

# Bitcoin

## Principes généraux, limites et perspectives

Jean-Luc Parouty  
Institut de Biologie Structurale (IBS)  
*Jean-Luc.Parouty<at>ibs.fr*

### Résumé

*Beaucoup de choses ont été dites ou écrites concernant Bitcoin et les crypto-monnaies...*

*À la fois monnaie du crime et véritable alternative aux monnaies traditionnelles, Bitcoin présente une innovation majeure en proposant un modèle de preuve en lieu et place des modèles classiques reposant sur la délégation de confiance.*

*Bitcoin est tout à la fois un système de paiement, une monnaie et une infrastructure de notariat électronique, à même de protéger l'intégrité et l'antériorité de nos données sensibles.*

*Évolution technologique majeure, Bitcoin est indépendant de tout organisme, banque, banque centrale ou état. Entièrement libre et transparent, Bitcoin est une infrastructure communautaire et open-source.*

*En appréhendant les concepts et mécanismes de Bitcoin, nous nous efforcerons de comprendre en quoi ce modèle de preuves est novateur, quelles en sont les limites et comment il pourrait être à même de répondre (ou non) à de multiples problématiques actuellement ouvertes.*

*Cet article est composé d'une seconde partie, disponible sur [docproof.org](https://docproof.org), destinée à approfondir les aspects techniques de l'architecture Bitcoin, intitulé « Bitcoin, Éléments de compréhension technique ».*

### Licence

Creative Commons BY-NC-SA -    

### Mots-clefs

Bitcoin, cryptographie, crypto-monnaie, preuve, blockchain, p2p, minage, ECDSA, SHA256, Base58Check, RIPMD160

### Table des matières

1/ L'échange et la preuve de possession dans un monde prénumérique .....	2
1.1 Du troc aux banques centrales .....	2
1.2 De la possession directe à la délégation de confiance .....	2
2/ Bitcoin, un modèle d'échange traditionnel .....	3
2.1 À la fois « matière première » et « monnaie » .....	3
2.2 Le retour du consensus transparent .....	4
3/ Utiliser Bitcoin - Concepts fondamentaux .....	5
3.1 Alice possède des bitcoins, mais où sont-ils ? .....	5
3.2 Bob présente sa facture .....	6
3.3 Alice prépare sa transaction .....	6
3.4 Diffusion de la transaction .....	7
3.5 Intégration de la transaction au sein de la blockchain .....	8
3.6 Transaction valide vs définitive .....	10
4/ <a href="https://docproof.org">docproof.org</a> , un service de notariat électronique .....	12
4.1 Principes et objectifs .....	12
4.2 Mise en œuvre .....	12
5/ Limites et perspectives .....	13
5.1 Limites .....	13
5.2 Perspectives .....	16
Bibliographie .....	18

## 1/ L'échange et la preuve de possession dans un monde prénumérique

L'un des bénéfices immédiat de notre aptitude à vivre de manière grégaire est de pouvoir effectuer des échanges très facilement et de fait, les **échanges** occupent depuis toujours une place essentielle au sein de nos communautés.

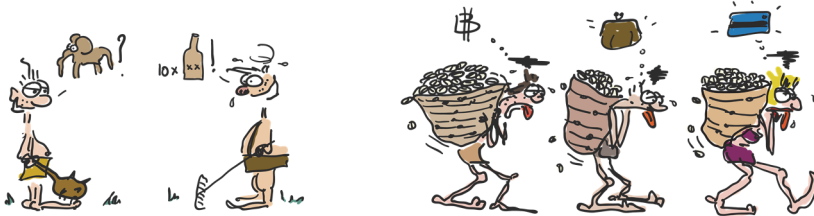
Indispensable au principe de l'échange, la possibilité de **posséder** un bien, est également centrale.

Les biens échangés ou possédés peuvent être matériels ou immatériels; idées, services, informations, et les modalités de ces échanges peuvent également être très variées : avec ou sans contreparties, entre deux personnes ou impliquant un grand nombre d'acteurs, ces derniers pouvant être des personnes physiques ou institutionnels, etc.

### 1.1 Du troc aux banques centrales

Si un échange entre deux personnes de confiance, au sein d'un même groupe, partageant des conventions identiques, est relativement simple, les choses se compliquent rapidement dès lors que la taille du groupe ou que le nombre d'acteurs augmente.

Le **troc**, atteint alors ses limites et l'usage d'un **bien de référence**, facilite alors les échanges. Sel, Coquillages, métaux furent ainsi utilisés. Le bien de référence étant garant de sa propre valeur et cette valeur étant liée à sa rareté.



L'invention de la **monnaie fiduciaire**, dont la valeur n'est plus intrinsèque, mais est garantie par un **tiers de confiance**, permet de résoudre certaines difficultés matérielles... tout en induisant l'épineux problème de la confiance vis-à-vis des émetteurs de cette monnaie.

Avec l'augmentation du nombre de transactions et l'implication d'acteurs géographiquement éloignés, d'autres outils furent imaginés. Chèques, virements et autres systèmes de compensations devinrent incontournables. Afin de faciliter les échanges, les **banques** se positionnèrent comme intermédiaires et gestionnaires, centralisant et hébergeant nos avoirs, facilitant nos transactions.

Contrôlant aussi bien **l'émission de la monnaie**, via la maîtrise du crédit ou la création monétaire, que les **mécanismes d'échanges**, les banques (et les états) ont acquis une position centrale et incontournable dans la mise en œuvre de nos échanges.

Avec l'abandon du troc, la **confiance** que nous pouvons avoir dans nos échanges est celle que nous avons en « nos » banques et états.

### 1.2 De la possession directe à la délégation de confiance

La possibilité de « prouver » la possession d'un bien est relativement simple dans le cas des biens matériels usuels. Le fait de porter l'objet étant généralement suffisant.

Dès lors que la possession peut être contestée, le témoignage d'autres membres du groupe devient nécessaire. Lorsque le groupe devient trop important, il est nécessaire de **déléguer** le soin de porter ce témoignage à une personne ou une **institution de confiance**.

À travers les banques, notaires, organismes de propriété intellectuelle, cadastres et autres *Internet registry*, notre confiance est déléguée à un grand nombre d'acteurs, dont les fonctions et missions dépassent souvent le simple fait de pouvoir témoigner de la possession d'un bien.

Nos banques sont ainsi dépositaires de nos avoirs et nous leur déléguons le soin de gérer ces avoirs.

Pouvoir établir une **preuve de possession** implique de pouvoir également **caractériser** et **dater** la possession. Lorsque le bien est matériel et statique, cette description est souvent relativement aisée et peut se faire via une particularité unique et stable, comme un numéro de série ou une adresse.

Les choses deviennent plus compliquées dans le cas de biens **immatériels** et/ou aisément **transformables**, où la caractérisation du bien doit commencer avec la **preuve** même de son **existence**.

## 2/ Bitcoin, un modèle d'échange traditionnel

Nous venons de voir que nos systèmes d'échanges reposaient sur une double délégation :

- l'utilisation de monnaies, dont l'émission et la valeur sont déléguées à des tiers de confiance,
- la mise en œuvre de nos échanges et la gestion de nos preuves de possession, également déléguées à des tiers de confiance.

Dans un cas comme dans l'autre, l'acteur d'une transaction et/ou détenteur d'un avoir, est tributaire de la **confiance** qu'il peut avoir vis-à-vis de ces **tiers de confiance**.

Le modèle **Bitcoin**, et plus généralement des **crypto monnaies**, est fondamentalement différent et peut être vu comme un retour aux fondamentaux :

- La quantité de monnaie en circulation est limitée et ne peut être augmentée arbitrairement,
- Les transactions et les avoirs ne sont plus centralisés, mais répartis et visibles par tous,
- La preuve de possession n'est plus centralisée, mais à la fois publique et détenue par le possédant.

### 2.1 À la fois « matière première » et « monnaie »

Le bitcoin peut être assimilable à une matière première finie, telle que l'or ou l'argent. Dans une décision récente, l'instance de régulation des marchés boursiers US [1] a ainsi estimé que le commerce des crypto monnaies relevait de la législation du commerce des marchandises.

A l'opposé, dans un arrêt du 22 octobre 2015, les juges de la cours de justice européenne ont estimés que les échanges de devises « traditionnelles » contre des bitcoins devaient bénéficier d'une exonération de TVA, au même titre que « les devises, les billets de banque et les monnaies qui sont des moyens de paiement légaux » [2].

Le bitcoin peut ainsi être vu comme une **monnaie** ou une **marchandise**, dont la quantité est finie et dont la valeur pourra fluctuer en fonction de l'offre et de la demande.

Les bitcoins peuvent être vendus ou achetés auprès de **places de marché**. On peut distinguer les **places de commerce**, qui permettent d'acheter directement des bitcoins (*Belgacoin, Kraken, Paymium, coinbase*, etc.) [3] et les **places d'échange**, permettant aux vendeurs et acheteurs de se mettre en relation (*bitcoin.de, localbitcoins*, etc.) [4].

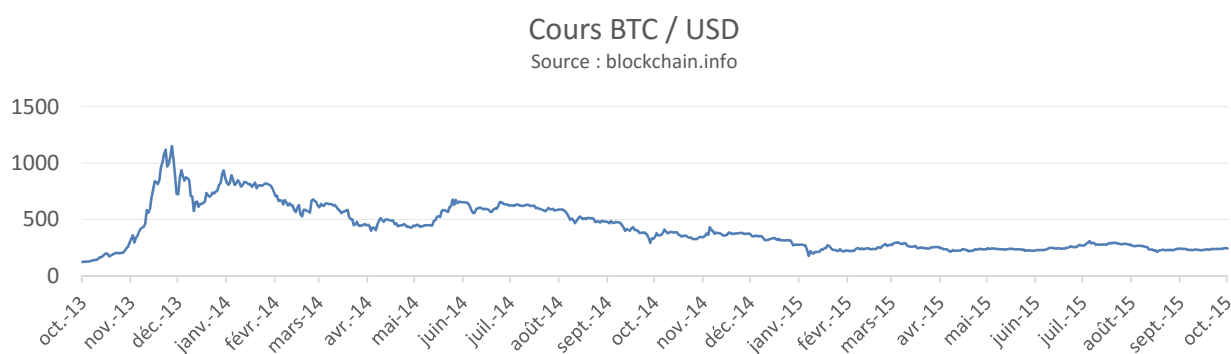


Figure 1 - Évolution du cours du bitcoin

Historiquement, le bitcoin a connu une période de **forte spéculation**, menant le cours au-delà des 1000 € fin 2013, suivi d'une période de **forts réajustements** durant l'année 2014, pour se stabiliser progressivement autour des 200 à 230 € en 2015.

La capitalisation monétaire du bitcoin est de l'ordre de 3,1 milliards d'euros (octobre 2015). De nombreuses statistiques sont disponibles en ligne [5].

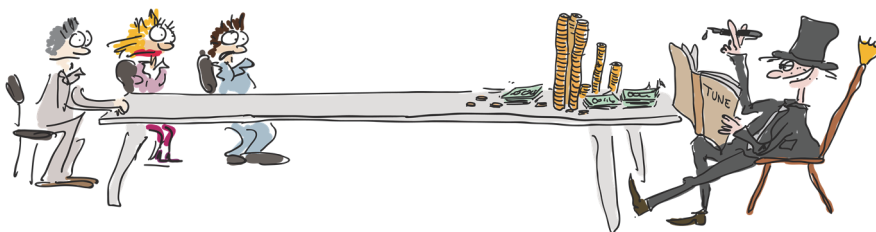
## 2.2 Le retour du consensus transparent

L'architecture Bitcoin ne fait pas qu'offrir une « unité d'échange », elle offre également la possibilité d'effectuer des échanges et de gérer nos avoirs, **sans devoir recourir à un tiers de confiance centralisateur**.

Imaginons un groupe souhaitant commercer, réuni autour d'une table.

Dans un système traditionnel, il faudrait un **banquier**, lequel tiendrait un **livre de compte**. Chaque transaction nécessiterait de s'adresser à lui et son livre de compte ferait **référence**.

Si plusieurs tables de commerçants coexistent, les différents banquiers devront s'organiser entre eux et les transactions inter-tables deviendront rapidement complexes. Incontournable, le banquier sera également tenté d'imposer ses propres règles.



Dans le modèle **Bitcoin**, les choses sont sensiblement différentes.

Le livre de compte n'est plus unique et il en existe de **multiples exemplaires**. Chacun peut en posséder une copie. Toute écriture effectuée au sein de l'un de livre apparaîtra dans toutes les instances du livre. Si une majorité est d'accord, l'écriture sera validée et celle-ci deviendra **infalsifiable**, impossible à retirer. Le processus de validation est donc à la fois **transparent** et basé sur le **consensus**. Il ne repose plus sur la confiance mais sur la **preuve**.

Le grand apport de Bitcoin est de nous offrir ce « livre magique » avec la technologie **blockchain**.

Dans ce modèle, notre ami banquier siègera toujours autour de la table, mais son rôle ne sera plus de réguler les transactions...

### 3/ Utiliser Bitcoin - Concepts fondamentaux

Regardons plus en détail le fonctionnement de Bitcoin, à travers un exemple.

Imaginons **Alice** et **Bob**. Tous les deux possèdent un portefeuille en bitcoins.

Alice se rend dans le café de Bob, consomme un café et va procéder au règlement de celui-ci.

Le processus de paiement est alors le suivant :

- Bob présente la note et une demande de paiement,
- Alice prépare une transaction et signe celle-ci,
- La transaction signée est diffusée sur le réseau Bitcoin,
- Un « mineur » la récupère et l'intègre à la *blockchain* – le livre de compte.
- Ce processus est pratiquement transparent et chacun peut vérifier l'état de la transaction.

Dès lors que la transaction est intégrée à la *blockchain*, le paiement est effectif et définitif.

#### 3.1 Alice possède des bitcoins, mais où sont-ils ?

Les bitcoins d'Alice sont gérés via un **porte-monnaie** électronique et n'existent que sous forme comptable, comme des euros sur un compte bancaire.

Les bitcoins sont **enregistrés dans la blockchain** et sont rattachés à des **adresses**. Chacune de ces entrées est protégée par un « **verrou** ». Les bitcoins ne peuvent être utilisés dans une transaction que sur présentation de la « **clef** » de ce verrou. Une transaction qui voudrait utiliser des bitcoins non déverrouillés serait purement et simplement rejetée par le réseau.

Le porte-monnaie d'Alice ne contient donc pas de bitcoins, mais les clefs permettant de les utiliser.

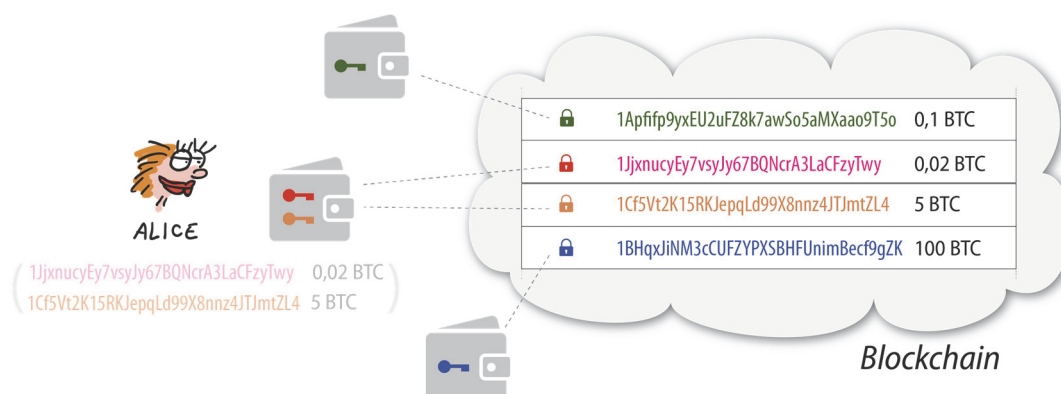


Figure 2 - Blockchain et porte-monnaie

Dans notre exemple, Alice possède 0,02 BTC et 5 BTC sur deux adresses différentes.

Le rattachement des bitcoins aux adresses est **visible par tous**, car le contenu de la *blockchain* est accessible à tous, mais seule Alice, qui possède la **clef des verrous**, pourra utiliser ces bitcoins.

Adresses, verrous et clefs sont gérées par les applications de manière quasiment transparente. Seules les adresses sont visibles lorsque l'on effectue une transaction.

Le client gérant le porte-monnaie d'Alice ne lui indiquera que son solde global : 5,02 BTC.

Le porte-monnaie, contenant les clefs d'accès aux bitcoins, **doit être sauvegardé avec soin**. Perdre son porte-monnaie reviendrait à perdre ses bitcoins. Nul ne pourrait les récupérer.

### 3.2 Bob présente sa facture

Bob va présenter à Alice une demande de paiement pour les 5 mBTC de son café. Un café valant 0,005 bitcoin, il est plus pratique de compter en *millième de bitcoin*.

Pour cela, il va générer une **adresse** et une **clef de déverrouillage**, qu'il conservera précieusement dans son porte-monnaie.

Il proposera ensuite à Alice d'effectuer le règlement vers cette adresse.



Figure 3 - Demande de règlement via un QRCode

Ergonomiquement, tout cela est géré par l'application qui gère le porte-monnaie de Bob. Cette dernière présentera à Alice un *QRCode* ou un lien, contenant l'adresse et le montant du règlement à effectuer.

Le nombre d'adresses Bitcoin qu'il est possible de créer est de l'ordre de  $10^{47}$ ... Pour des questions de sécurité et de confidentialité, une adresse n'a pas vocation à être utilisée plusieurs fois. L'adresse de Bob que va utiliser Alice ne servira donc que pour ce règlement.


### 3.3 Alice prépare sa transaction

Par le biais d'un *QR Code*, Alice a pu récupérer toute les informations nécessaires à l'élaboration de sa transaction, à savoir l'**adresse** vers laquelle envoyer le règlement et le **montant** à envoyer.

Une transaction Bitcoin est composée de deux parties :

- Des « **entrées** », qui font référence à des bitcoins enregistrés dans la blockchain et dont on possède les clefs de déverrouillage,
- Des « **sorties** », composées d'adresses protégées par des verrous, vers lesquelles seront envoyés les bitcoins spécifiés en « entrée »

Le montant cumulé des entrées doit évidemment être supérieur ou égal aux sorties.

Une entrée utilisée doit être intégralement dépensée, comme lorsque l'on utilise un billet ou une pièce. Il est donc nécessaire de rajouter une sortie pour **récupérer la monnaie**. 

La différence, entre les entrées et les sorties sont considérés comme des **frais de transaction**, qui serviront à rétribuer ceux qui procède à l'enregistrement de la transaction.

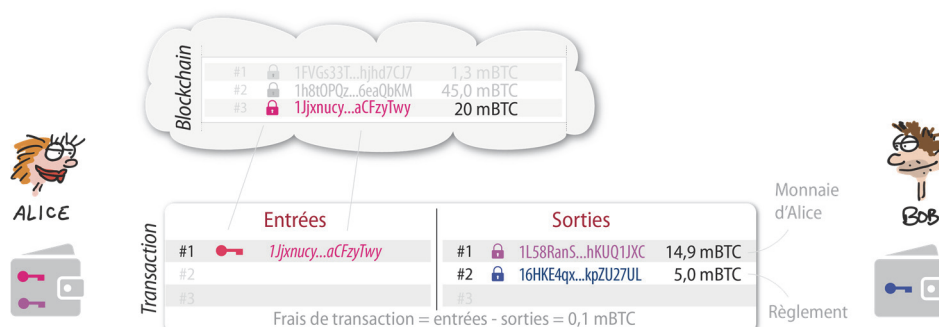


Figure 4 - Principe d'une transaction Bitcoin

Dans notre exemple, Alice utilisera son entrée de 20 mBTC ayant l'adresse 1jxnucy...aCFzyTwy

En sortie, elle affecte 5 mBTC à l'adresse fournie par Bob, pour le règlement de son café, et 14,9 mBTC à une adresse qu'elle s'est générée et dont elle possède la clef, afin de récupérer sa monnaie.

La différence de 0,1 mBTC, entre les entrées et les sorties, sera récupérée par ceux qui traiteront la transaction.

Une transaction peut comporter un très grand nombre d'entrées et de sorties.

Si aucune sortie n'est ajoutée pour récupérer sa monnaie, celle-ci sera considérée comme ...des frais de transaction !

Heureusement, dans le vrai monde, toute cette **complexité est masquée par les applications** :

Après lecture du *QRCode* par l'application de son smartphone, la seule chose que verra Alice sera une demande de validation pour le paiement de 0,5 mBTC vers l'adresse de Bob :



Figure 5 - Exemple de règlement via une application (Mycelium)

L'opération de paiement, ci-dessus, s'effectue en « 3 clics »

1. Depuis l'écran d'accueil, Alice choisit **d'envoyer** des bitcoins,
2. Le **montant** de la transaction est ensuite récupéré via un *QRCode*,
3. La transaction est présentée pour **validation**

### 3.4 Diffusion de la transaction

Une fois la transaction validée par Alice, celle-ci sera envoyée au **réseau Bitcoin** pour être prise en compte.

Le réseau Bitcoin est composé de plusieurs milliers de nœuds [6], formant un réseau de type *peer to peer*, dans lequel chaque nœud communique avec ses voisins :

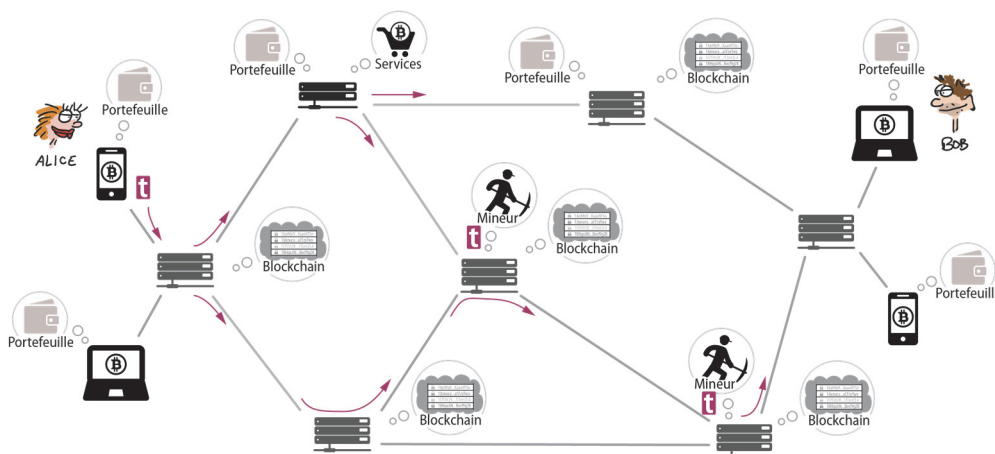


Figure 6 - Réseau P2P Bitcoin

Les nœuds Bitcoin peuvent remplir différentes fonctions, telle que l'hébergement d'une instance de la **blockchain**, la gestion de **portefeuilles** ou encore l'intégration des transactions au sein de la **blockchain (minage)**.

Une fois prise en charge par l'un des nœuds, auquel Alice est connectée, la transaction sera immédiatement propagée à l'ensemble des nœuds du réseau. Du fait de cette



architecture **pair à pair (P2P)**, le délai de propagation est extrêmement rapide [7]. La diffusion d'une transaction à 90% des nœuds s'effectue la plupart du temps en moins de 6 secondes [8].

Chacun peut librement ajouter un nœud au réseau Bitcoin. Nulle démarche n'est à effectuer auprès d'un quelconque organisme. Dès lors que ce nouveau nœud respecte les règles du réseau, il pourra être intégré avec le même niveau de privilège que n'importe quel autre nœud.

Une implémentation de référence, appelée *Bitcoin Core*, est disponible [9] sous licence MIT [10].

### 3.5 Intégration de la transaction au sein de la blockchain

La transaction d'Alice ne sera **définitive** qu'une fois **intégrée à la blockchain**.

#### 3.5.1 À propos de la blockchain...

La **blockchain** peut être vue comme un **grand livre de compte** qui contient **toute les transactions** depuis le début de Bitcoin, permettant ainsi de suivre le devenir de chaque bitcoin.

**Toute entrée d'une transaction est nécessairement la sortie d'une autre transaction.**

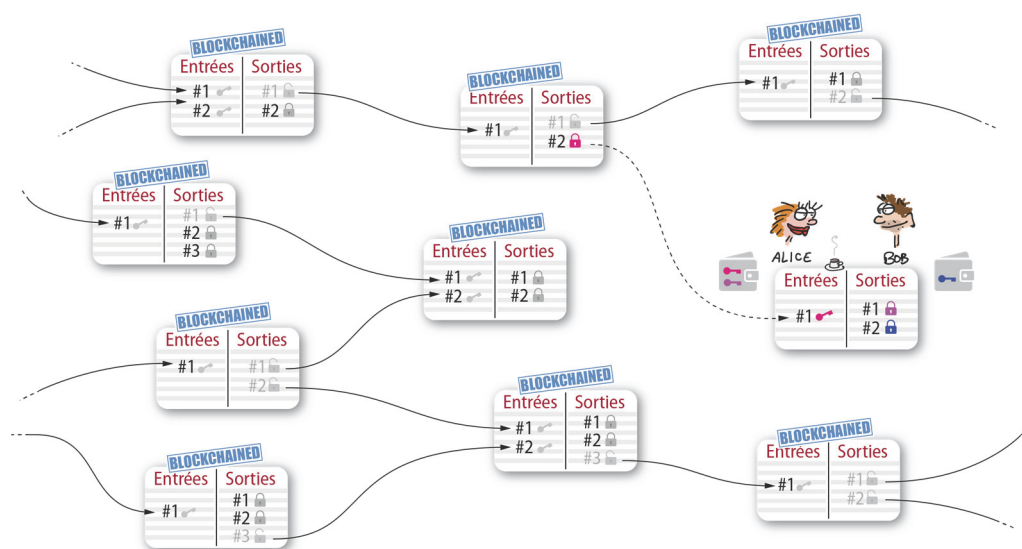


Figure 7- Enchaînement des transactions au sein de la blockchain

Une transaction ne peut être **acceptée** que si ses **entrées** contiennent les **clefs de déverrouillage** des sorties qu'elle utilise.

Lorsqu'une sortie est utilisée, tous les bitcoins de cette sorties sont utilisés.

La blockchain étant publique, il est relativement aisé de suivre le parcours des bitcoins [11] et l'anonymat des transactions bitcoins est un problème complexe sur lequel nous reviendrons.

Bitcoin possède un jargon particulier, qu'il est bon de connaître :

- Au sein d'une transaction, les entrées sont appelées « **inputs** » et les sorties « **outputs** »,
- Les sorties non dépensées sont appelées **UTXO** pour *Unspent Transaction Output*

#### 3.5.2 Création des blocs (et des bitcoins)

Comme le nom l'indique, la blockchain est constituée de blocs consécutifs, constituant une chaîne.

Une fois prêtes à être intégrées, les transactions sont envoyées et diffusées sur l'ensemble du réseau Bitcoin. Certains nœuds spécialisés – appelés « **mineurs** » – vont regrouper ces transactions et **tenter de fabriquer un nouveau bloc**, susceptible d'être intégré à la blockchain.



La construction d'un nouveau bloc est une compétition ouverte à tous, qui demande un énorme travail **cryptographique**. Le premier qui réussit à construire ce nouveau bloc gagne la compétition, récupère les **frais de transaction**, et touche une **récompense en bitcoins**.

La difficulté cryptographique de cette compétition est régulièrement adaptée de manière à ce que la durée de création d'un bloc soit maintenue à 10 minutes environ. La récompense que touche le mineur, initialement de 50 BTC, est diminuée de moitié tous les 210.000 blocks (4 ans).

Les bitcoins gagnés par les mineurs sont créés *ex nihilo*, mais de manière déterministe et finie. Le dernier bitcoin sera ainsi « miné » le 8 octobre 2140 et le nombre total de bitcoin sera alors de 21 millions. **Il n'existe pas d'autres mécanismes de génération des bitcoins.**

La courbe de génération des bitcoins est proche des courbes de production minière.

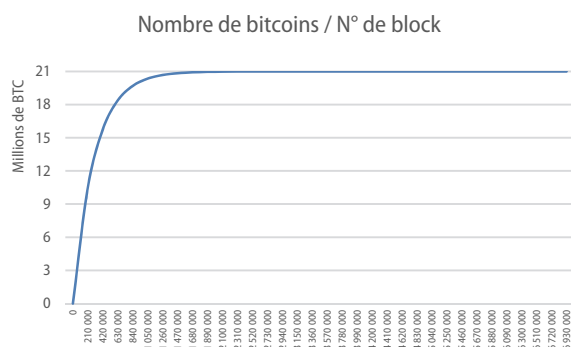


Figure 9 – Émission des bitcoins

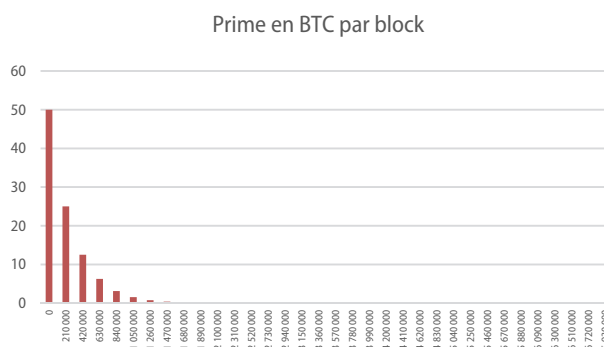


Figure 8 - Évolution de la récompense

Lorsque un nœud reçoit un nouveau block, il va systématiquement **contrôler** celui-ci, et **vérifier** que toutes les transactions contenues sont bien valides, notamment que les entrées correspondent bien à des **sorties non dépensées** et **qu'aucune double dépense n'est présente**.

Un block qui ne serait pas conforme serait purement et simplement ignoré.

### 3.5.3 Évolution de la blockchain

Les blocs sont conçus pour s'enchaîner les uns aux autres, à la manière des pièces d'un puzzle, où chaque pièce ne peut s'enchaîner qu'avec la pièce précédente.



Figure 10 - Enchaînement des blocs

Vouloir remplacer (fraudemment) l'un des blocs nécessiterait de reconstruire tous les blocs suivants, ce qui serait très difficile, à moins que le fraudeur ne dispose d'une puissance de calcul supérieure à tous les autres nœuds réunis.

Il est possible que plusieurs blocs apparaissent simultanément, parce que deux mineurs sont arrivés ex-aequo ... ou qu'un mineur malhonnête tente de faire *diverger* la chaîne.

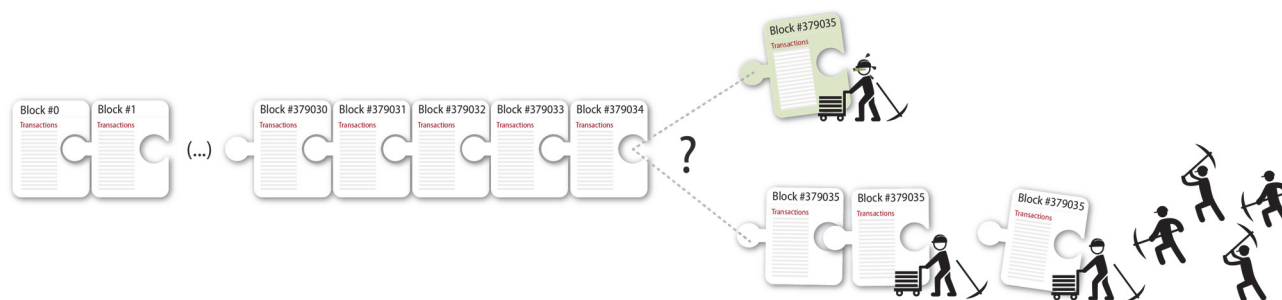


Figure 11 - Divergence de la blockchain

En cas de divergence, la règle consiste à considérer comme légitime la branche la plus longue, tout en conservant les différentes branches, dans le cas où l'une d'entre elles deviendraient plus longues.

Dans la mesure où les nœuds honnêtes possèdent une puissance de calcul supérieure aux nœuds frauduleux, la chaîne honnête deviendra rapidement plus longue.

### 3.6 Transaction valide vs définitive

Les bitcoins n'existent qu'au travers des transactions **enregistrées** dans la blockchain. Une transaction validée par chaque nœud lors de sa diffusion sur le réseau ne deviendra effective que lorsqu'elle sera **définitivement intégrée à la blockchain**.

#### 3.6.1 Appartenance à la blockchain

On pourrait penser que dès l'instant où une transaction est intégrée à la blockchain, celle-ci peut être considérée comme définitive. Cela est *presque* vrai.

Nous avons vu que la construction de la blockchain était un processus collaboratif, basé sur le consensus, mais sujet à d'éventuelles divergences. Il est donc possible qu'une transaction, frauduleuse ou non, soit intégrée dans un bloc divergent, temporairement intégré par les nœuds. Le temps que s'établisse un consensus de rejet, cette transaction apparaît bien dans la blockchain.

Compte-tenu de la difficulté qu'aurait un mineur malhonnête à constituer et maintenir une branche importante, on considère qu'un bloc **recouvert par 6 autres blocs** peut être considéré comme étant **définitivement intégré**.

Dans la pratique, lorsque les transactions portent sur de petites sommes, on se contentera souvent d'une profondeur beaucoup plus faible.

Dans le cas du café d'Alice, Bob considérera même que le règlement est acquis dès lors que la transaction est validée et prise en charge par les nœuds. On parle alors d'une profondeur de 0.

Statistiquement et en l'absence de divergence, il faut attendre environ une heure, pour qu'un bloc atteigne une « profondeur » de 6 blocs.

#### 3.6.2 Vérification Simplifiée de Paiement (SPV)

Pouvoir vérifier l'état d'une sortie, le fait qu'une transaction appartienne bien à un bloc et un bloc à la blockchain est donc **indispensable** pour un client Bitcoin.

Les nœuds qui maintiennent une instance complète de la blockchain peuvent effectuer ces vérifications aisément. Chaque nouveau bloc qui arrive est intégralement vérifié, chaque transaction est contrôlée et une base des sorties non dépensées est maintenue à jour.

Ces nœud « lourds » disposent d'une vue complète et peuvent ainsi offrir le meilleur niveau de sécurité possible.

Malheureusement, maintenir une instance complète de la blockchain est un processus long et très gourmand en ressources [12] et de nombreux nœuds ne peuvent disposer de ressources suffisantes.

C'est le cas, par exemple, des **smartphones et tablettes**. Pour ces nœuds « légers », un protocole particulier existe, appelé **SPV** pour ***Simple Verification Payment***.

Un tel nœud ne disposera que d'une vue limitée de la blockchain et ne pourra vérifier que deux choses :

- l'enchaînement des blocs de la blockchain,
- la présence de la transaction au sein d'un bloc donné.

Si cela permet de vérifier qu'une transaction est bien intégrée à la blockchain, cela ne donne pas d'informations concernant l'état des sorties de cette transaction.

## 4/ docproof.org, un service de notariat électronique

Comme nous l'avons vu précédemment, la preuve de possession, d'existence ou d'antériorité s'est toujours appuyée sur des **tiers de confiance**, tandis que la technologie blockchain s'appuie sur un principe d'archivage de « **preuve** », basée sur le **consensus**.

En s'appuyant sur cette capacité à enregistrer de manière transparente et (quasi) « infalsifiable », il a été possible de développer une solution de notariat électronique.

**Docproof.org** est un développement original, destiné à proposer à une large communauté un service de **notariat électronique**, basé sur la technologie blockchain.

### 4.1 Principes et objectifs

**docproof.org** permet :

- **D'enregistrer la preuve d'existence d'un document**, données binaires, cahier de laboratoire, logiciel, photo, document sonore, etc. en toute indépendance d'un quelconque tiers de confiance,
- L'enregistrement est effectué en toute **confidentialité**, car votre document reste en votre seule possession,
- La vérification de votre « preuve » s'effectue en toute **indépendance** de docproof.org.

**docproof.org** reprend les principes du site **proofofexistence.com**, développé par Manuel Araoz [13].

### 4.2 Mise en œuvre

Le site est accessible à l'URL suivante : <http://docproof.org>

Le processus est extrêmement simple et se déroule en 3 étapes :

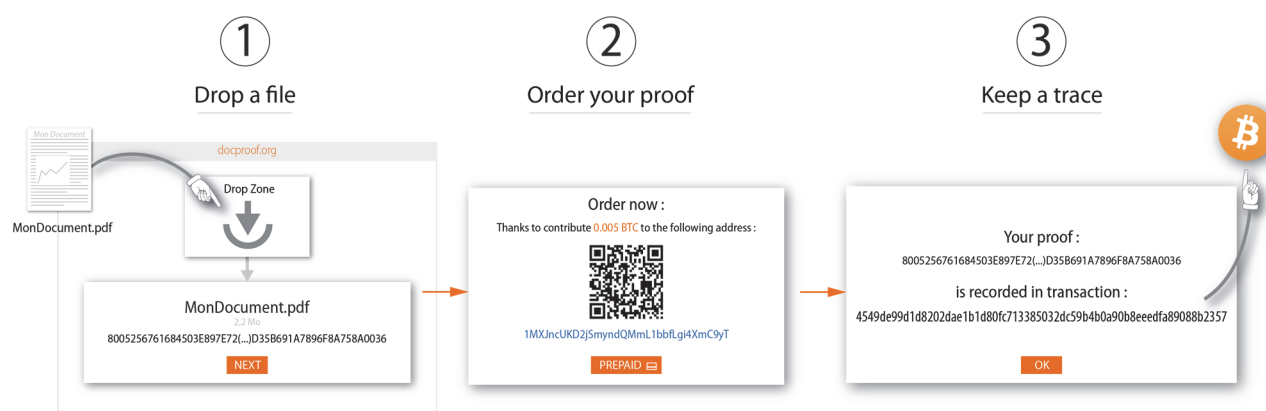


Figure 12 - docproof.org

#### (1) Dépôt du document :

- Le document est déposé via un simple *drag-and-drop*.
- Une fois déposé, l'empreinte du document est calculée localement – aucun fichier n'est *uploadé*

#### (2) Enregistrement de la preuve

- Une demande de règlement est affichée, destinée à financer la transaction d'enregistrement.
- Le règlement peut être effectué en bitcoins ou via un compte prépayé.

#### (3) Archivage de la trace

- Dès le règlement effectué, les paramètres d'enregistrement vous sont donnés. Le numéro de la transaction comportant la preuve est à conserver.
- Il est immédiatement possible de suivre l'intégration de votre preuve au sein de la blockchain par le biais du numéro de transaction.

## 5/ Limites et perspectives

Imaginer quel peut être l'avenir de Bitcoin en particulier, et des crypto-monnaies en général, est impossible.

La richesse fonctionnelle apportée par ces projets est objectivement une avancée majeure de nature à induire des mutations profondes dans des domaines jusqu'ici protégés.

Avec une capitalisation monétaire supérieure à 3 milliards d'euros et une stabilité raisonnable sur les 12 derniers mois, Bitcoin est objectivement devenu un acteur monétaire de fait. Petit, mais réel.

La très récente décision de la cours de justice européenne, qui reconnaît le statut de devise à Bitcoin, ne devrait qu'encourager le développement des crypto-monnaies.

Reste qu'un certains nombres de limitations existent.

### 5.1 Limites

Les limites ou problématiques présentées ici ne le sont qu'à titre d'illustration et ne sauraient nullement être exhaustives. Elles n'ont pour intérêt que de présenter quelques exemples de difficultés et enjeux, présents et à venir, liés à l'évolution de Bitcoin.

#### 5.1.1 Anonymat

L'anonymat de Bitcoin est souvent mis en avant, à tort.

Nous avons vu que l'ensemble des transactions étaient enregistrées et qu'elles constituaient un énorme graphe. Il est donc tout à fait possible de suivre « à la trace » les bitcoins d'une transaction.

Cette transparence peut être un point parfaitement positif, en offrant à chacun la possibilité de vérifier les comptes de son association ou ONG favorite.

Elle peut également être un problème sérieux concernant nos vies privées. Si nos banques savent aujourd'hui tout de nos dépenses et si l'utilisation des monnaies fiduciaires se restreint progressivement, peu d'acteurs ont cependant accès à ces informations.

Dans le cas de Bitcoin, l'accès à ces informations est totalement ouvert et le nombre d'acteurs à même d'utiliser ces informations n'est plus contrôlable.

Une étude récente montre qu'une analyse passive de graphes de transactions est déjà tout à fait possible, et qu'une analyse active, via des points concertés injectant des bitcoins marqués pourrait être extrêmement efficace [14].

Comme trop souvent, ces limitations exposent essentiellement les gens honnêtes... les personnes souhaitant rester discrètes sauront rapidement mettre en œuvre des moyens susceptibles de les protéger :

- Multiplication des adresses et usage unique de celles-ci,
- Usage de portefeuilles multiples,
- Anonymisation des connexions via des outils tels que *Tor*, afin de limiter les risques d'appariement adresses ip/adresses bitcoin,
- Utilisation de site d'anonymisation, tel que *bitcoinfog.com* [15]...

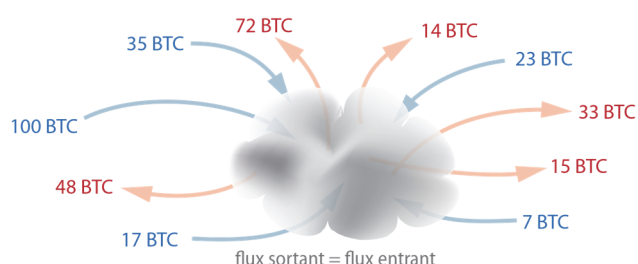


Figure 13 - Principe du "brouillard" d'anonymisation

Le principe d'un « brouillard d'anonymisation » consiste à déposer son argent au sein d'un « nuage » et de ne récupérer que progressivement l'argent déposé. L'intérieur du nuage étant opaque, il sera très difficile de relier les entrées aux sorties. Si la méthode peut être efficace, il est toutefois nécessaire de faire confiance au nuage...

Certaines crypto-monnaies, telle que *Darkcoin* sont conçues de manière à améliorer l'anonymat.

### 5.1.2 Minage

L'organisation et la « régulation » du minage est également l'une des grandes problématique des monnaies virtuelle. En nécessitant des moyens de plus en plus importants pour un gain qui se réduit inexorablement, la situation des mineurs s'est progressivement dégradée.

La source de financement des mineurs provient quasiment exclusivement des récompenses. La part des frais de transaction ne représente aujourd'hui que moins de 1% des revenus.

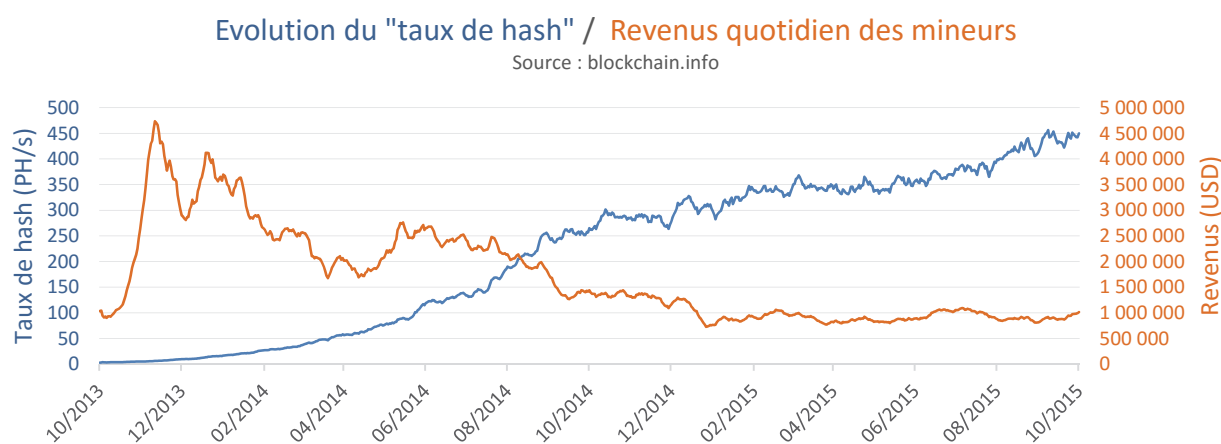


Figure 14- Évolution du taux de hash et du revenu quotidien des mineurs

Au fil du temps, les mineurs se sont naturellement regroupés au sein de coopératives de plus en plus importantes et les 10 plus gros « pool » de mineurs ont minés plus de 90 % des blocks sur les 10 derniers mois.

### Répartition des blocks minés par pool de mineur - janvier-octobre 2015

source : <https://bitcoinchain.com/pools>

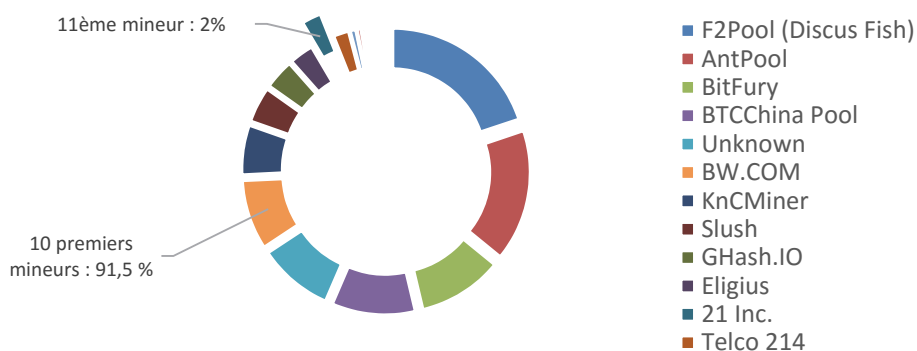


Figure 15 - Répartition des blocks minés par coopératives

Les coopératives actuelles sont ouvertes par nature et rien ne pourrait empêcher un « pool » mal intentionné de pénaliser ses concurrents en envoyant des mineurs malhonnêtes, qui ne participeraient que de manière apparente au minage. Les bénéfices étant partagés entre les mineurs d'une même coopérative, cela baisserait *de facto* le gain de l'ensemble des mineurs de la coopérative honnête, pénalisant celle-ci.

Une étude récente s'est intéressée à ce problème [16]. Un modèle basé sur le « dilemme du prisonnier » montre que le pacte de non-agression qui prévaut actuellement n'est qu'un équilibre précaire et que si l'une des coopératives s'en prenait à une autre, cela conduirait à une déstabilisation complète du système actuel, pénalisant l'ensemble des coopératives.

De ce fait, une évolution du modèle actuel pourrait être la constitution de coopératives privées de moindre taille, basées sur la confiance.

Dans tous les cas, la concentration croissante des coopératives de mineurs est l'un des grands problèmes que devra résoudre l'écosystème Bitcoin.

### 5.1.3 Une utilisation inégale

Les facteurs conduisant à l'utilisation (ou non) de Bitcoin sont très variables et le développement de Bitcoin est géographiquement très inégal.

Une étude récente [17], publiée par la plateforme d'échange suisse ECUREX, apporte un certain nombre d'éléments intéressants, illustrant notamment l'engouement chinois :

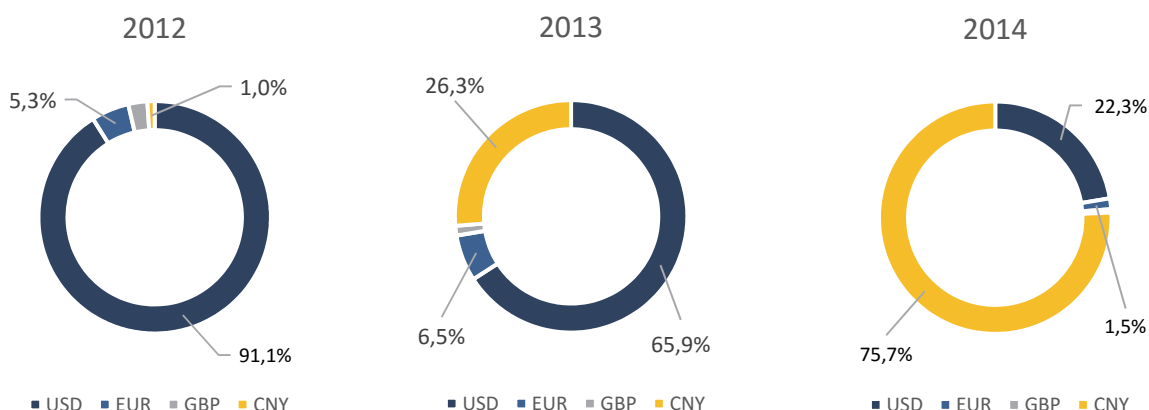


Figure 16 - Devises utilisées dans les échanges de BTC

En 2012, 91% des achats de bitcoins s'effectuaient en dollars, deux ans plus tard, 75% des achats sont effectués en Yuan.

Un facteur qui contribue de manière importante à l'attractivité du bitcoin est le degré de « liberté financière ». Selon une étude du département de finance de l'université de Caroline du Sud [18], dans les pays où la liberté économique est moindre, comme cela est actuellement le cas en Chine ou comme ce fut le cas durant la crise Grecque, le cours du Bitcoin est supérieur, car il apparaît comme une alternative aux monnaies locales.

Cet engouement est également visible au niveau des coopératives de mineurs, dont les plus importantes sont aujourd'hui chinoises.

Si les utilisateurs actuels de Bitcoin sont majoritairement chinois, la maîtrise et le développement de la technologie Bitcoin se poursuit, quant à elle, essentiellement outre atlantique.

En n'étant ni demandeurs d'une devise refuge, ni acteurs dans l'évolution technologique de Bitcoin, la présence d'acteurs européens, au sein de l'écosystème Bitcoin, reste assez limitée.



## 5.2 Perspectives

Bitcoin peut être vu comme une alternative « libre » aux systèmes monétaires traditionnels, au même titre que de nombreuses autres monnaies locales (ou complémentaires). Ces monnaies ayant pour caractéristiques d'être utilisées dans des environnements restreints.

Certaines de ces monnaies complémentaires ont acquis une importance de premier plan dans certains secteurs. On peut citer le WIR en suisse, qui est utilisé par près de 60.000 PME et qui représente 1,6 milliards de francs Suisse.

Bitcoin est un peu à la croisée des chemins, pouvant être vu à la fois comme la « monnaie locale du crime » et un « outsider technologique ».

### 5.2.1 Un avenir au sud ?

Le développement de Bitcoin est en concurrence avec un grand nombre d'acteurs issus des GAFA (Google, Amazon, Facebook, Apple) ou de « l'ancien monde » (Visa, Western Union, ...).

Il est peu probable que Bitcoin puisse s'imposer face à une concurrence dotée de moyens aussi importants et en situation d'oligopole.

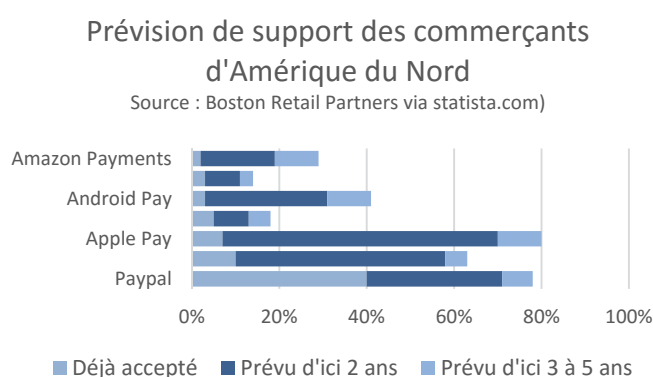


Figure 18 - Prévision de déploiement des moyens de paiement électroniques en Amérique du Nord

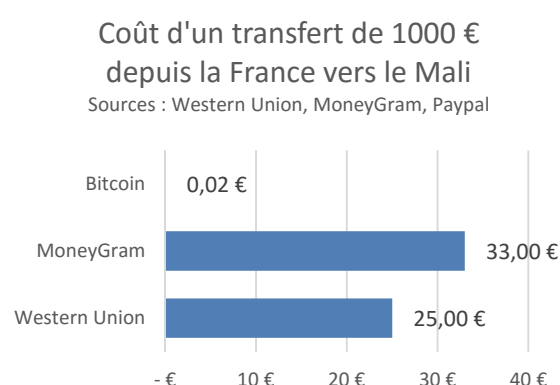


Figure 17 - coût d'un transfert de 1000€ depuis la France vers le Mali

Le coût d'un transfert de 1000€, depuis la France vers le Mali, est supérieur à 25 €, contre environ 2 centimes pour une transaction Bitcoin, soit un coût plus de 1000 fois inférieur...

Annuellement, plus de 500 millions d'Euros sont envoyés par la diaspora malienne...

Utiliser Bitcoin ne nécessite aucun compte en banque. La seule infrastructure nécessaire étant un smartphone et un accès Internet.

Bitcoin pourrait ainsi se révéler être une solution très intéressante dans les pays du sud, en étant tout aussi efficace pour effectuer des micro-paiements que des transferts internationaux et extrêmement souple à déployer dans des pays où 80% de l'économie est informelle mais où tout le monde possède un téléphone...

Aujourd'hui, 2 milliards de personnes n'ont pas de compte bancaire dans le monde.

### 5.2.2 Un avenir financier ?

A l'opposé des pays du sud, où le nombre de personnes disposant d'un compte bancaire sont rares, les grandes banques témoignent un grand intérêt pour les technologies issues de Bitcoin.

22 banques se sont regroupées au sein d'un consortium porté par la startup américaine R3 CEV, autour d'un projet de blockchain commerciale, destinée à la gestion des transactions financières.

### 5.2.3 Au-delà de la monnaie ?

Le potentiel de l'architecture Bitcoin dépasse largement les échanges monétaires et nous avons vu, par exemple, que la blockchain pouvait être utilisée pour des solutions de notariat électronique.

Un terrain particulièrement prometteur est celui de la gestion des actifs et des contrats.

#### Gestion d'actifs (*colored bitcoins*)

Le principe des *colored bitcoins* est très simple. Imaginons un bien dont on souhaiterait partager la propriété entre des actionnaires.

Pour réaliser cela, une centaine de bitcoins colorés sont créés et distribués entre les actionnaires. Le principe étant qu'un bitcoin coloré reste coloré et qu'il ne peut être mélangé avec d'autres bitcoins.

Chaque actionnaire peut ensuite transférer ou revendre, sa part, via une simple transaction.

La propriété d'un actif peut ainsi être partagée et échangée en toute indépendance d'un quelconque organisme ou tiers de confiance.

Ce concept peut être utilisé aussi bien pour de la réservation de ressources que pour la gestion de propriété.

Pour réaliser cela, deux approches sont possibles :

- Ajouter des protocoles au-dessus de Bitcoin, On peut citer les projets *Mastercoin*, *Couterparty* et *Open Assets* [19] avec le portefeuille *Coinprism* [20].
- Utiliser des blockchains alternatives. On peut citer les projets *namecoins* (gestion de noms de domaine) et surtout *Etherum* [21]

Des centaines de crypto monnaies [22] sont apparues à la suite de Bitcoin. Si chacune possède des caractéristiques propres, très peu parviennent à émerger significativement [23].

#### Gestion de contrats (*Ethereum*)

La gestion de *smart contract* (contrats intelligents) est imaginée depuis longtemps. L'idée étant de pouvoir transférer des valeurs entre deux ou plusieurs acteurs, sur la base de conditions acceptées par l'ensemble des protagonistes.

La technologie blockchain est peut-être celle qui permettra d'implémenter ce concept et le projet *Ethereum* [21] est sans doute l'un des plus prometteurs.

Son architecture reprend le principe d'une blockchain, protégée par un système de preuve par le travail, mais l'objet des transactions n'est plus seulement de gérer de la monnaie, mais également des contrats.

Ces contrats – des « *smart contracts* » - peuvent être écrits dans un (presque) langage de Turing, *Solidity* [24], disposant notamment de boucles. Toute opération, compilation, intégration dans la blockchain et autres exécution, nécessitera du « carburant » : la monnaie interne d'*Ethereum*, l'*Ether*.

Pour en savoir davantage concernant ce projet, qui pourrait faire l'objet d'un article au moins aussi long que celui-ci, vous pouvez consulter les deux excellents articles de Stéphane Bortzmeyer [25] et [26] :-)

## Bibliographie

- [1] CFTC, «CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering,» <http://www.cftc.gov/PressRoom/PressReleases/pr7231-15>.
- [2] Cours de justice européenne, «Arrêt du 22 octobre 2015 - Opérations de change de la devise virtuelle 'bitcoin' contre des devises traditionnelles – Exonération,» 22 10 2015. [En ligne]. Available: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=606120>.
- [3] Achats directs, «Sites d'achat direct de bitcoins,» [En ligne]. Available: <https://belgacoin.com>, <https://www.kraken.com>, <https://paymium.com>, <https://www.coinbase.com/>.
- [4] Places d'échanges. [En ligne]. Available: <https://www.bitcoin.de>, <https://localbitcoins.com>.
- [5] Blockchain.info, «Graphiques Bitcoin / Divers graphiques sur bitcoin et statistiques monétaires,» [En ligne]. Available: <https://blockchain.info/fr/charts>.
- [6] Bitnodes, «Global Bitcoin Nodes Distribution,» [En ligne]. Available: <https://bitnodes.21.co/>.
- [7] R. W. Christian Decker, «Information Propagation in the Bitcoin Network,» chez *13-th IEEE International Conference on Peer-to-Peer Computing*.
- [8] Bitcoinstats, «Data propagation - Daily snapshots,» [En ligne]. Available: <http://bitcoinstats.com/network/propagation/>.
- [9] Bitcoin Core, [En ligne]. Available: <https://bitcoin.org/en/bitcoin-core/>.
- [10] Licence MIT, [En ligne]. Available: <https://bitcoin.org/en/bitcoin-core/>.
- [11] Blockchain.info, «Exemple de visualisation graphique de l'une des plus grosse transaction effectuée en 2013 (193.000 BTC, soit 147 M€),» [En ligne]. Available: <https://blockchain.info/fr/tree/43189250>.
- [12] Blockchain.info, «Statistiques / Taille de la blockchain,» [En ligne]. Available: <https://blockchain.info/fr/charts/blocks-size>.
- [13] M. Maraoz, «Proof Of Existence,» [En ligne]. Available: [proofofexistence.com](http://proofofexistence.com).
- [14] M. H. Fergal Reid, «An Analysis of Anonymity in the Bitcoin System,» 2012.
- [15] Bitcoin Fog, «Bitcoin Fog Clearnet Portal,» [En ligne]. Available: <http://bitcoinfog.com/>.
- [16] I. Eyal, «Bitcoin, the miners's dilemma,» chez *IEEE Symposium on Security and Privacy*, Oakland, 2015.
- [17] P. Tasca, «Digital Currencies: Principles, Trends, Opportunities, and Risks,» ECUREX, Zurich, 2015.
- [18] R. Viglione, «Does Governance Have a Role in Pricing? Cross-Country Evidence from Bitcoin Markets,» University of South Carolina - Department of Finance, 2015.
- [19] Open Assets, «Colored coins and the Open Assets protocol,» [En ligne]. Available: <https://github.com/OpenAssets/>.
- [20] Coinprism, «Colored Coin Wallet,» [En ligne]. Available: <https://www.coinprism.com/>.
- [21] Ethereum, «Projet Ethereum,» [En ligne]. Available: <https://www.ethereum.org/>.
- [22] mapofcoins.com, «Map of coins,» [En ligne]. Available: <http://mapofcoins.com/>.
- [23] coinmarketcap.com, «Crypto-Currency Market Capitalizations,» [En ligne]. Available: <http://coinmarketcap.com/>.
- [24] Ethereum, «The Solidity Programming Language,» [En ligne]. Available: <https://github.com/ethereum/wiki/wiki/The-Solidity-Programming-Language>.
- [25] S. Bortzmeyer, «Ethereum, la prochaine étape des systèmes transparents,» [En ligne]. Available: <http://www.bortzmeyer.org/ethereum.html>.
- [26] S. Bortzmeyer, «Un exemple de contrat Ethereum,» [En ligne]. Available: <http://www.bortzmeyer.org/contrat-ethereum.html>.