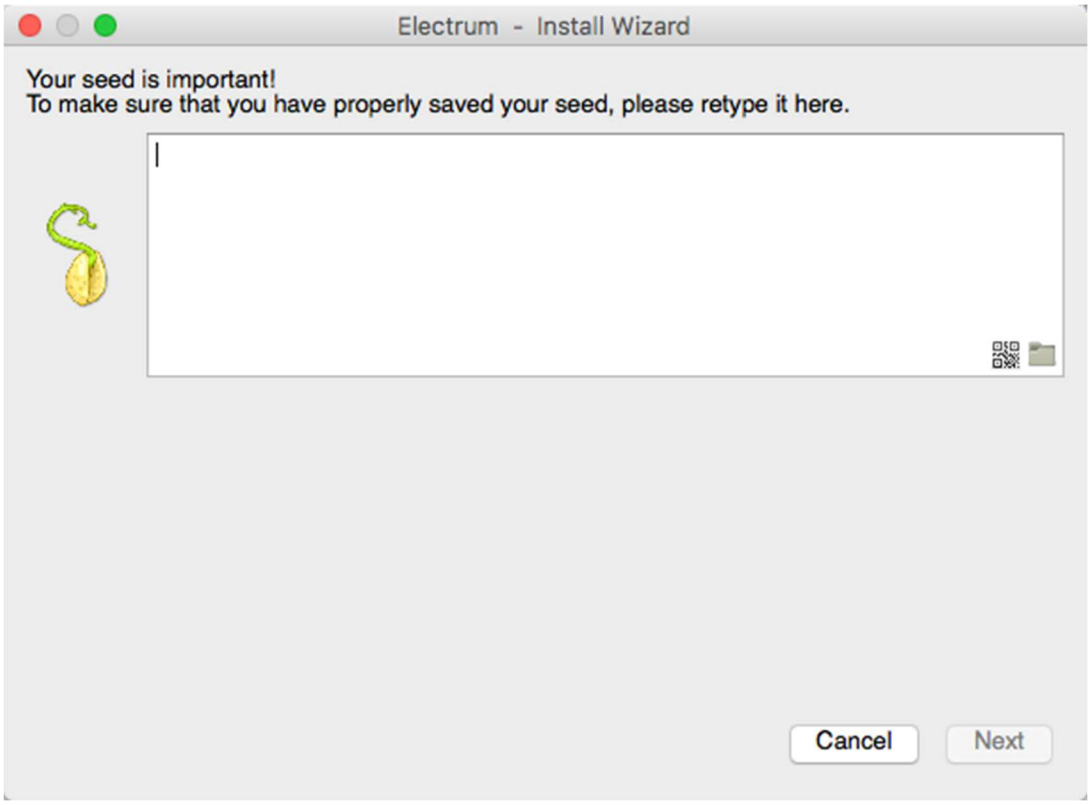


Notez bien ces mots sur une feuille de PAPIER que vous conserverez en sécurité

Gardez cette feuille de papier au chaud dans un endroit secret. J'entends par là idéalement un coffre-fort, mais pour commencer votre (vrai) portefeuille pourra faire l'affaire.
Je répète. Notez ces mots sur une feuille de papier. Ils sont la clé de tout.

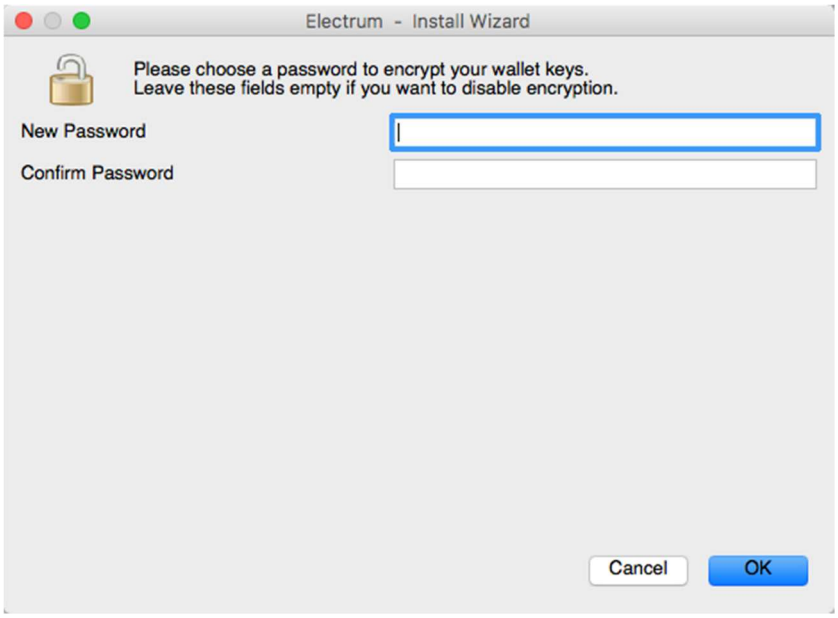
A partir de ces mots, vous pouvez régénérer les paires de clés. Si vous perdez votre ordinateur, votre argent ne sera donc pas perdu, vous pourrez le retrouver juste en ayant cette liste de mots magiques en main.

Ah, et notez bien sur une feuille de papier. Pas dans un fichier sur votre ordinateur (qu'un virus pourrait lire). N'utilisez même pas votre imprimante pour imprimer ces mots. Ne faites pas de capture d'écran de cette liste de mots non plus.
Si vous voulez une solution à l'épreuve du feu, de l'eau et des bombes (!), regardez du côté de Cryptosteel.
Pour vous montrer à quel point il est important d'avoir noté la graine (liste de mots), Electrum vous impose de réécrire ces mots un à un. Histoire d'être sûr que vous les avez bien notés !



Retapez la graine !

Ensuite, Electrum vous propose d'ajouter une sécurité supplémentaire en saisissant un mot de passe pour chiffrer votre clé privée. Ce n'est pas obligatoire mais je vous le recommande fortement. Ainsi, si quelqu'un venait à récupérer votre clé privée, il ne pourrait rien faire sans le mot de passe pour la déchiffrer.
Surtout, utilisez un VRAI mot de passe dont vous ne vous êtes jamais servi nulle part, sinon la sécurité ne sert à rien.



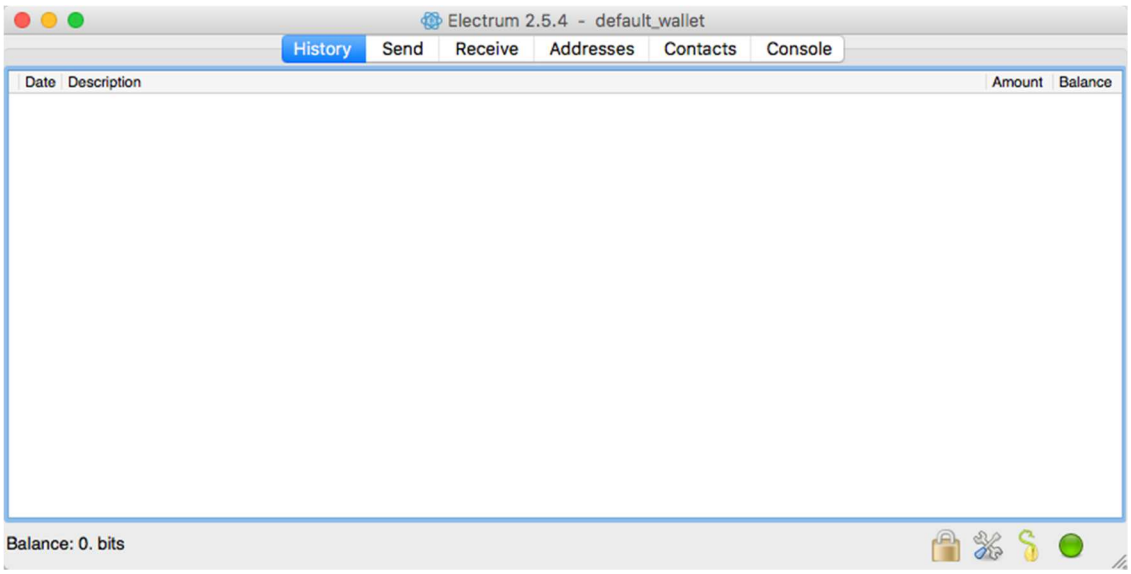
Protégez la clé avec un mot de passe

Félicitations, vous êtes maintenant propriétaire d'un nouveau portefeuille de Bitcoins.
Votre portefeuille est représenté par des paires de clés (qu'on ne vous montre jamais à l'écran, car c'est ennuyeux à lire).

La liste de mots (graine) permet de retrouver la paire de clés grâce à un algorithme. Elle a l'avantage d'être plus facile à retenir et retaper. Quiconque connaît la liste de mots dispose des clés, et donc de l'argent.

Utiliser Electrum

Voici à quoi ressemble l'accueil d'Electrum la première fois :



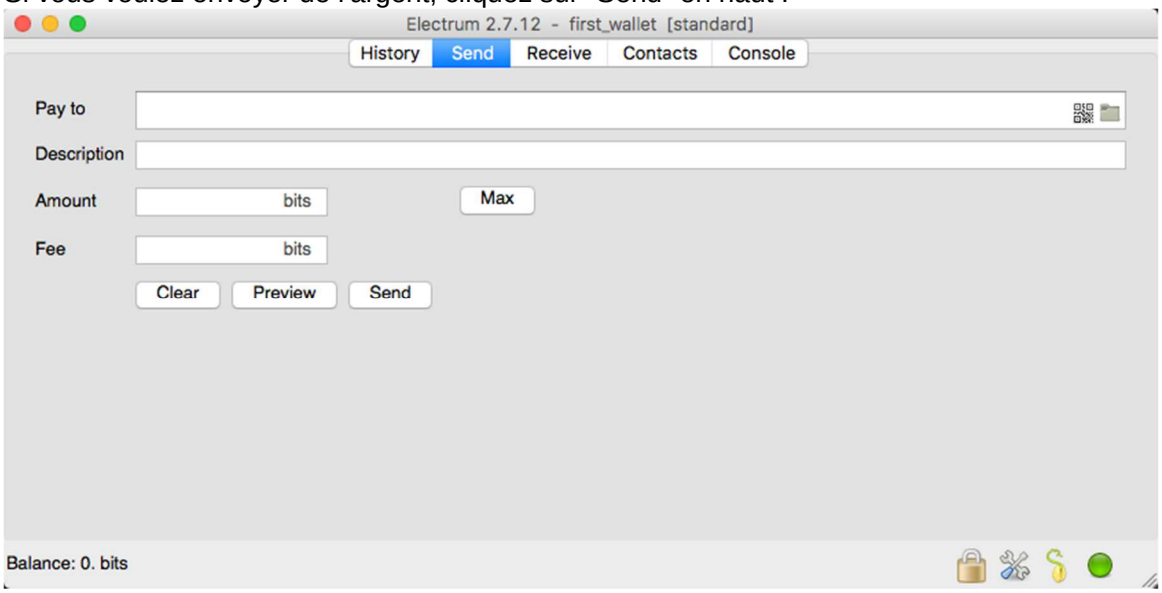
Ecran d'accueil d'Electrum. Pas très "accueillant", mais fonctionnel

L'écran n'est pas très sexy, je vous l'accorde. Ici s'affiche normalement la liste des transactions effectuées avec ce portefeuille (aucune pour l'instant).

En bas à gauche s'affiche la quantité d'argent stockée dans ce portefeuille (0 bits, soit la somme rondelette de 0,000000 Bitcoins). En bas à droite, le rond doit être vert pour indiquer que vous êtes connecté à un serveur. Si ce n'est pas le cas, vous pouvez cliquer dessus pour changer de serveur au besoin.

Enfin, l'icône de graine à côté vous permet d'afficher à nouveau la graine au besoin.

Si vous voulez envoyer de l'argent, cliquez sur "Send" en haut :

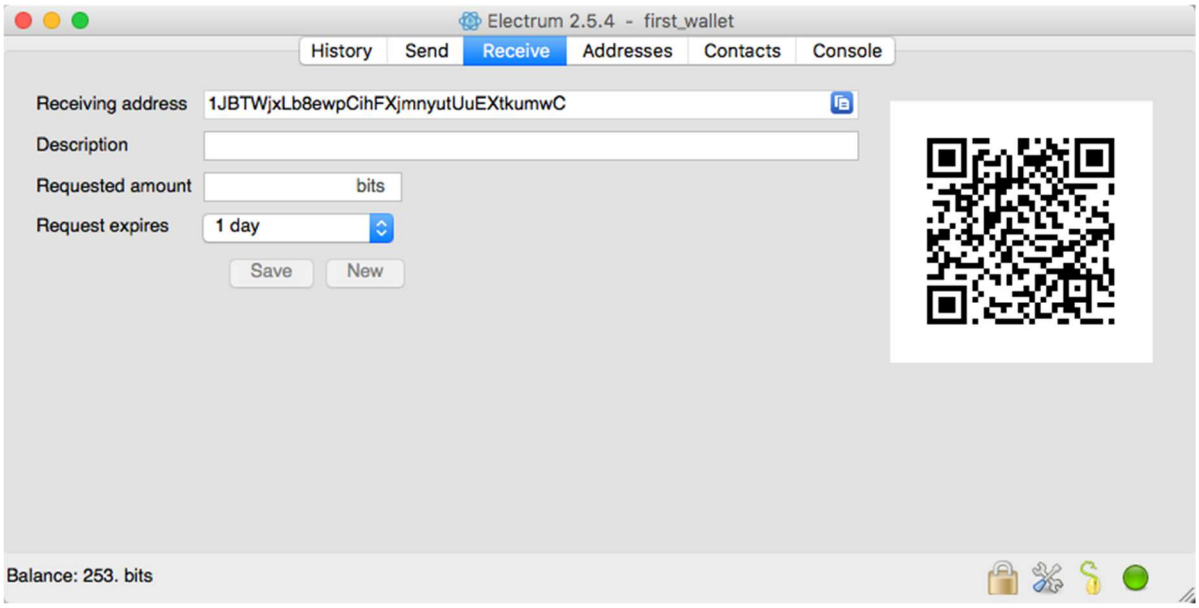


Envoi de Bitcoins avec Electrum

Vous devez y copier l'adresse à qui vous souhaitez envoyer de l'argent. La description est facultative, mais en revanche le montant est obligatoire.

Attention à l'échelle, ici j'ai configuré Electrum pour afficher des bits (mini-morceaux de Bitcoins) et non des BTC.
Le champ "Fee" (frais) vous permet d'indiquer combien de frais vous êtes prêt à payer pour cette transaction. Plus vous payez de frais, plus vite votre transaction sera traitée par les ordinateurs du réseau.
Vous pouvez aussi choisir de ne pas payer de frais, mais dans ce cas la transaction pourrait mettre du temps à être prise en compte. Dans le doute, laissez Electrum faire ce qu'il propose par défaut.

Si vous voulez recevoir de l'argent dans ce portefeuille, cliquez sur "Receive" :



Adresse permettant de recevoir des Bitcoins

On vous propose une adresse que vous pouvez communiquer pour y recevoir des Bitcoins (ainsi qu'un QR Code si quelqu'un a un smartphone à côté de vous pour le scanner).

A ce stade, vous devriez avoir :

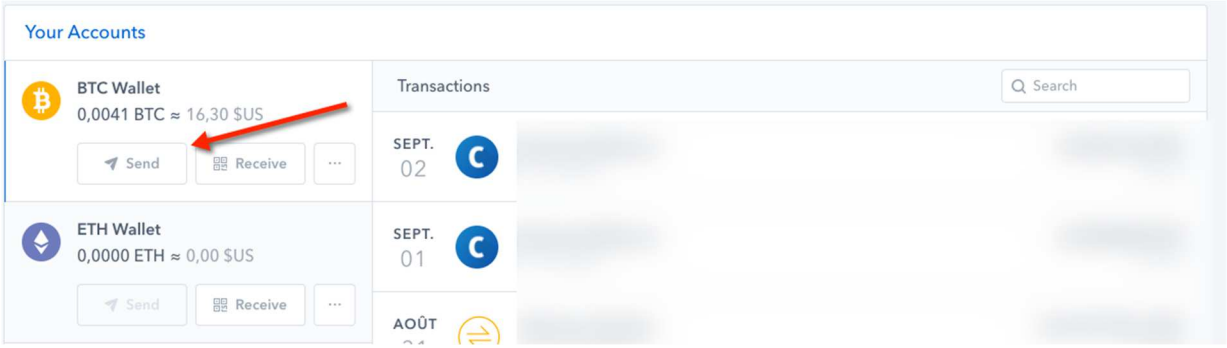
- Acheté des Bitcoins avec des Euros sur une plateforme comme Coinbase
- Installé un portefeuille de Bitcoins comme Electrum sur votre ordinateur

Dans ce chapitre, nous allons rapatrier nos Bitcoins de Coinbase vers notre machine sur Electrum. Ainsi, nous garderons nos Bitcoins plus près de nous plutôt que de les laisser en ligne sur un site.

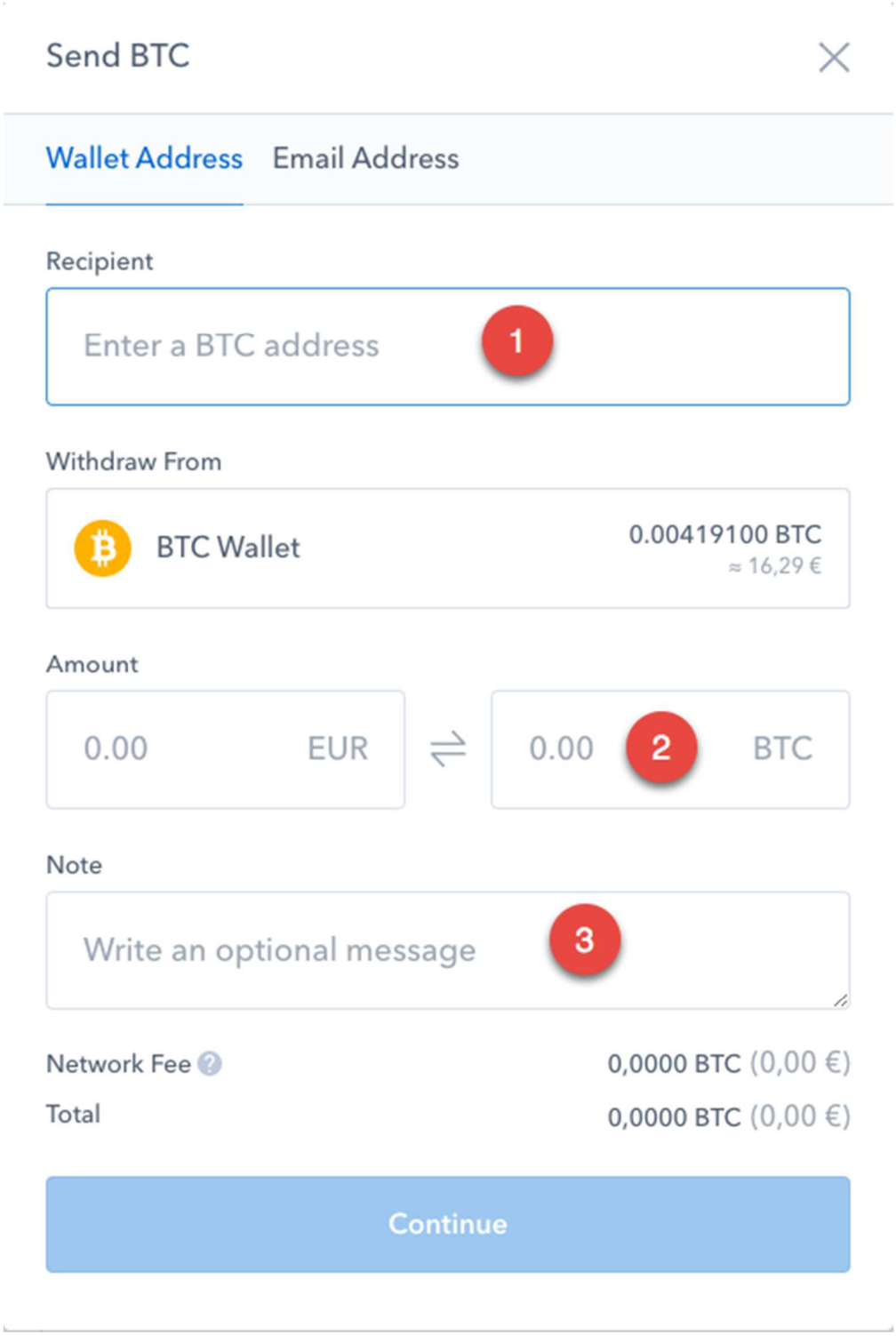
Ensuite, nous verrons comment faire nos premiers achats (ou dons !) en Bitcoins !

Rapatrier nos Bitcoins sur notre machine

Retournons sur Coinbase, où nous avons acheté quelques Bitcoins. Dans la section "Accounts", nous allons cliquer sur "Send" pour envoyer nos Bitcoins vers notre portefeuille Electrum.



Cliquez sur "Send" pour envoyer vos Bitcoins ailleurs
Dans la fenêtre qui suit, vous pouvez indiquer où vous souhaitez envoyer vos Bitcoins :



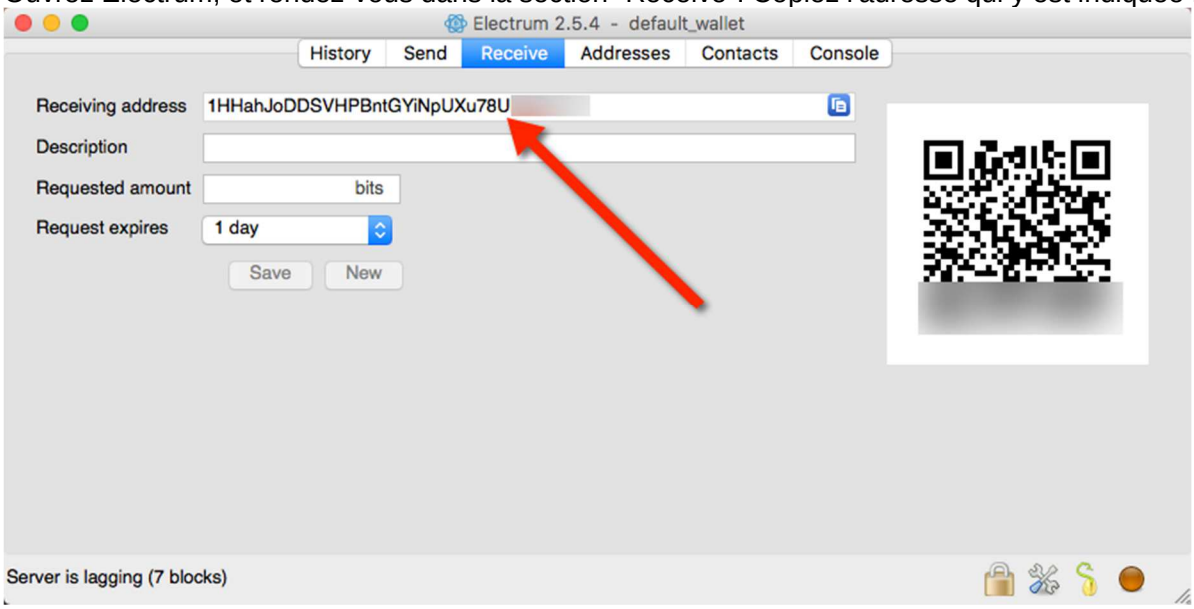
L'interface de Coinbase nous permet de déplacer nos Bitcoins

Vous allez remplir les champs suivants :

1. **Adresse Bitcoin** : c'est là où vous voulez envoyer vos Bitcoins. Dans Electrum, rendez-vous dans "Receive" et copiez-y l'adresse indiquée.
2. **Montant** : vous devriez normalement transférer tous vos Bitcoins disponibles sur Coinbase (vous pouvez cliquer sur le bouton "Send max").
3. **Commentaire** : facultatif, si vous voulez associer un message à la transaction.

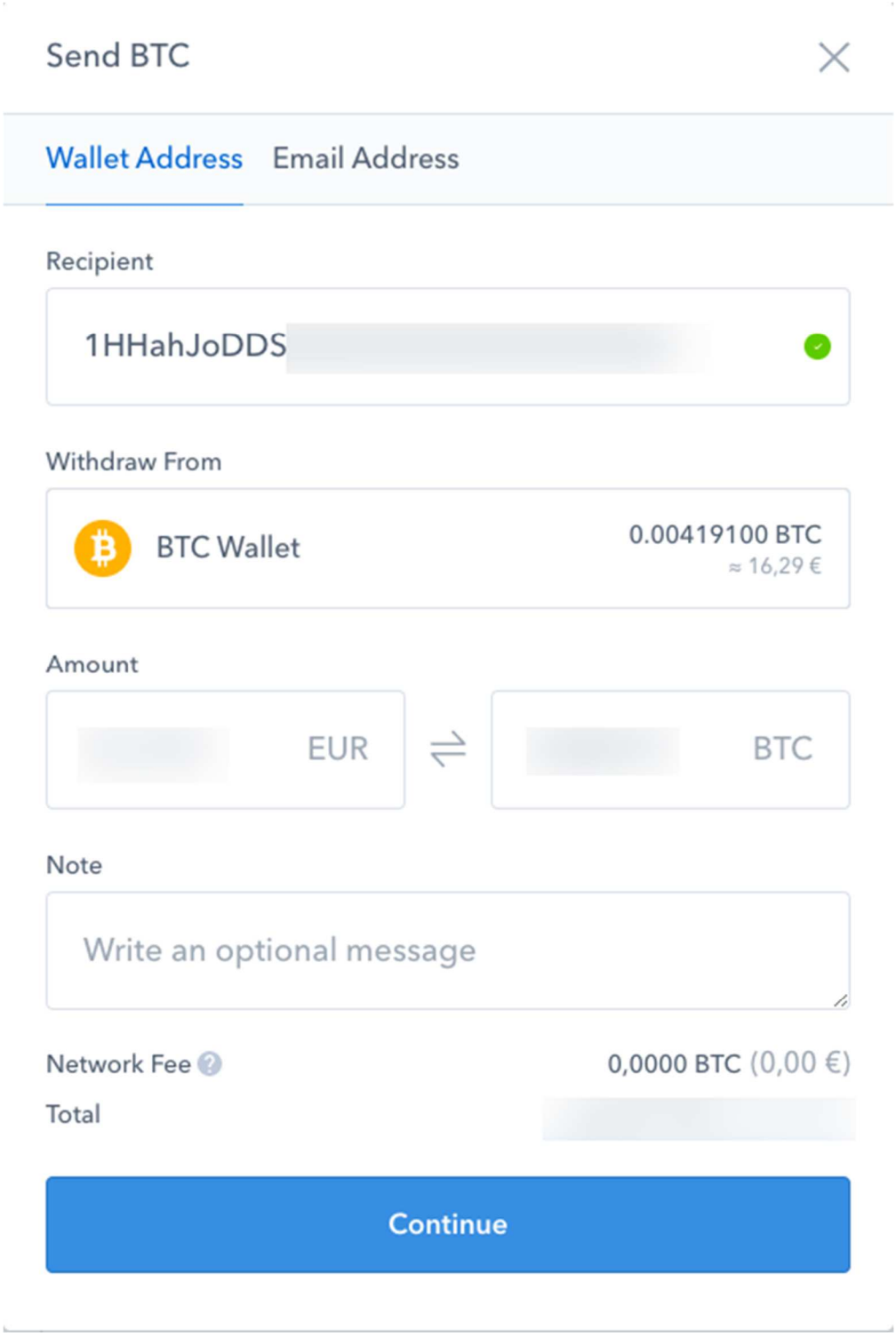
L'essentiel est de ne pas se tromper d'adresse destinataire !

Comment récupérer l'adresse à laquelle je dois envoyer mes Bitcoins ?
Ouvrez Electrum, et rendez-vous dans la section "Receive". Copiez l'adresse qui y est indiquée :



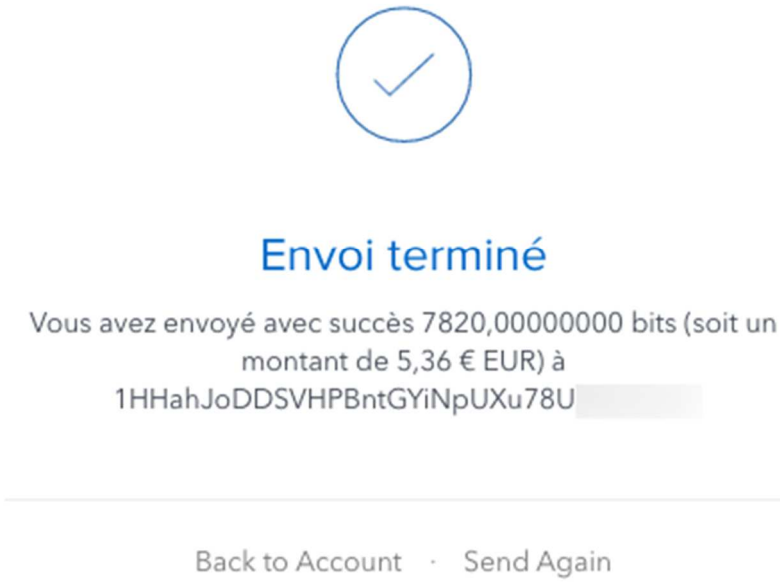
Copiez l'adresse indiquée dans Electrum...

... puis collez-la dans Coinbase :



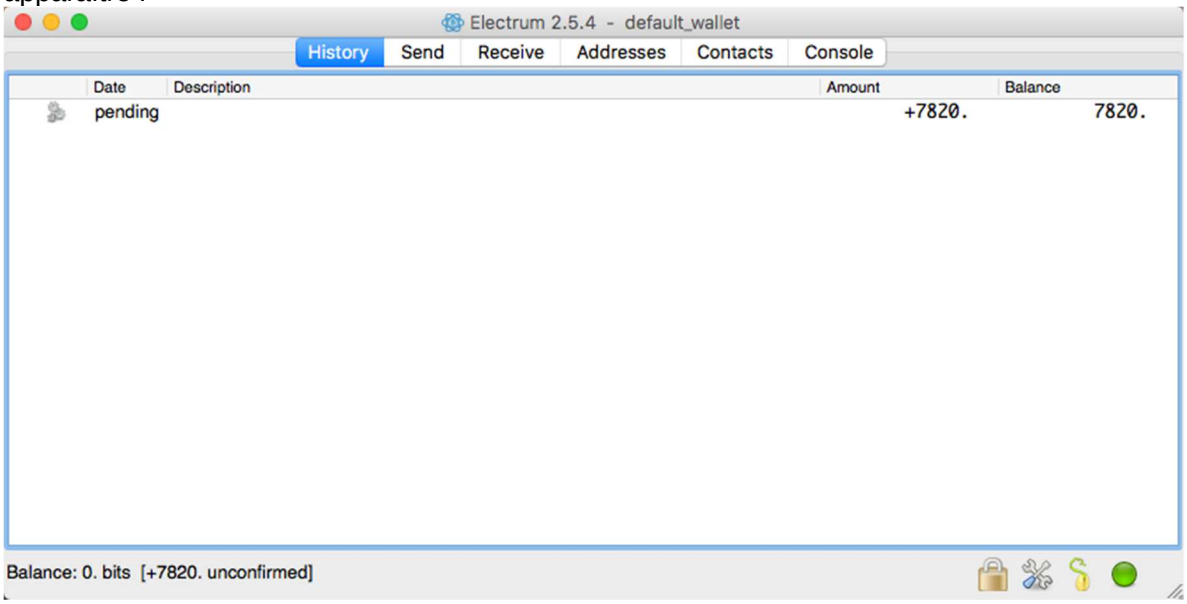
... puis collez l'adresse dans Coinbase !

J'envoie donc ici tous mes Bitcoins à mon portefeuille Electrum.
Cliquez sur "Envoyez les fonds". Si vous avez activé la double authentification sur Coinbase, on vous demandera de saisir un code par sécurité (je le recommande fortement). Ensuite... c'est fait !



Les Bitcoins ont été transférés !

Retournez sur Electrum. Au bout de quelques secondes à peine, vous devriez voir vos Bitcoins apparaître !



Electrum a bien et rapidement reçu les Bitcoins !

Si vous recherchez votre adresse sur Blockchain.info, vous devriez aussi y voir la transaction. Allez-y vous verrez !
En fait, la transaction n'est pas encore confirmée. Il faut que plusieurs blocs soient ajoutés à la Blockchain pour que ça soit le cas.
Une transaction non confirmée est considérée comme "encore douteuse" par les autres ordinateurs (qui craignent que vous puissiez dépenser votre argent deux fois). Lorsqu'environ 6 confirmations auront eu lieu au moins, on considèrera que l'argent est vraiment à vous.

Payer en Bitcoins

Vos Bitcoins sont bien au chaud sur votre machine ? Parfait !
Et si vous les dépensiez maintenant ? Certes, vous pouvez aussi les garder pour les revendre plus tard contre des euros, en espérant que le prix du Bitcoin ait augmenté, mais c'est un jeu ennuyeux (et dangereux).

Les boutiques

Les boutiques qui acceptent les Bitcoins sont de plus en plus nombreuses. Vous avez des annuaires comme :

- http://usebitcoins.info : liste des sites acceptant les Bitcoins
- https://coinmap.org : liste des commerces acceptant les Bitcoins

Vous trouverez plus facilement des sites qui acceptent les Bitcoins que des commerces dans la rue. Quelques idées :

- https://bitgear.co : vend des Tshirts à l'effigie du Bitcoin (un peu ironique d'acheter des Bitcoins pour s'offrir un Tshirt Bitcoin, mais bon !)
- https://store.bitcoin.com/ : un peu plus de choix, des Tshirts toujours mais aussi des mugs et des stickers.
- https://www.shopify.com/blog/10480345-75-places-to-spend-your-bitcoins : une liste de boutiques très différentes sur Shopify qui acceptent les Bitcoins.

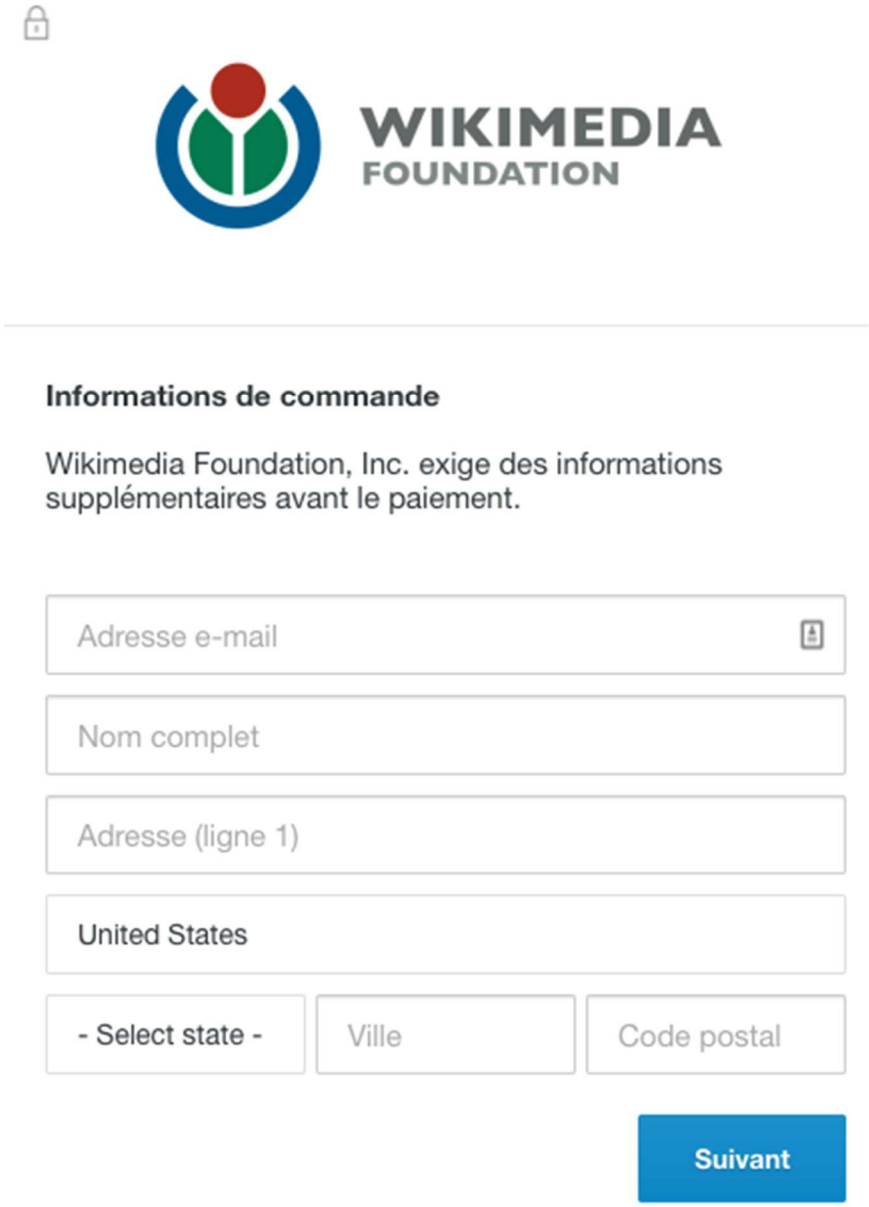
Il y en a d'autres, je vous laisse faire vos recherches !

Tous ces efforts pour acheter un Tshirt Bitcoin !

Les dons

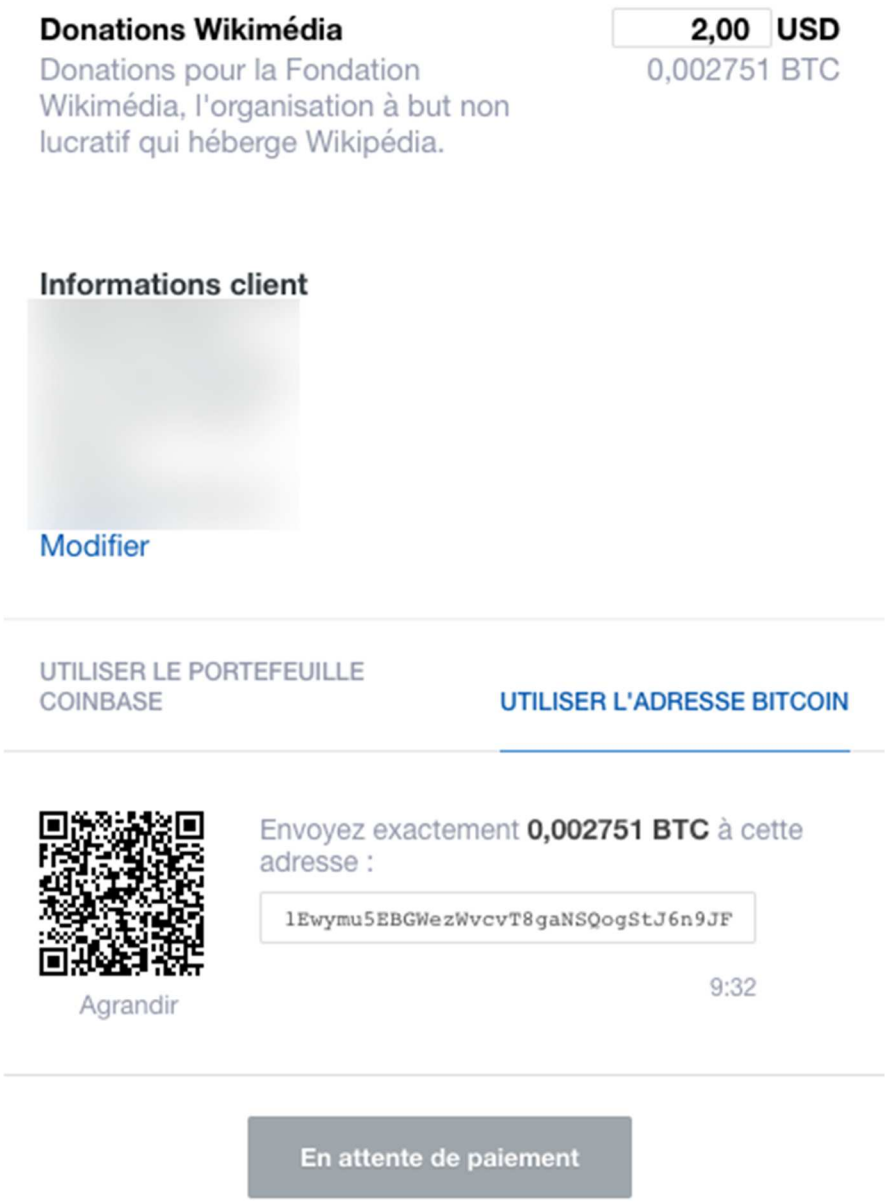
Le Bitcoin est rapidement devenu un moyen de faire des dons pour des associations à but non lucratif et différents projets open source. Voici une liste de projets acceptant des dons en Bitcoins. Voyez si vous pouvez donner un peu à l'un d'eux.
Si vous hésitez, vous pouvez donner par exemple à la fondation Wikimedia (c'est-à-dire à Wikipedia). Combien de fois avez-vous utilisé Wikipedia et combien de fois avez-vous donné, hmm ? Ca peut être l'occasion de réparer les choses.

Parmi les moyens de paiement proposés sur la page, vous verrez qu'il y a le Bitcoin. Cliquez sur "Donner en Bitcoins". Une page s'ouvre vous demandant quelques renseignements :



Formulaire de don pour Wikimedia

Remplissez le formulaire, puis indiquez combien vous voulez donner. Tous les montants, même les plus petits, font la différence !
La page vous donne alors une adresse à laquelle envoyer vos Bitcoins, avec le montant exact à transmettre :

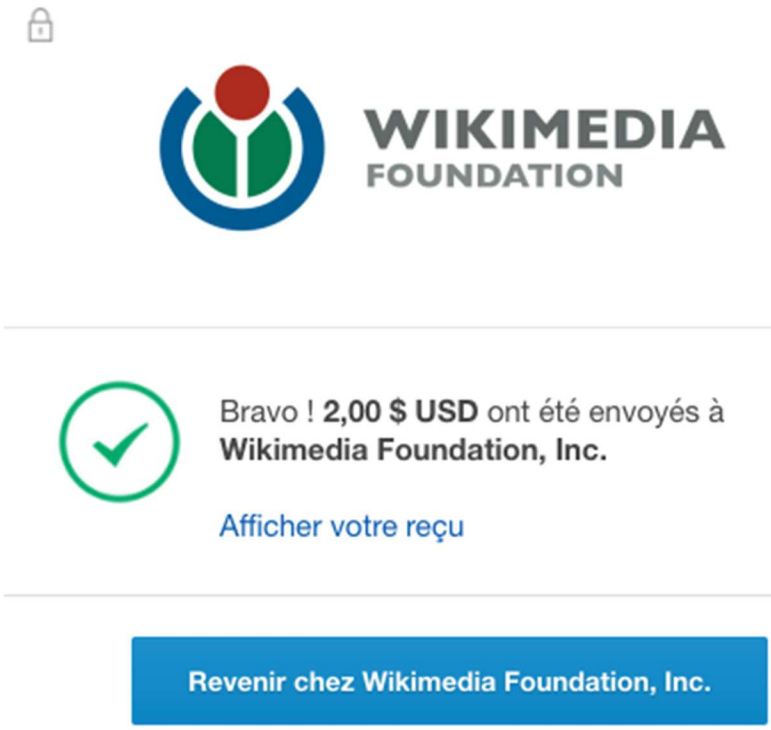


On vous communique l'adresse à laquelle envoyer votre don

Utilisez Electrum pour envoyer l'argent (copiez l'adresse dans la section "Send"). Au bout de quelques secondes, le bouton "En attente de paiement" se transforme :

Le paiement a été reçu, mais il faut attendre un peu que la transaction soit confirmée

Bravo, vous avez fait votre bonne action du jour !



Les portefeuilles de Bitcoins pour smartphones ne manquent pas, bien au contraire ! C'est généralement la solution idéale si vous voulez vous balader avec vos Bitcoins dans la poche.
Je vous propose de jeter un oeil à breadwallet, qu'on retrouve sur iOS et Android, mais vous pouvez choisir une autre application si vous voulez.

Configurer son portefeuille sur breadwallet

La première fois que vous lancez l'application, celle-ci vous propose de créer un nouveau portefeuille ou de récupérer un portefeuille existant.

Accueil de breadwallet

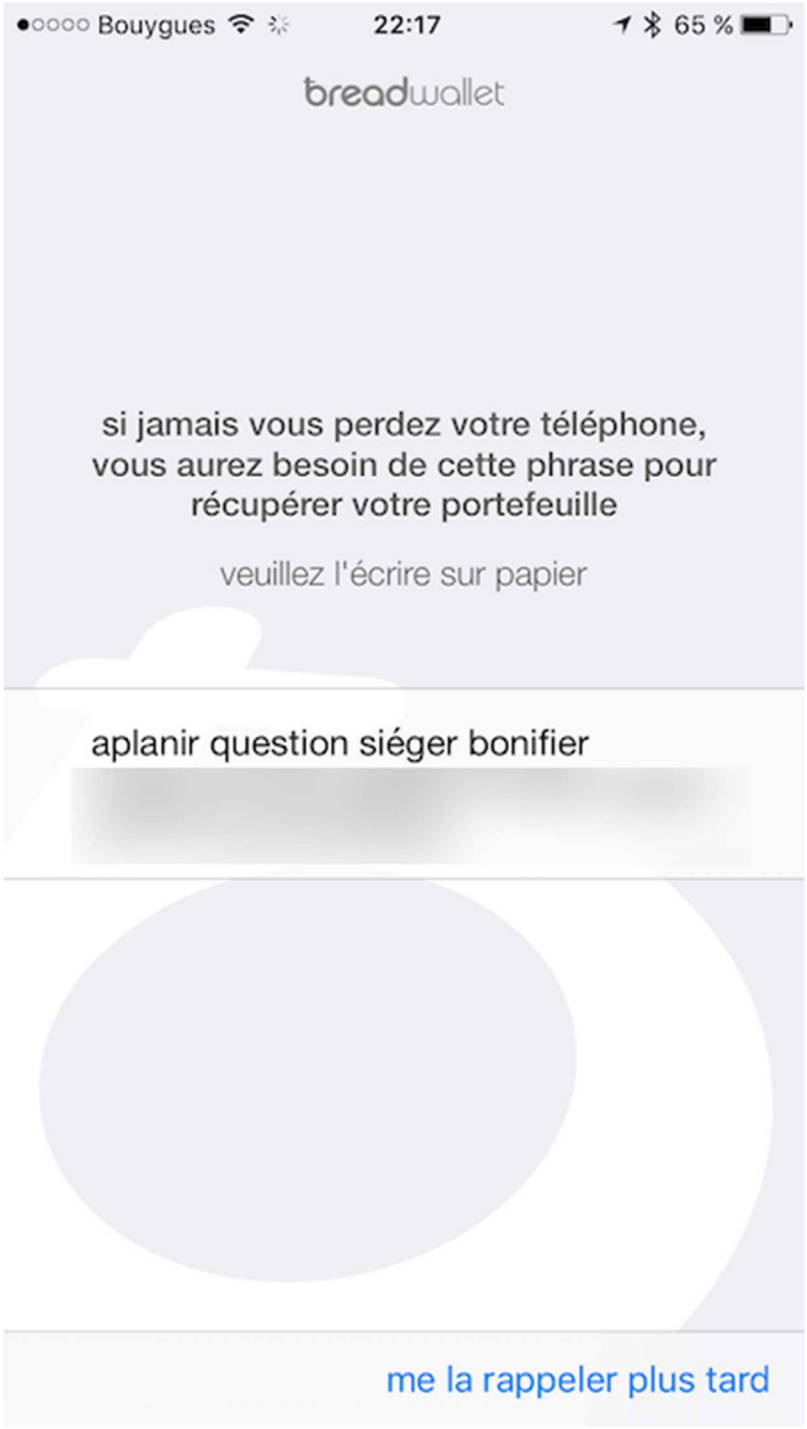
La première fois, vous allez probablement créer un nouveau portefeuille.

Création de la phrase de récupération

Breadwallet vous avertit qu'il va générer une phrase de récupération (c'est la fameuse graine, **très très importante**). On vous demande de faire très attention à la phrase qui va s'afficher : notez-la sur papier et nulle part ailleurs.

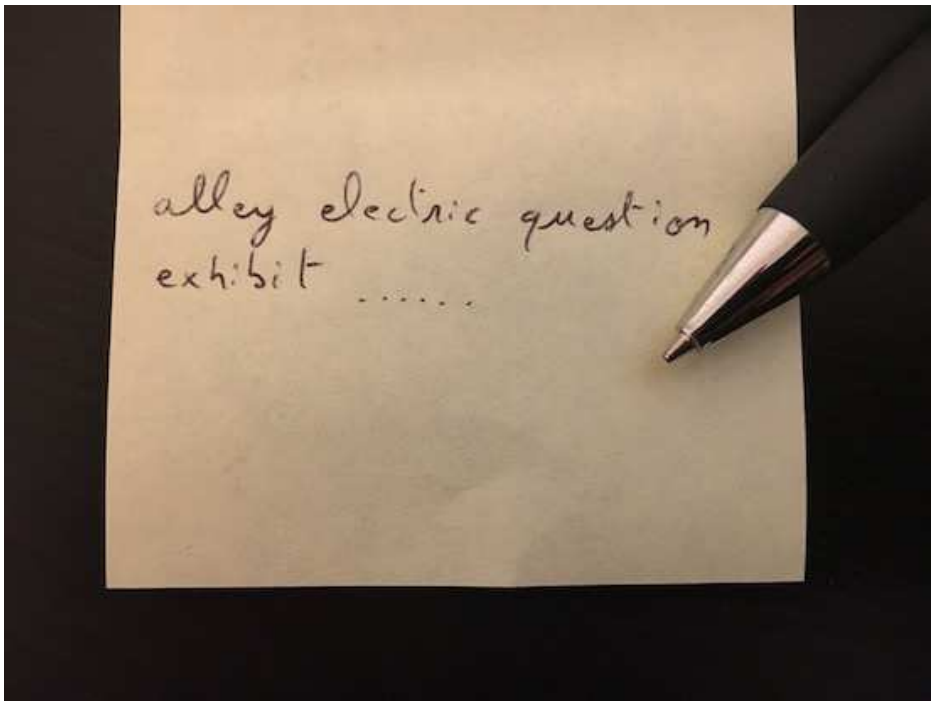
On vous avertit avant de vous afficher la graine

Ensuite, la graine s'affiche enfin. C'est une suite de mots (phrase de récupération) :



Votre graine s'affiche. NOTEZ-LA !

Vous devriez bien noter la suite de mots sur une feuille de papier comme ceci :



La graine doit être notée sur une feuille de papier

Si vous perdez votre téléphone, vous pourrez récupérer tout votre argent à partir de votre graine (il suffira de la saisir à l'initialisation de l'application). Votre graine devrait être écrite sur papier et nulle part ailleurs. Si vous pouvez placer ce papier dans un coffre-fort, c'est encore mieux !

Dans tous les cas, n'en laissez jamais une trace informatique. Pas de capture d'écran, pas de fichier sur Dropbox, rien.

Utiliser l'application

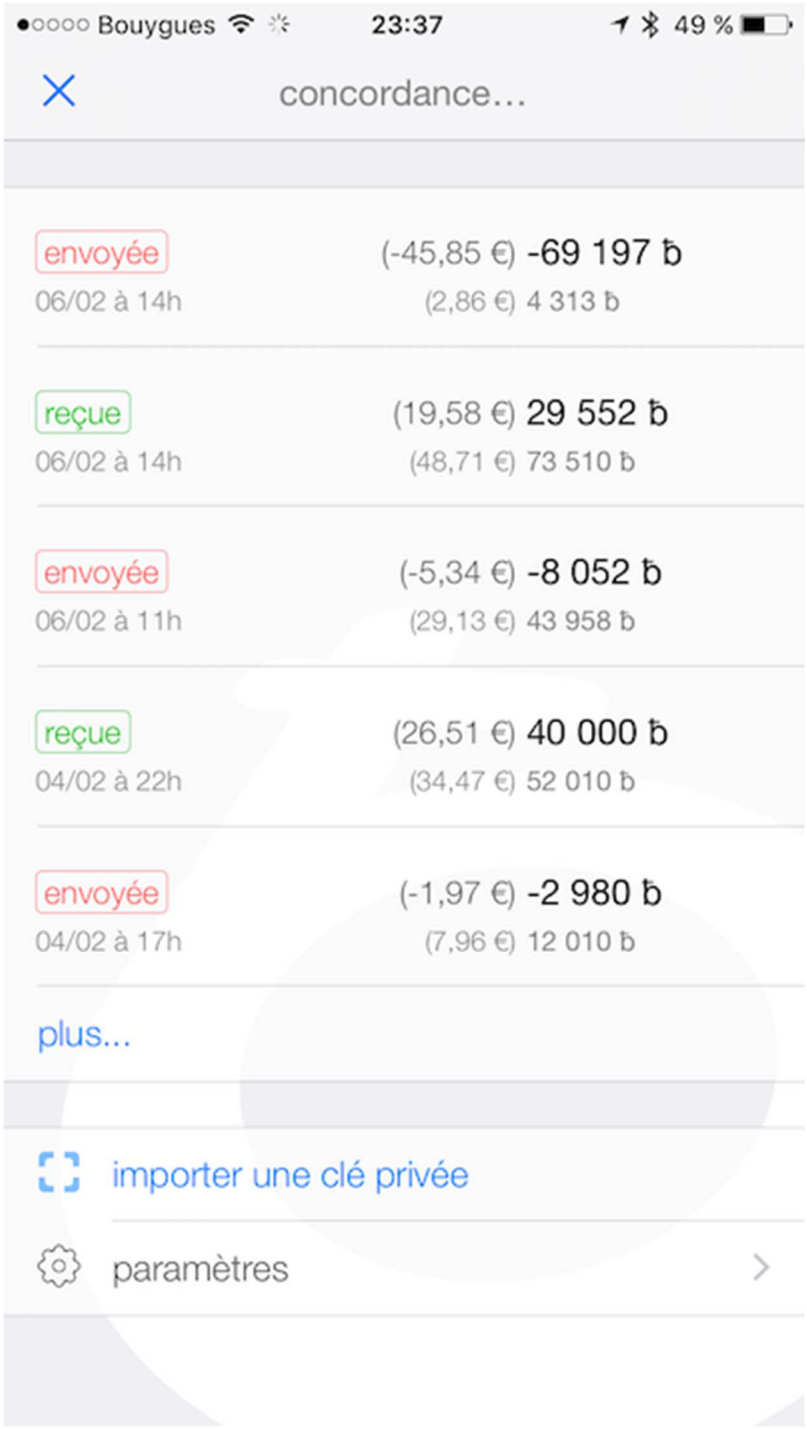
La première fois, l'application va s'initialiser et télécharger une version abrégée de la Blockchain (le mot "concordance" s'affiche en haut). Ca va plus vite mais ça prend du temps quand même.
Au bout d'un moment, vous voyez alors votre portefeuille :

Accueil de breadwallet : vous permet d'envoyer des Bitcoins

Votre solde est écrit en haut (ici 0 bits, soit 0,000000 BTC, soit 0,00 €). Vous pouvez envoyer de l'argent en numérisant un QR Code, ou en saisissant une adresse copiée depuis le presse-papier.
Si vous *slidez* à droite, un autre écran s'affiche avec un QR Code et une adresse. Cela vous permet de recevoir des paiements à cette adresse.

breadwallet vous donne une adresse et un QR Code à communiquer pour que vous puissiez recevoir de l'argent

Enfin, si vous appuyez sur le menu en haut à gauche, vous retrouverez tout l'historique de vos transactions. Voici ce que ça donne lorsque vous avez un peu d'historique :



L'historique de transactions sur votre portefeuille breadwallet

Vous voilà prêts à vous balader avec un vrai portefeuille numérique en Bitcoins dans la poche !

Portefeuille matériel

Les portefeuilles "hardware" sont ce qui se fait de mieux en matière de sécurité si vous voulez protéger vos Bitcoins. Pourquoi ? Parce que vos clés sont stockées *dans* un matériel dédié et n'en sortent jamais. Elles ne peuvent pas être récupérées à distance par quelqu'un via Internet.

Ces portefeuilles sont encore très récents mais sont déjà prometteurs. Ils sont peu nombreux, mais on peut déjà citer Ledger, Trezor et Keepkey par exemple. Le coût varie de 20€ à près de 100€ (les plus chers sont plus pratiques et un peu plus sûrs car ils possèdent un écran de confirmation intégré).
Dans ce chapitre, je vais vous montrer comment fonctionne le Ledger Nano S, un appareil français qui rencontre un certain succès.

Aperçu du Ledger Nano S

Le Ledger Nano S se présente sous une forme proche d'une clé USB :

Boîte du Ledger Nano S

L'appareil se branche via un câble micro USB à l'ordinateur. Lorsque vous l'allumez la première fois, il va s'initialiser et vous demander de définir un code PIN pour le déverrouiller à l'avenir.
Il va aussi créer une graine (vous savez, la fameuse liste de mots qui permet de générer les clés). Ces mots s'affichent un par un à l'écran. Des boutons au-dessus de l'appareil vous permettent de les faire défiler.

Le Ledger affiche les mots de la graine

Notez ces mots sur une feuille de papier ! Une feuille est d'ailleurs fournie avec le matériel. Conservez-la dans un lieu sûr (un vrai coffre-fort par exemple). Si vous perdez votre Ledger, vous pourrez récupérer l'accès à vos Bitcoins grâce à cette liste de mots.
Une fois que vous avez noté tous les mots de la graine, le menu principal s'affiche :

Menu du Ledger Nano S

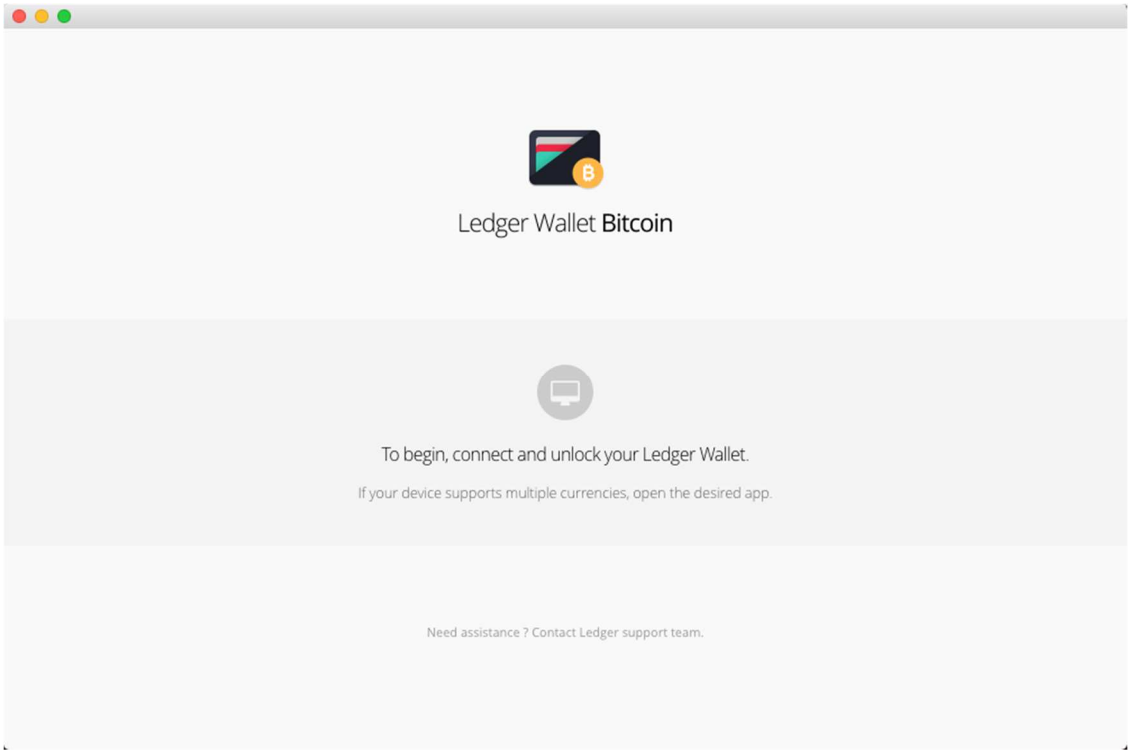
L'appareil est compatible avec plusieurs monnaies et systèmes d'authentification. Sélectionnez "Bitcoin" en appuyant sur les deux boutons à la fois. Votre portefeuille est alors déverrouillé et connecté à votre ordinateur.
S'il est déverrouillé, ça veut dire qu'un virus sur mon ordinateur pourrait maintenant récupérer les clés ?!
Non, pas du tout !

Les clés restent sur votre appareil et *ne peuvent techniquement pas en sortir*. C'est l'appareil qui signe les transactions, et autorise donc l'argent à sortir de chez vous.
Dans le pire des cas, un virus pourrait tenter d'appeler le Ledger connecté à l'ordinateur pour lui demander de signer la transaction, mais l'écran du Ledger vous demanderait une confirmation. Il faut presser *physiquement* les boutons de l'appareil pour confirmer.

Utilisation du Ledger Nano S

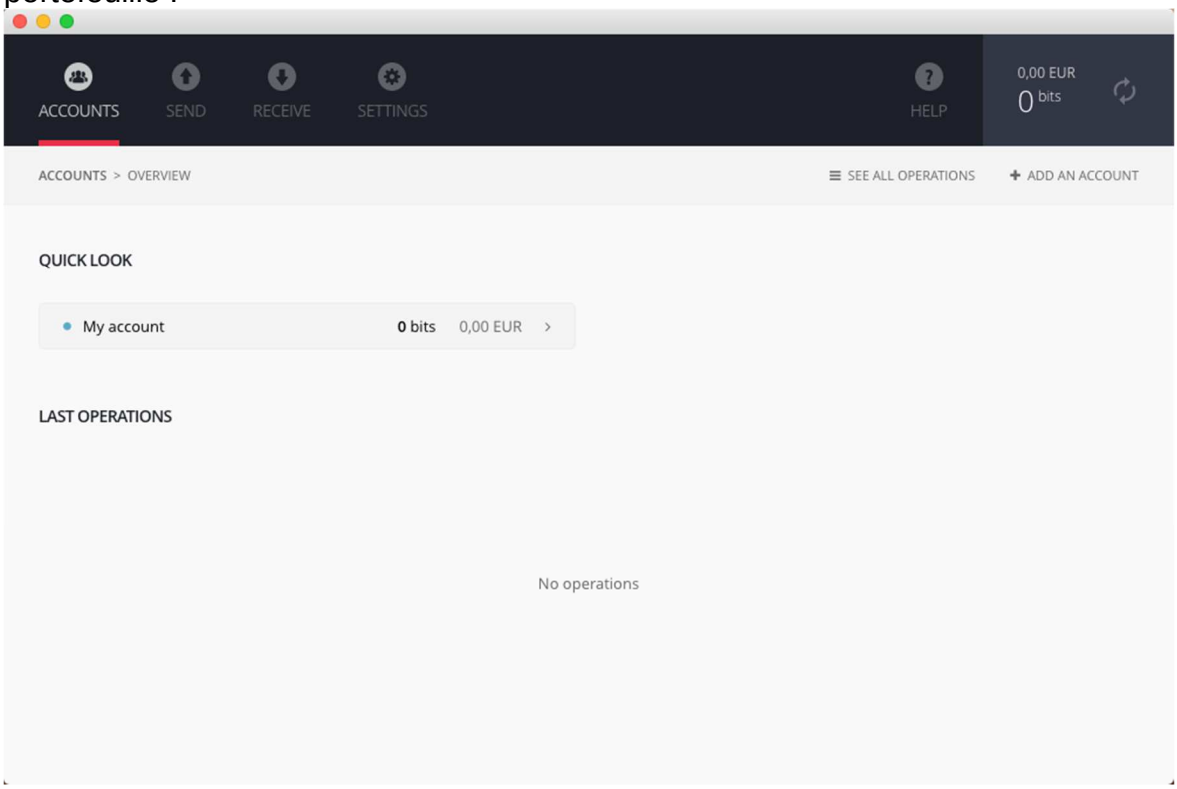
Dans le cas du Ledger, une application pour ordinateur est fournie sur le site du constructeur. Elle est faite pour se connecter au matériel.
Comme l'appareil est basé sur un standard, vous pouvez aussi utiliser le Ledger avec une autre application comme Ethereum ! Créez simplement un portefeuille de clé matériel avec Ethereum, tout en ayant connecté le Ledger déverrouillé à votre ordinateur.
Bonne nouvelle : l'application Ledger Wallet Bitcoin est bien plus jolie que les autres que j'ai pu tester. Elle se présente sous la forme d'une application pour Google Chrome.

Si vous la lancez sans connecter et déverrouiller votre Ledger, elle ne pourra rien faire :



L'application ne peut fonctionner sans Ledger connecté

Branchez donc votre Ledger et déverrouillez-le. L'application peut alors afficher votre portefeuille :

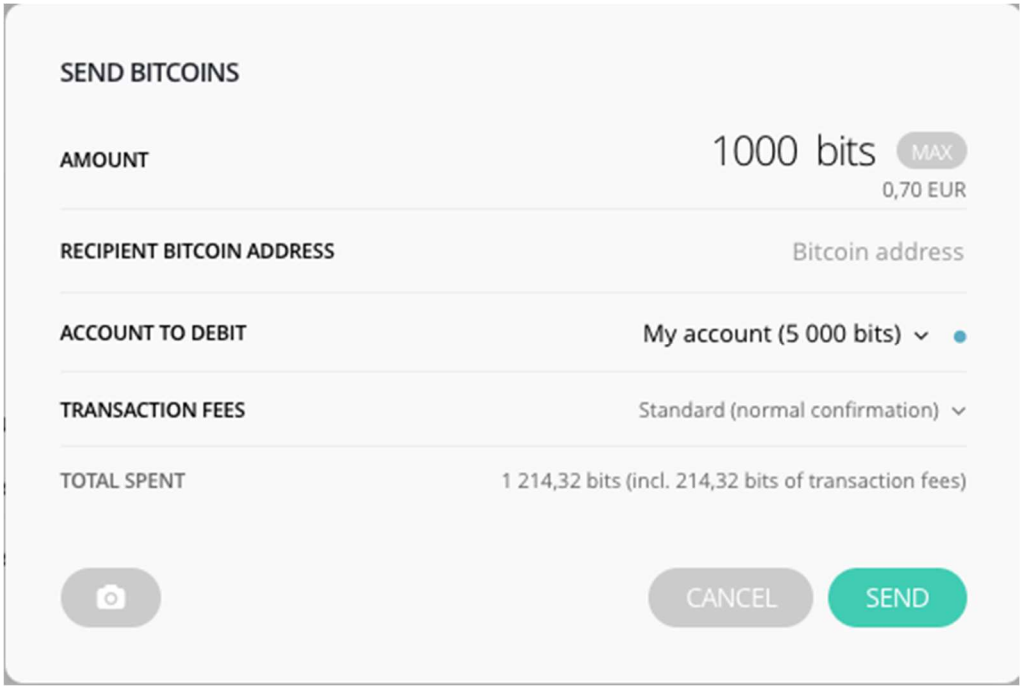


L'application une fois le Ledger déverrouillé

Vous avez des écrans pour envoyer et recevoir des Bitcoins. Le principe est le même... à une exception près, vos Bitcoins ne peuvent pas être envoyés sans une confirmation *physique* depuis l'appareil Ledger.

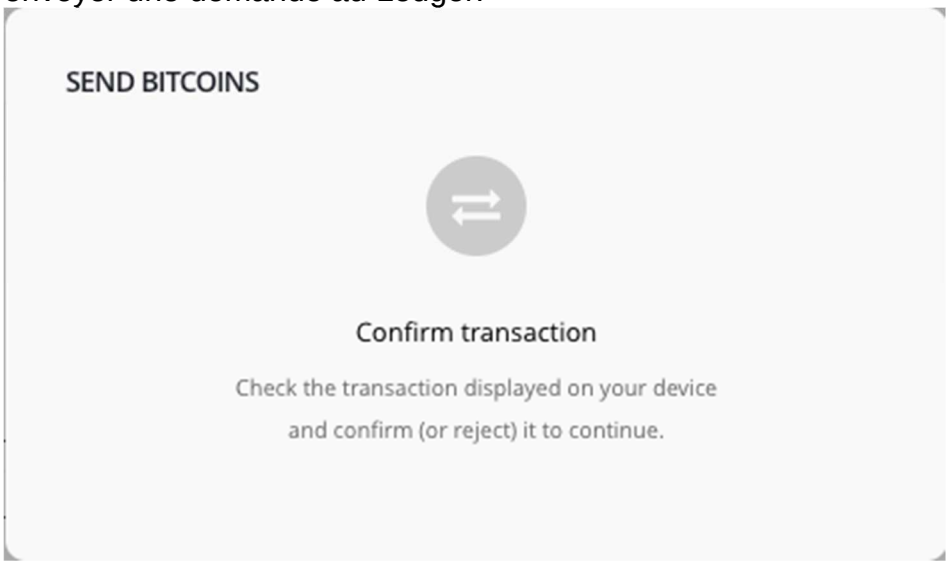
La méthode sécurisée pour envoyer de l'argent avec le Ledger

Cliquez sur "Send" pour demander à envoyer de l'argent :



Ecran d'envoi de Bitcoins depuis l'application Ledger

Rien d'extraordinaire pour le moment. Vous indiquez le montant, l'adresse du destinataire et vous cliquez sur "Send". Sauf que voilà, l'application n'est pas capable d'envoyer l'argent elle-même vu que les clés sont sur votre appareil. Elle va donc envoyer une demande au Ledger.



L'application n'a pas accès aux clés : vous devez confirmer sur le Ledger

Vous verrez que votre Ledger attend maintenant une confirmation pour signer la transaction :

Le Ledger vous demande de confirmer la transaction en appuyant sur un bouton

L'écran affiche le montant de l'envoi, mais aussi l'adresse du destinataire. Vérifiez bien que c'est ce que vous voulez faire et validez. L'argent est parti !
Ce système est sûr au point qu'on peut l'utiliser même sur une machine infectée. En effet, même dans le pire des cas, personne ne pourra envoyer l'argent à moins d'avoir accès physiquement au Ledger pour confirmer la transaction.
Voilà, si vous comptez conserver beaucoup d'argent en Bitcoins un jour, vous saurez qu'il est préférable d'investir dans ce type de matériel !

Le Bitcoin vous plaît ? Pour vous c'est le futur ? Vous êtes déjà en train de brûler vos billets en euros dans un feu de joie ?
Pas si vite moussaillon ! Rien n'est jamais parfait et le Bitcoin ne fait pas exception. Rivalités, coups bas, rebondissements dans les médias... ici, c'est un peu Dallas dans le cyberespace !

Un Bitcoin sans parent

Qui est à l'origine du Bitcoin ? Nous ne connaissons que son pseudonyme, un certain Satoshi Nakamoto. Est-ce un homme, une femme ? Vit-il en Asie, en Europe, en Afrique ? Ou bien est-ce en fait un groupe de personnes ?
Pour l'instant, **personne n'en sait rien**. Il n'y a que des spéculations, quelques coups de théâtre, mais rien de concret.
Certains pensent qu'il s'agit de Nick Szabo, activiste qui a participé à la création d'un ancêtre du Bitcoin, le Bit Gold. Ils sont même allés jusqu'à comparer la façon dont parle Nick avec les messages de Satoshi Nakamoto. Quant à l'intéressé, il dément être le père du Bitcoin.
Les parents possibles du Bitcoin ne manquent pas parmi les spécialistes de la cryptographie, mais personne n'a pu prouver qui était vraiment derrière le Bitcoin. Un certain Craig Steven Wright, un australien, a bien prétendu être le père du Bitcoin pendant quelques mois. Une histoire rocambolesque relayée dans les médias qui a finalement fait pschit, puisqu'il a reconnu ne pas être en mesure de le prouver dans un ultime article intitulé "I'm sorry".


Craig Wright : "Je suis le créateur du Bitcoin !... En fait, non, rien."

Vous imaginez bien que cela alimente les théories du complot. Pour certains, ce serait un projet de la NSA, pour d'autres un consortium de plusieurs entreprises technologiques (oui, si vous assemblez SAmsung, TOSHIba, NAKAmichi et MOTOrola, ça fait SATOSHI NAKAMOTO, c'est bien LA PREUVE !).
Qu'est-ce que ça change en fait, de connaître l'identité du créateur du Bitcoin ?
Pas grand chose en réalité. Il ne contrôle plus la monnaie car le logiciel est open source. Bitcoin est aujourd'hui géré par des développeurs bien identifiés.
En revanche, cela alimente toujours les spéculations les plus folles car, techniquement, Satoshi Nakamoto possède toujours beaucoup de Bitcoins. En effet, il a été le premier mineur et on peut calculer combien de Bitcoins il possède. D'après cet article, il détiendrait environ **1 million de Bitcoins** (à l'heure où j'écris ces lignes, cela fait près d'1 milliard de dollars tout de même).
L'identité de Satoshi Nakamoto risque d'être révélée le jour où certains de ses anciens Bitcoins seront dépensés. En effet, les transactions étant publiques, on pourra tracer l'argent et remonter potentiellement jusqu'à son identité.

Taille des blocs

Cependant, l'un des plus gros enjeux n'est pas la paternité du Bitcoin (bien que cela attire beaucoup les journalistes)
Non, le gros sujet de débat est celui de **la taille des blocs**. Depuis le début, la taille d'un bloc de Bitcoin est fixée à 1 Mo, ni plus ni moins. Cela veut dire qu'on peut mettre un nombre limité de transactions dans chaque bloc (dans chaque "livre de comptes"). Aujourd'hui, nous avons atteint une sorte de saturation du réseau. Il y a tellement de transactions en Bitcoins que chaque bloc fait 1 Mo ou presque.

Index Blocs récemment extraits de la blockchain bitcoin — **Près de 1 Mo !** — Plus...

Hauteur	Âge	Transactions	Total envoyé	Relayé par	Taille (kB)
446139	12 minutes	1678	6,643.41 BTC	AntPool	998.17
446138	21 minutes	172	332.27 BTC	HaoBTC	998.12
446137	22 minutes	665	2,118.07 BTC	HaoBTC	998.08

La plupart des blocs font 1Mo (ou presque) : ils sont complets !

Qu'est-ce que ça signifie ? Quel est le risque ?

Lorsqu'un bloc est complet, vous ne pouvez pas ajouter votre transaction et devez attendre la transaction suivante. En réalité, vous pouvez toujours dépenser et acheter

des Bitcoins... mais le réseau met plus de temps à le prendre en compte, les confirmations sont plus longues.
Pourquoi ne pas augmenter cette taille de bloc de 1 Mo ?
Cela paraît être une bonne idée... après tout, la taille initiale de 1 Mo est un peu arbitraire. Sauf que voilà, les mineurs ne sont pas d'accord entre eux. Désormais, nous avons donc 2 camps :

- Ceux qui pensent qu'il faut **augmenter la taille maximale des blocs**. Ils sont allés jusqu'à créer un *fork* du Bitcoin, qu'ils ont appelé le Bitcoin Cash. Le Bitcoin Cash est une nouvelle monnaie dérivée du Bitcoin, qui est désormais totalement indépendante.
- Ceux qui pensent qu'il ne faut **surtout pas changer la règle d'origine**, car cela signifie que le réseau serait plus centralisé qu'auparavant. Ils ont néanmoins trouvé quelques "astuces" fin juillet 2017 pour gagner un peu de place tout en conservant la limite de 1 Mo du Bitcoin.

Il est intéressant de noter qu'avec Bitcoin les utilisateurs votent véritablement avec leur puissance de calcul. Lorsque la majorité des utilisateurs fait tourner un nouveau logiciel, les règles du réseau changent.

Une monnaie volatile

Rien ne garantit que le Bitcoin ne va pas disparaître subitement... et en tout cas ce n'est certainement pas une monnaie stable ! Si vous envisagiez de garder (beaucoup) d'argent en Bitcoin, réfléchissez-y à deux fois : **êtes-vous prêt·e à prendre le risque de tout perdre ?**
La monnaie peut fluctuer brutalement. Un jour vous pouvez acheter 1 BTC pour 400€, et quelques semaines plus tard cela n'en vaut plus que 200€.

Le prix du Bitcoin peut varier brutalement dans un sens et dans l'autre
Comme vous le voyez sur ce graphique, cela monte aussi vite que cela descend. La valeur de vos Bitcoins peut donc varier très rapidement.

Par ailleurs, on ne peut pas exclure le scénario catastrophe où une faille dans le fonctionnement du Bitcoin serait découverte. A priori, le système est solide... jusqu'à présent. Mais si quelqu'un découvre une faille, il est possible que le cours du Bitcoin chute drastiquement.

Exister face aux altcoins

Aujourd'hui, le Bitcoin n'est plus seul. Il existe de nombreux "altcoins" (monnaies alternatives) dont on va parler un peu plus en détail dans le prochain chapitre.
Toutes ces monnaies reposent sur le principe d'une blockchain, mais cela ne les empêche pas d'être parfois très différentes et innovantes dans leur fonctionnement.
Par ailleurs, les banques commencent à être conscientes du danger que cela peut représenter à terme pour leur existence même (le Bitcoin étant conçu pour fonctionner sans banque). Elles tentent de développer leurs propres monnaies et parlent régulièrement de la **technologie blockchain**.
En quelques années, Bitcoin est devenu en quelque sorte **le papy des monnaies électroniques**. Pourtant, il s'en sort encore étonnamment bien. La mort du Bitcoin a été pronostiquée un nombre incalculable de fois, et pourtant il ne s'est jamais échangé autant de Bitcoins.

Bitcoin n'est plus la seule monnaie électronique. Il est challengé par de nombreuses autres monnaies électroniques (les "altcoins") qui se sont inspirées de son fonctionnement, parfois en l'améliorant de façon très intéressante.
Si les altcoins sont nombreux, cela n'empêche pas le Bitcoin d'être de loin la monnaie électronique la plus populaire encore aujourd'hui.
Faisons donc un petit tour d'horizon de quelques uns des altcoins !

Bitcoin Cash

Bitcoin Cash est une monnaie dérivée de Bitcoin. Elle a été créée début août 2017, suite à des désaccords entre les mineurs du Bitcoin à propos de la taille maximale des blocs.
Que s'est-il passé ?
Le Bitcoin ayant connu beaucoup de succès, il y avait de plus en plus de transactions chaque minute et les blocs se remplissaient à vive allure. La taille maximale des blocs avait été initialement fixée à 1 Mo et jamais changée jusqu'alors. Le réseau arrivait à saturation. Cela signifiait que les transactions prenaient plus de temps à être validées (un comble pour une monnaie qui peut en théorie être transférée très rapidement !).
Suite à ce désaccord :

- Ceux qui ne voulaient pas augmenter la taille des blocs sont restés sur **Bitcoin**. Ils ont quand même fait quelques concessions en implémentant des solutions techniques comme Segregated Witness qui donnent un peu d'air sans avoir à augmenter la taille des blocs.
- Ceux qui voulaient augmenter la taille des blocs ont créé **Bitcoin Cash**, une monnaie dérivée du Bitcoin (on parle de *fork*). La taille des blocs y a été montée à 8 Mo.
  Le Bitcoin et le Bitcoin Cash partagent le même historique de Blockchain jusqu'au 1er août 2017, date à partir de laquelle le Bitcoin Cash a été créé.

Nous ne savons pas si une monnaie va l'emporter sur l'autre (les deux peuvent très bien coexister). Une chose est sûre : faites le plein de popcorn, car le feuilleton n'est pas terminé !

Le Bitcoin Cash a été créé suite aux désaccords entre mineurs de Bitcoin

Litecoin

Litecoin est une monnaie alternative fortement inspirée du Bitcoin. En fait, le code est à la base le même mais il a été amélioré pour proposer quelques avantages :

- Les blocs sont minés toutes les 2 min 30 environ au lieu de toutes les 10 min
- Les transactions sont ainsi confirmées plus rapidement
- On peut miner des Litecoin avec un ordinateur standard

Voilà donc une monnaie assez proche du Bitcoin qui a su rester simple. Sa valeur est en revanche bien plus faible à l'heure où j'écris ces lignes.

Le Litecoin est très proche du Bitcoin

Dogecoin

Dogecoin est une autre monnaie électronique... dont on ne sait pas toujours bien si c'est juste pour rire ou un peu sérieux quand même. Elle met en avant un célèbre *meme* d'Internet, sous la forme du Shiba Inu, une race de chien japonais. Oui, des fois, il ne faut pas chercher à comprendre.

Le Dogecoin, une monnaie pour le lol ?

Techniquement, le Dogecoin est un dérivé du Litecoin, qui est lui-même un dérivé du Bitcoin. Il ne vaut pas bien cher. Oui mais voilà, il y a un chien sur leur logo, et ça, ça change tout.

Ethereum

Plus sérieusement, Ethereum est probablement l'un des plus sérieux challengers du Bitcoin aujourd'hui.
Son originalité vient du fait qu'il permet de faire tourner des programmes appelés "*Smart contracts*" sur tous les ordinateurs du réseau simultanément. Le mécanisme n'est pas évident à comprendre, mais il mérite clairement de s'y pencher si le sujet vous intéresse.

Ethereum est bien plus qu'une monnaie... c'est un moyen de faire tourner des programmes de contrat
En quelques mots, vous pouvez écrire un programme qui sera exécuté par tous les ordinateurs de la blockchain d'Ethereum. Que fait ce programme ? C'est à vous de le décider. On peut s'en servir par exemple pour :

- Créer une sorte de Kickstarter décentralisé. Vous avez un projet, vous avez besoin d'argent, vous lancez un smart contract sur Ethereum. Dans ce modèle, des gens peuvent vous prêter de l'argent sans risque que vous partiez avec sans rien dire : le code du programme indique que l'argent ne vous sera réellement distribué que si vous atteignez un objectif.
- Créer une entreprise dans la blockchain. Les parts de cette entreprise, et donc les droits de vote, sont définies par le programme. En fonction du nombre de parts que vous achetez, vous obtenez la possibilité d'influer sur le fonctionnement de l'entreprise.

- Pourquoi pas un gouvernement dans la blockchain, dont la constitution serait écrite dans un programme et ne pourrait pas être changée.

Je... ne comprends rien ?!
C'est normal, ce n'est pas évident pour moi non plus rassurez-vous.

En gros, vous pouvez acheter des objets avec Ethereum, mais l'intérêt de la monnaie vient de sa capacité à gérer des contrats sous forme de programmes informatiques. Peut-être qu'un jour, vous n'aurez plus besoin de signer une feuille de papier chez un notaire ou un avocat : vous signerez un contrat électronique dans la blockchain d'Ethereum.

Un jour, vous n'aurez plus besoin de signer des contrats... ils seront écrits sous forme de programmes dans la blockchain d'Ethereum !
Une fois un contrat lancé en ligne, personne ne peut l'arrêter (sauf si le code du contrat l'a prévu lui-même). En clair, le contrat peut tourner indéfiniment sur le réseau. Tous les ordinateurs sont en mesure de le faire tourner. C'est à la fois fascinant et flippant (le jour où une intelligence artificielle tourne sur ce réseau, personne ne peut la débrancher).

Si vous voulez en savoir plus sur le langage utilisé, lisez le cours sur le langage Solidity sur le site d'Ethereum.

Zcash

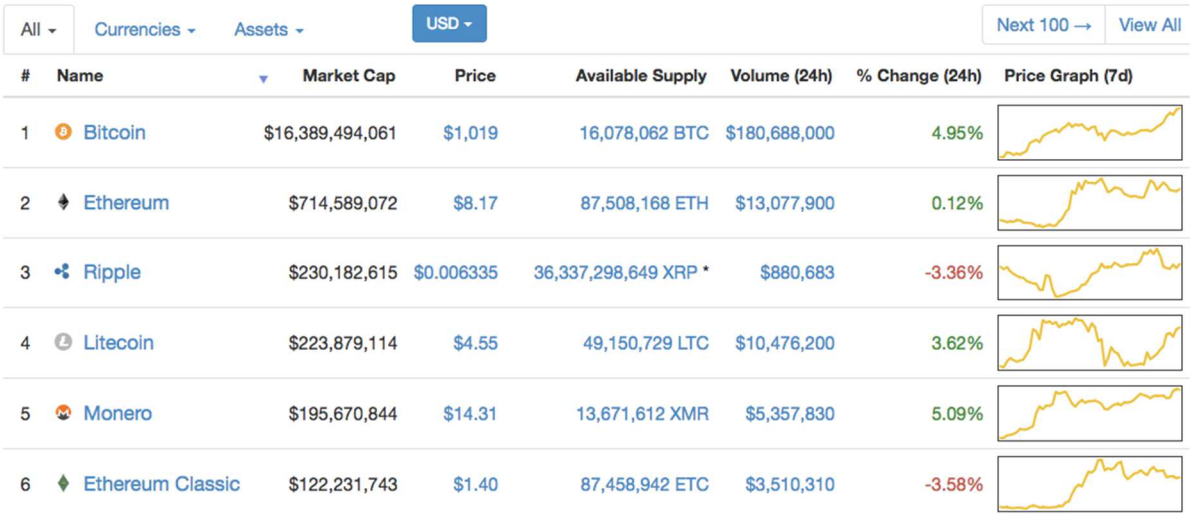
Zcash est un nouveau type de monnaie qui se veut **réellement anonyme**.
Je croyais que Bitcoin était anonyme ?
Erreur ! Avec Bitcoin, les transactions sont publiques et il est en théorie possible de remonter jusqu'à la personne physique qui possède l'argent (on peut "suivre l'argent" et voir où il est dépensé). Si vous parcourez blockchain.info vous pouvez voir tout ce qu'il s'y passe... eh bien avec Zcash cela ne sera pas possible

Zcash est basé sur un nouveau système appelé "zero knowledge proof". Cela permet de prouver que vous avez effectué un calcul sans nécessiter qu'une autre personne refasse le même calcul pour savoir s'il était vrai. D'une certaine façon, vous pouvez dire "ceci est vrai" et tout le monde vous croira (et vous n'aurez pas pu mentir).

Zcash est un nouveau type de cryptomonnaie totalement anonyme
Cette monnaie a été en développement 2 ans par des spécialistes des cryptomonnaies. Elle est prometteuse mais risque d'être encore plus volatile que les autres à cause de sa jeunesse !

... et des dizaines d'autres !

Terracoin, Zetacoin, Unobtanium, Infinitecoin, Primecoin, Yacoin... Vous pouvez découvrir des tonnes de monnaies plus ou moins obscures sur le site altcoins.com.
Vous pouvez comparer les valeurs de ces altcoins sur un site comme coinmarketcap.com :



#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$16,389,494,061	$1,019	16,078,062 BTC	$180,688,000	4.95%	
2	Ethereum	$714,589,072	$8.17	87,508,168 ETH	$13,077,900	0.12%	
3	Ripple	$230,182,615	$0.006335	36,337,298,649 XRP *	$880,683	-3.36%	
4	Litecoin	$223,879,114	$4.55	49,150,729 LTC	$10,476,200	3.62%	
5	Monero	$195,670,844	$14.31	13,671,612 XMR	$5,357,830	5.09%	
6	Ethereum Classic	$122,231,743	$1.40	87,458,942 ETC	$3,510,310	-3.58%	

Comparatif des altcoins

Un peu de vocabulaire pour comprendre ce tableau :

- **Price** : valeur d'un coin
- **Available supply** : nombre de coins disponibles
- **Market capitalization** : valeur en dollars de tous les coins de la monnaie en circulation. Ca se calcule en multipliant la valeur d'un coin par le nombre de coins disponibles (market capitalization = available supply * price).
- **Volume (24h)** : valeur des coins échangés ces dernières 24h. Permet de savoir si une monnaie est très active sur le réseau en ce moment.

Inutile de chercher à connaître toutes ces monnaies, il y en a trop. Si la plupart sont probablement vouées à disparaître par manque de succès, il faut reconnaître que le secteur des cryptomonnaies est devenu très actif grâce au Bitcoin.

Je serais bien incapable de vous dire lesquelles vont décoller. Aujourd'hui Ethereum et Zcash semblent parmi les monnaies les plus prometteuses, mais qui sait ce qu'il en sera dans quelques années voire dans quelques mois ? Une seule certitude : les choses évoluent très vite !
Certaines nouvelles cryptomonnaies lèvent des fonds auprès du grand public : on parle d'ICO (Initial Coin Offering). Cela permet notamment d'acheter des parts dans une cryptomonnaie avant son lancement.

Voilà, vous en savez plus sur le bitcoin !

A vous de jouer !

FIN