

Blockchain

Etat de l’art

|  |  |
| --- | --- |
| **Team n°** | 7 |
| **Rédacteurs** | Yoann BILIATO, Antonin BROQUET, Lucie MERCENNE, Michael PERRIN |
| **Date de création** | 25 septembre 2017 |
| **Statut** | En cours de rédaction |
| **Version** | 2.0 |

# 

**SOMMAIRE**

[**0 - ABSTRACT**](#_b1fwfc789utz) **2**

[**1 - INFORMATIONS GÉNÉRALES BLOCKCHAIN**](#_4kj75s8wgoc9) **2**

[1.1 - Historique des transactions](#_fgn4uxa3eit9) 2

[1.1.1 - Tiers de confiance, monnaie et propriété](#_2f6v6z31aik) 2

[1.1.2 - Virtualisation des transactions](#_60p303yfp3mw) 3

[1.1.3 - La confiance renforcée par la technologie](#_esyhsqxzd1so) 3

[1.2 - A l’origine, le bitcoin](#_3euao2du5a28) 3

[1.3 - Comment cela fonctionne](#_rg0zvbb8w2m0) 4

[1.3.1 - Notions de cryptographie](#_bbdazzboc7d) 4

[Hash : le hachage](#_3uf03wveo3vb) 4

[Qu’est-ce que le chiffrement ?](#_1hmdgrko3of6) 5

[Chiffrement symétrique/asymétrique](#_i9by7xapaj6) 5

[1.3.2 - La chaîne de blocs](#_m4bms3egtmmx) 6

[Timestamp](#_sxccxtjzqw89) 6

[Nonce](#_84zw29cuhzuu) 7

[Tx\_Root : Registre des transactions](#_pmfccudwtchk) 7

[1.3.3 - Transactions](#_96qpit3qh58f) 7

[1.3.4 - Réseau distribué](#_2ihiy0kliliq) 9

[1.3.5 - Le minage](#_4290bt8u3ym7) 10

[1.3.6 - Les consensus: POW / POS](#_qq6a5yky355d) 12

[1.3.7 - Tableau comparatif des algorithmes de hachage](#_iyk3ypyq1vls) 13

[1.4 - L'écosystème](#_whwoshs1f9i6) 15

[**2 - FOCUS ETHEREUM**](#_ufz7l9broktw) **16**

[2.1 - Présentation](#_gf5lcutdqhbs) 16

[2.2 - La machine virtuelle d’Ethereum](#_d9kdm2smypgs) 17

[2.3 - Les Comptes: notion majeure dans Ethereum](#_4t2ahigr6lyf) 17

[2.4 - Contrats et Transactions](#_gj132bdruul4) 18

[2.4.1 La transaction](#_b9twex5y5b4w) 18

[2.4.2 Le contrat](#_fzvj9kn4uctt) 18

[2.5 - Le minage dans Ethereum](#_o2ozyeuviuoa) 18

[2.5.1 - L’algorithme Dagger-Hashimoto](#_xijvf7hulhmn) 19

[2.5.2 - Les blocs “oncles”](#_ra2r7bkw8d6z) 19

[2.6 - Le modèle économique d’Ethereum](#_4y5v9hlxbc2z) 19

[2.6.1 - C’est quoi l’Ether?](#_gn2wry9l630y) 19

[2.6.2 - Le WEI](#_p80abtyacqqt) 19

[2.6.2 - Le GAS](#_6mp2woa129q6) 19

[**3 - USE CASES**](#_fnko3g1er4l9) **21**

[3.1 - Tableau récapitulatif](#_8ep28jwfxidg) 21

[**4 - Conclusion**](#_xd9o9taq3l5v) **23**

[**5 - Acronymes & Définitions & Sources**](#_7f6f8tjhhgcs) **24**

[**6 - Annexes**](#_jpw12x1j1wtv) **25**

[6.1 - Le Wallet](#_q8gbaiqa5kh) 25

[6.2 - Comment acheter des bitcoins?](#_4svceknqt0hk) 26

[6.3 - Focus sur le minage](#_goverlvxuni7) 27

[6.3 - Focus sur les mineurs](#_goverlvxuni7) 28

[6.4 - Focus sur les cas de hacking](#_b92imrz9r527) 29

[6.4 - REX: participation à une conférence midi minatec](#_owwotirs587j) 30

# PREAMBULE

Ce document présent a pour vocation d’éclaircir le fonctionnement d’une blockchain même pour les plus néophytes.

**Note:** Les références bibliographiques sont notées entre crochets *[X]*. Si une information est directement tirée d’une référence, le texte est formaté en *italique*.

# 

# 

# 1 - INFORMATIONS GÉNÉRALES BLOCKCHAIN

La blockchain n’est pas une technologie révolutionnaire, c’est une association astucieuse de plusieurs technologies existantes. Elle permet de simplifier grandement le déploiement de solutions qui semblaient trop complexes avec les technologies existantes. Il y a toujours un aspect économique derrière la mise en place d’une blockchain qui est disruptive avec les modèles existants. Nous ferons souvent référence au Bitcoin qui est à l'origine du développement de la technologie blockchain.

## 1.1 - Historique des transactions

### 1.1.1 - Tiers de confiance, monnaie et propriété

A la sortie de la Renaissance, **la notion de propriété** commence à émerger avec les écrits de Rousseau et de Locke. Les premiers registres nationaux sont créés à la faveur du renforcement et de la consolidation des états européens.

En France, le cadastre napoléonien répond au besoin d’un document de référence utilisable pour les transactions des particuliers. La stature de l’Empire français et son administration rendent le document “digne de confiance”.

**Cette confiance absolue** du particulier envers les administrations de sa nation est **à la base de la monnaie fiduciaire** car contrairement à une pièce de monnaie en métal, le billet possède une valeur intrinsèquement nulle. Des organismes de confiance sont nécessaire pour garantir la valeur de la monnaie fiduciaire : Les banques centrales.

**Un tiers de confiance est alors la condition première du développement de la monnaie et de la propriété.**

### 1.1.2 - Virtualisation des transactions

Suivant l’évolution de l’économie mondiale, les modalités des transactions se complexifient. Depuis les accords GATT en 1947, le commerce international se développe et nécessite **de sécuriser et garantir les transactions transfrontalières**. De nouveaux tiers de confiance internationaux voient le jour comme le système interbancaire **SWIFT** à la fin des années 70 ou l’**OMC** à la fin des années 90.

Ces organismes apporte les conditions d’un échange sécurisé, sans risque de pertes et fluide. **La transaction doit être la plus rapide possible et la moins coûteuse**.

### 1.1.3 - La confiance renforcée par la technologie

En 1976, le concept de la cryptographie présentée dans le protocole Diffie-Hellman, du nom des chercheurs américains, permet à deux agents d’échanger des informations cryptée sans avoir besoin de mot de passe. **Le concept de double clé publique et privée** est à la base de la technologie blockchain.

De nos jours, l’augmentation de la puissance de calcul informatique associé à la disponibilité d’unités de calcul décentralisées permettent l’utilisation d’une cryptographie virtuellement incassable et à la portée de tous.

En parallèle, l**es architectures distribuées sont des références en termes de stabilité et de sécurité**. Le web créé en 1990 au **CERN** en est le parfait exemple : aucune attaque informatique majeure n’a mis à mal son architecture globale.

**Ces deux technologies avancées ont permis,grâce à leur haut taux de confiance, la formation de la couche technologique à la base du bitcoin et des crypto-monnaies : la blockchain.**

## 1.2 - A l’origine, le bitcoin

C’est en étudiant le bitcoin que nous allons comprendre comment fonctionne la blockchain. En effet derrière cette cryptomonnaie précurseuse se cache la technologie qui nous intéresse.

Le bitcoin a été inventé par une personne (ou groupe de personne) anonyme, appelée **Satoshi Nakamoto en 2008**. On ne sait toujours pas qui est cette personne. Certains soupçonnent que derrière ce pseudo, se cache une réelle organisation qui a lancé le concept du Bitcoin.

Il publie un papier blanc [2] sur une méthode capable selon lui de résoudre un célèbre problème de cryptographie : *le problème du double paiement.* Ce problème empêchait deux agents de s'échanger des actifs **sans le concours d’un tiers de confiance*.***

La solution au problème réside dans l’utilisation d’une architecture décentralisée support du **bitcoin** : la *blockchain*. La découverte de cette solution ouvre de nouveaux horizons : **elle autorise ce qui n’était pas possible auparavant**. Une nouvelle *désintermédiation* est alors créée: deux personnes peuvent effectuer des transactions monétaires sans l’autorisation et la sécurisation d’un organisme central.

La confiance créée par la blockchain est un outil permettant de se passer du tiers de confiance, l’ensemble des actifs pouvant être échangés (financiers, propriétaires, transactions nécessitant un registre,..) peuvent se faire sur la blockchain.

Cette infrastructure a pour effet de **réduire les coûts et de fluidifier les échanges.**

Les transactions statiques ne sont pas les seuls éléments possibles dans la blockchain: les contrats passés entre personne peuvent inclure des variables, comme la performance ou la condition d’exécution. Dès lors, **le contrat devient intelligent** et capable d’opérer sans être régi par un organisme de de référence.

**L’émergence des monnaies utilisant la blockchain, l’absence de contrôle des marchés financiers et l’anonymat des utilisateurs et des transactions deviennent des sujets importants débattus au sein des institutions internationales.**

Pour preuve le bitcoin a été radié de Chine, mais approuvé comme monnaie au Japon et en Corée du Sud. L’Europe, quant à elle, est encore frileuse sur le sujet. Elle a refusé la création d’une crypto monnaie nationale de l’Europe envers l’Estonie (pays précurseur des nouvelles technologies).

Le cours du bitcoin est déterminé sous l’offre et la demande.

## 1.3 - Comment cela fonctionne

Le fonctionnement du bitcoin en quelques phrases :

Pour s’échanger des bitcoins, on réalise une transaction de type paye sur un réseau distribuépeer 2 peer. Ces transactions, partant d’un wallet (portefeuille virtuel) vers un autre wallet, sont enregistrées dans des registres distribués qui sont visibles par tous. Elles sont réalisées directement entre bénéficiaires, sans tiers de confiance. Ces registres sont représentés par des blocs. Il y a des mineurs sur le réseau qui grâce à de la puissance de calcul et aux concept PoW (Proof of Work) et PoS (Proof of Stake) permettent de créer des nouveaux blocs.

Pas si simple de comprendre ce processus complexe… nous avons besoin de développer toutes ces notions afin de saisir le fonctionnement.

### 1.3.1 - Notions de cryptographie

### **Hash : le hachage**

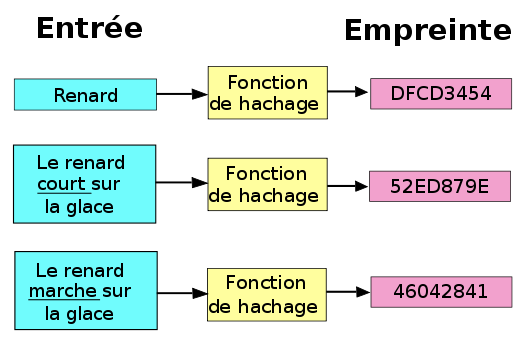
La fonction de hachage est une fonction qui va prendre en entrée un fichier de données et qui va en produire une empreinte unique de taille fixe dépendant de l’algorithme utilisé. L’empreinte, appelée *hash*, ne permet pas de retrouver les données d’origine, ce n’est donc pas un chiffrement. Elle permet cependant d'identifier des données : en effet, la moindre modification des données se répercute sur le hash qui devient totalement différent du précédent.

Les propriétés du hachage sont la rapidité, la résistance à la collision (pas de risque de doublons) et sa non réversibilité.

Le hachage est utilisé dans les cas suivants :

* Intégrité de l’envoi : vérification que le fichier d’origine est non corrompu
* Optimisation des transferts : création d’une signature pour des fichiers redondants afin de ne pas avoir à les télécharger à nouveau (exemple dropbox ou docker)
* Signature électronique : utilisation dans l’usage des certificats ssl
* Base de réputation : recherche de virus ou détection d’urls malicieuses

La figure 1 montre le principe d'empreinte du hachage:



*Figure 1: La fonction de hachage*

*(source:* [*http://www.ibibliotech.fr/4803-fonction-hachage*](http://www.ibibliotech.fr/4803-fonction-hachage)*)*

Dans le cadre des blockchains, le hash est utilisé pour garantir l’intégrité de la chaîne de blocs, et empêcher un utilisateur mal intentionné d’ajouter ou de supprimer des transactions dans la chaîne.

les principaux algorithmes de hachage utilisés sont les suivants:

* SHA256 (Bitcoin/Ethereum)
* Scrypt (Litecoin)
* X11 (Dash)
* Cryptonight (Monero)

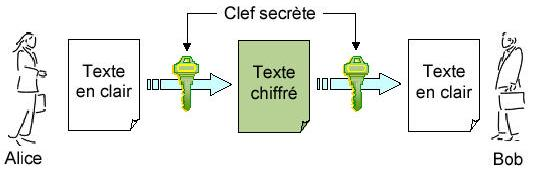
#### **Qu’est-ce que le chiffrement ?**

D’après [1], *le chiffrement est l’ensemble des processus permettant à une donnée d’être transformée en une autre incompréhensible pour qui ne connaît pas la donnée originale, puis, partant de la transformation, d’être retransformée en donnée d’origine.*

Pour une transaction, il faut donc avoir recours à deux traitements conjoints et bijectifs : l’un de chiffrement, l’autre de déchiffrement. On parle alors de correspondance univoque entre l’ensemble des données en clair et l’ensemble des données chiffrées.

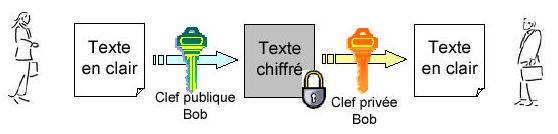
#### **Chiffrement symétrique/asymétrique**

**Symétrique**: la même clé sert à chiffrer et déchiffrer (il faut garder sa clé secrète, les deux parties connaissent la clé)



*Figure 2: Chiffrement symétrique (source: http://igm.univ-mlv.fr/~dr/XPOSE2007/vma\_PKI/concepts\_de\_base.html)*

**Asymétrique**: Chacun possède une clé publique (visible par tous) et une clé privée. La clé privée sert à déchiffrer les messages chiffrés par la clé publique.



*Figure 3: Chiffrement asymétrique (source: http://igm.univ-mlv.fr/~dr/XPOSE2007/vma\_PKI/concepts\_de\_base.html)*

La transaction asymétrique garantit la confidentialité (seul le destinataire peut déchiffrer le message avec sa clé privée) et l’authentification (la clé privée permet de signer les messages et la clé publique à vérifier le signataire).

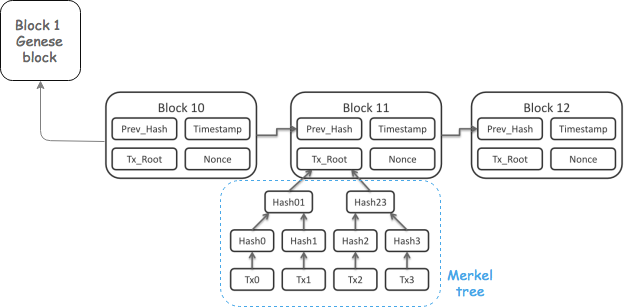
Les figures 2 et 3 montrent la différence entre le chiffrement symétrique (figure 2) et le chiffrement asymétrique (figure 3).

### 1.3.2 - La chaîne de blocs

Nous allons développer un peu plus en détails le fonctionnement de cette blockchain.

La chaîne de blocs porte bien son nom : à partir d’un premier bloc appelé *bloc genèse*, des blocs vont être liés au bloc genèse pour créer la chaîne. Chaque bloc contiendra les informations hachées des blocs précédents et du registre des transactions effectuées sur le réseau.

Pour créer un bloc, il suffit de rassembler un certain nombre de transactions (fixe et déterminé par la taille du bloc) et de les ajouter à un bloc.

[](https://www.draw.io/#G0BxYwN-yW1kTbWFg2VEJRVWhPOW8)

*Figure 4: Constitution d’un chaîne de bloc.*

*(source: https://blockgeeks.com/guides/what-is-hashing/)*

Comme le montre la figure 4, l’intégrité de la chaîne de blocs est garantie par le fait que chaque bloc contient un hash du bloc précédent (**Prev\_Hash**), d’où la nécessité d’un bloc genèse qui aura une construction différente. De cette manière, un utilisateur mal intentionné ne peut pas tenter de rajouter ou de supprimer une transaction ancienne sur le registre, car cette modification invaliderait le bloc qu’il tenterait de modifier.

Le bloc contient également d’autres données décrites ci-dessous.

#### **Timestamp**

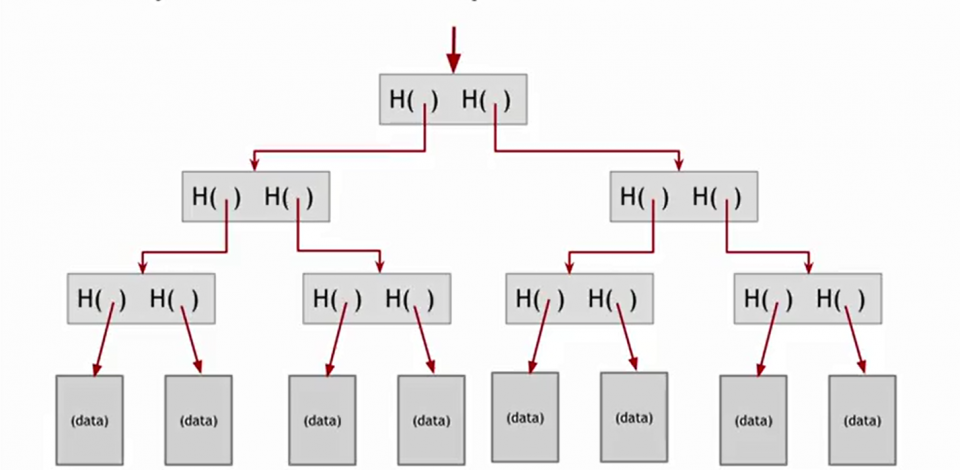
C’est la preuve temporelle de l’action effectuée relayée par le bloc. Cette information ajoute une variable supplémentaire dans la complexité du hash, qui devient encore plus dur à décrypter. Il rend également le bloc entier plus dur à manipuler pour d’éventuels utilisateurs malveillants.

#### **Nonce**

C'est le nombre qui valide le bloc. Le nonce est un nombre unique qui, associé aux données du bloc, donne un hash avec un nombre de "leading" 0 demandé dépendant de la difficulté. Il permet également de protéger les blocs contre les attaques par rejeu (qui permettent notamment d’usurper une identité).

#### **Tx\_Root : Registre des transactions**

Le registre des transactions effectuées sur le réseau est stocké ici, sous la forme d’un Merkle tree (figure 5). Un Merkle tree est un arbre de hash successifs qui permet de transmettre des données de manière cachée et simplifiée : les données brutes sont aux racines de l’arbre, et pour monter aux feuilles, on réalise le hachage successif des données.



*Figure 5: Merkle tree*

*(source: http://learningspot.altervista.org/hash-pointers-and-data-structures/merkle\_tree/)*

Si nous avons besoin de prouver l'existence d’une donnée, il n’est pas nécessaire de prendre tout l’arbre, il suffit de prendre une branche de l’arbre remontant jusqu’au hash feuille.

### 1.3.3 - Transactions

Une transaction s’effectue en plusieurs étapes. Prenons deux acteurs, Bob qui veut envoyer de l’argent à Alice, comme le montre la figure 6:

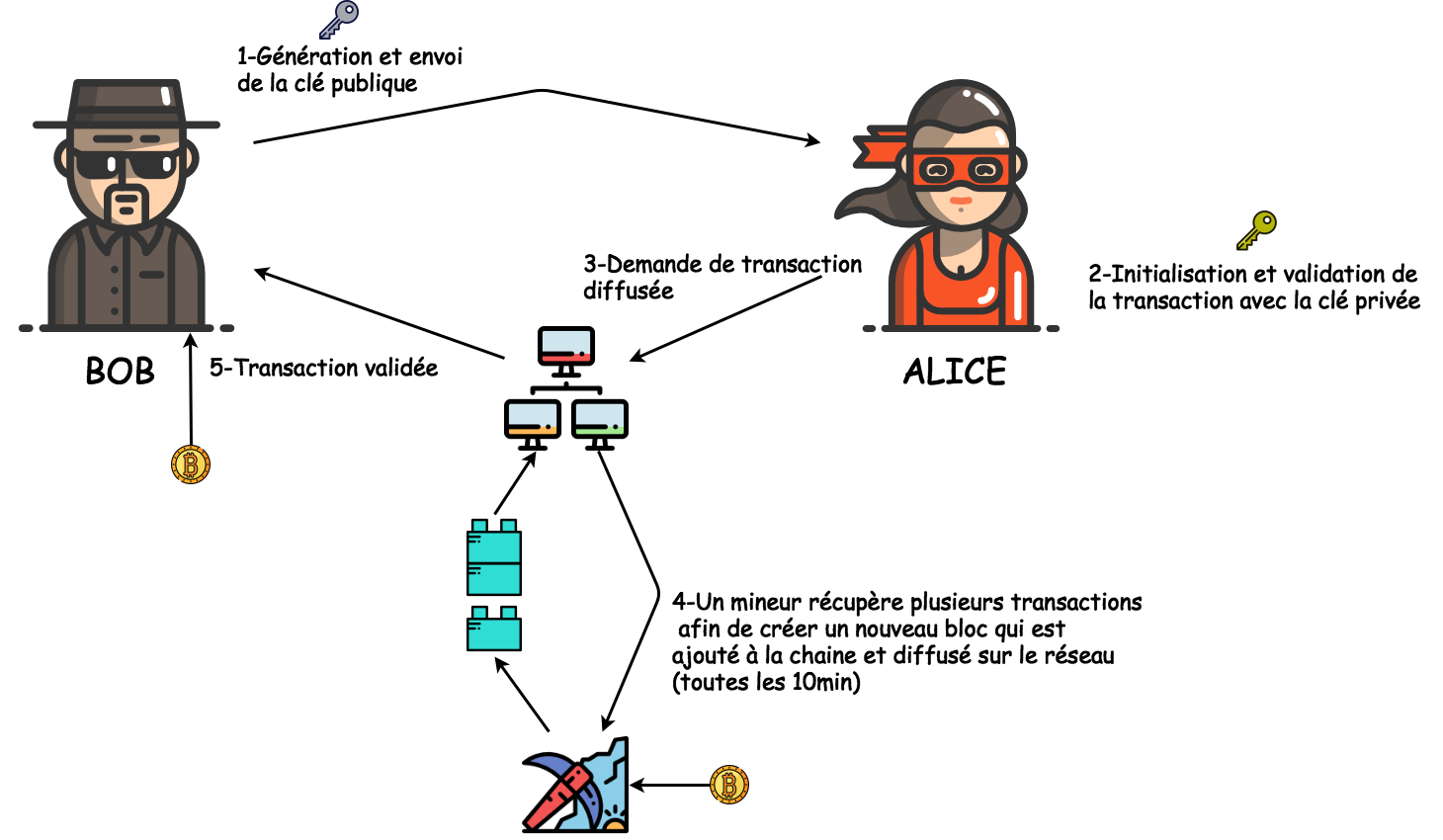
[](https://www.draw.io/#G0BxYwN-yW1kTbZUlRT0VJRzYxNGM)

*Figure 6: Exemple de transaction d’argent de Bob à Alice.*

Tout d’abord, Bob et Alice ont pris soin de créer un wallet, le fonctionnement et les différents types de wallets sont développés en annexe 6.1. Pour la suite, il faut simplement retenir que le wallet fonctionne avec un jeu de clé asymétrique. Une clé privée est créée et garde les comptes, une clé publique est distribuée afin de recevoir le paiement.

|  |  |
| --- | --- |
| **Clé publique**  Elle représente l’adresse “externe” de livraison des bitcoins. C’est cette clé qui est transmise pour recevoir des paiements. Toutefois il est possible de générer une clé publique unique lié à une transaction. C’est la méthode qui est conseillée. | **Clé privée**  Cette clé permet d’accéder au wallet et de pouvoir envoyer des bitcoin. Cette clé doit être protégée et mise en sécurité. |
| Ce jeu de clé est généré avec ECDSA (algorithme basé sur les courbes elliptiques). Ethereum et Bitcoin utilisent “secp256k1” qui fait référence aux paramètres de l'algorithme ECDSA défini dans un document de certicom research.  source: <http://e-ducat.fr/links/ecdsa/>, | |

La figure 7 décrit le cycle d’une transaction dans le cadre de la monnaie Bitcoin:

[](https://www.draw.io/#G0BxYwN-yW1kTbTEI0SzV0MGdqLVk)

*Figure 7: Processus d’une transaction.*

1 - Bob donne une clé publique à Alice. Cette clé est soit directement la clé publique correspondant au compte de Bob, soit une clé générée spécialement pour cette transaction, avec un identifiant unique.

2 - Alice initialise le paiement à l’aide de sa clé privée vers la clé publique de Bob. C’est le seul moyen d’initier une transaction: avoir une clé privée pour signer sa transaction.

3 - La transaction est diffusée sur le réseau. Tout le monde sera au courant de cette transaction qui sera identifiée par un “hash”.

4 - Toutes les 10min, cette transaction est récupérée avec d’autres par un “mineur” qui les rassemble dans un bloc.

5 - Le bloc est ajouté à la chaîne et identifié par un “hash”. Celui-ci contient les informations du bloc précédent.

|  |  |
| --- | --- |
|  | **Est ce anonyme?** Oui, personne ne peut remonter à votre clé privée à partir de votre clé publique grâce au système de chiffrement asymétrique. Toutefois, on peut noter que plusieurs facteurs/étapes peuvent rompre cet anonymat. (lors de l’envoi de la clé publique, lors de l’échange du bitcoin en dollar / euro etc…  **Peut-on envoyer des demi-bitcoin?** Oui, si nous avons 50 bitcoins et que l’on veut en envoyer que 0.5, 2 transactions sont créées. Une de 0.5 pour le destinataire et une de 49.5 pour soi même. La figure 8 illustre cette opération:    *Figure 8: Exemple d’une transaction de 0.5BTC (Bitcoins)*  *(source: https://bitcoin.stackexchange.com/questions/32772/how-do-i-find-the-txid-and-vout-values-for-an-input-i-want-to-spend)* |

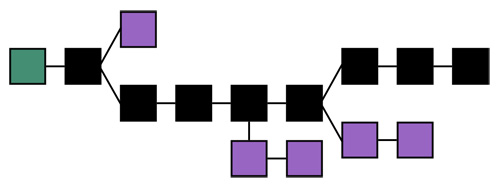
Pour le bitcoin, on peut opérer cette division jusqu’à .

### 1.3.4 - Réseau distribué

Comme nous l’avons cité, les blocs sont distribués et diffusés sur tout le réseau pair-à-pair. Il faut s’assurer que les blocs ne sont pas créés en double sur un réseau. C’est ici qu’intervient la notion de “fork”.

comme le montre la figure 9, le “fork” est une séparation dans la chaîne qui crée une nouvelle branche. Deux nouveaux blocs dépendent d’un même bloc source. Il faut déterminer lequel est le bon.

Dans Bitcoin, c’est la chaîne la plus longue qui est valide. Pour déterminer si le bloc est bon il suffit de chercher et de compter les blocs sous-jacents créés.



*Figure 9: Représentation de plusieurs forks sur une blockchain*

*(source medium.com)*

Afin d’être sûr qu’une transaction est valide, il faut attendre quelques blocs. Généralement celle-ci est considérée sûre à partir de 6 blocs antécédents créés (cette valeur est amené à changer selon la technologie et les personnes).

* 3 blocs, rare que la transaction soit invalide
* 6 blocs, transaction considérée comme valide

Les transactions sont toujours enregistrées quelque soit la branche empruntée.

|  |  |
| --- | --- |
|  | **Le réseau est-il sujet au SPAM?** Non, la parade a été de rendre toutes transactions payantes. Par ce biais, un spammeur aurait à débourser beaucoup d’argent pour attaquer le réseau.  **Quelqu’un de malveillant peut il influer sur les forks?** Il faudrait beaucoup de puissance de calcul et qu’il soit majoritaire sur le réseau (>51%). Il pourrait peut être aller plus vite qu’une branche déjà créée. Il peut annuler les transactions mais pas faire des transactions à la place d’autres. |

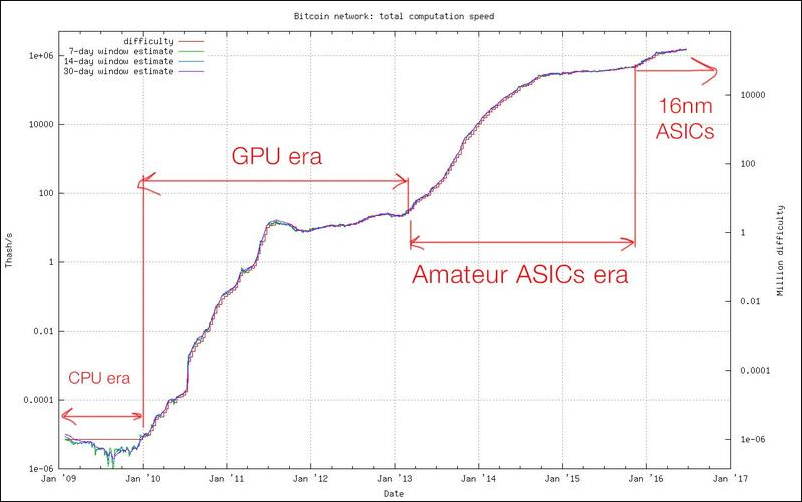
### 1.3.5 - Le minage

Le minage est l’action clé de la blockchain. Le principe est de rassembler les transactions diffusées sur le réseau et de les écrire dans un registre. Cette action permet de valider un bloc. Le minage nécessite beaucoup de puissance de calcul. Les acteurs pour réaliser le minage sont appelés “Mineur”. l existe plusieurs types de minage, le PoW et PoS qui sont développés dans la section suivante.

Au début, il s’agissait de personnes qui croyaient en la technologie, aujourd’hui ce sont des personnes qui font cela pour la rémunération.

L’algorithme de Bitcoin permet aux mineurs la création de blocs sans transactions pour générer des bitcoins. La rémunération par minage du bitcoin est plafonnée, les mineurs ne seront à terme plus rémunérés par la création de bloc mais par les validations des transactions seulement. Cependant il reste encore du temps, cette échéance serait prévue pour 2140...

Le minage est lié à une difficulté qui est pondérée au temps de création d’un bloc défini. Pour le bitcoin, un bloc est créé toutes les 10min. Si de nouveaux mineurs avec beaucoup de puissance de calcul arrivent sur le réseau, la difficulté augmente. Avec les courbes présentées dans la figure 10, nous pouvons bien observer l’influence des mineurs sur la difficultés avec tout d’abord l’introduction des GPU et des FPGA, bien plus adaptés que les CPU pour miner, et par la suite l’introduction des processeurs dédiés au minage (ASICS).



*Figure 10: Influence de l’introduction des FPGA et ASIC pour le minage*

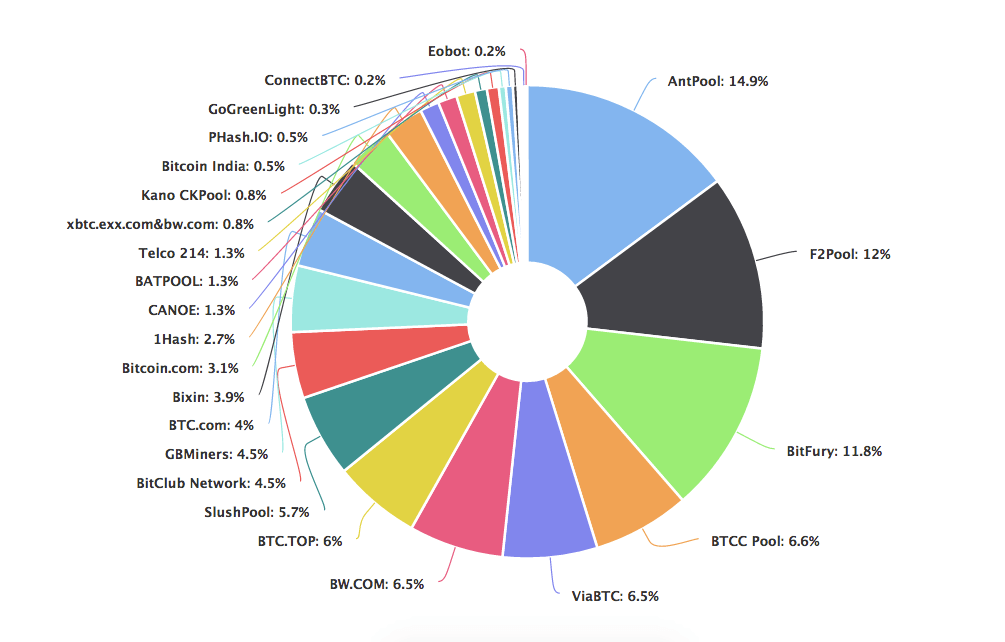
*(source: Google Images - jehf.gmjk.me)*

Il faut savoir que le Bitcoin et son principe de difficulté de minage a causé l’inflation rapide du prix des cartes graphiques. L’apparition des processeurs dédiés au minage a vu le jour pour ralentir cette inflation, qui devient handicapante pour les utilisateurs.

Le seul avantage de ce choix serait de sécuriser le réseau, car pour avoir la mainmise sur le réseau entier, il faut réunir plus de 50% de la puissance de calcul totale. Cependant ce choix défavorise les mineurs indépendants qui ne peuvent pas investir dans beaucoup de puissance. Ce choix a donc favorisé l’apparition de pools de minage.

**Les Pools de minage** sont des “organisations” réunissant des mineurs se répartissant les gains minés par l’ajout de bloc. A chaque fois qu’un membre d’une pool trouve un bloc, l’argent gagné est répartie sur le pool entier. Les gains sont donc amoindris, mais plus régulier qu’en minant de manière indépendante.

Le camembert ci-dessous (figure 11) montre la répartition de la puissance de minage dans les pools et les indépendants.



*Figure 11: Répartition des pools sur la puissance de calcul*

*(source: kaspersky.fr )*

On remarque que si quelques pools s’allient, ils seraient capables d’avoir la main sur le réseau entier, étant donné qu’ils détiendraient plus de 50% de la puissance globale. De ce fait, ces pools ont déjà subi des attaques pour manipuler les blocs, mais comme toutes les transactions sont publiques et visibles par tout un chacun, la supercherie a été vite révélée. L’économie du bitcoin ne s’est donc pas effondrée.

|  |  |
| --- | --- |
|  | **Consommation?** Cela n’est pour le moins pas très écologique, pour le minage du Bitcoin et de l’Ethereum, la consommation est estimée à 19,23 Térawatts par heure, soit plus que la consommation de l’Islande et de quoi alimenter 1.2 millions de foyer.  *src:http://www.clubic.com/antivirus-securite-informatique/cryptage-cryptographie/crypto-monnaie/actualite-833314-crypto-monnaie-minage-consomme-islande.html* |

### 1.3.6 - Les consensus: PoW / PoS

**Proof of Work (PoW) :**  Ce concept permet d’avoir un nombre limité d’utilisateurs qui valident des blocs en même temps. Il se base sur une règle sur le hash : **pour tout hash d’un bloc on doit avoir la valeur de ce hash inférieur à une valeur déterminée aléatoirement (difficulté).**

Le résultat de cette règle est nommée **nonce** comme vu précédemment.

Comme la distribution d’un hash est aléatoire, la manière la plus efficace d’arriver au bon résultat est de faire l’algorithme suivant:

|  |
| --- |
| tant que block\_hash > difficulty  nonce = rand()  block\_hash = hash(block\_header :: nonce) //On effectue à nouveau le hash du bloc fin tant que |

Cet algorithme donne donc la validité d’un bloc. Seuls les mineurs ayant un bloc valide à poser peuvent le faire, dans le cas contraire la branche créée sera mise à l’écart.

Le POW recentralise donc le concept de blockchain. La valeur difficulty représente le nombre de possibilités pour créer un bloc.

Les défauts de ce concept sont que ce concept amène celui de l’augmentation de la difficulté de minage et la consommation épouvantable du réseau, car tout le monde mine pour qu’au final seul un bloc soit porteur de la chaîne.

**Proof of Stake (PoS) :** L'idée du PoS a été introduite pour tenter répondre à la problématique environnementale (de consommation d'énergie élevée, pollution) liée au minage de la PoW. Le but du PoS est de supprimer le minage et de le remplacer par un autre mécanisme.

Le PoS est un minage “virtuel” qui est basé sur la cryptomonnaie elle-même. Un utilisateur investit un certain montant ce qui lui donne le statut de validateur. Sur la base du dernier bloc, l’algorithme sélectionne de manière aléatoire un validateur qui doit créer le prochain bloc. Si ce validateur ne crée pas le bloc dans un intervalle de temps déterminé, un autre validateur est sélectionné, et ainsi de suite. L'aléa sur la sélection du validateur est pondéré par le dépôt (l’investissement) de ce dernier. Un validateur qui a déposé 2000 unités de cryptomonnaie a 2 fois plus de chance d'être sélectionné qu’un validateur qui n’en a déposé que 1000 unités.

### 1.3.7 - Tableau comparatif des algorithmes de hachage

< EN COURS DE REDACTION >

source: <https://en.wikipedia.org/wiki/List_of_cryptocurrencies>

<https://en.bitcoin.it/wiki/Comparison_of_cryptocurrencies>

Cette liste est non exhaustive. Elle a pour but de reprendre le tableau de la source et de restituer le résultat en classant avec comme premier critère les algorithmes hachage.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Algorithmes** | **Type POW or POS** | **Crypto-monnaie(s)** | **ASICs / GPU** | **Anonymat** | **Génération clé** |
| SHA-256d | Pow | Bitcoin, NXT.. | ASICs | Faible | ECDSA |
| Etash | PoW | Ethereum, Ubiq.. | GPU | Faible | ECDSA |
| Scrypt | PoW | Litecoin, Dogecoin.. | ASICs | Faible |  |
| CryptoNight | PoW | Monero, Aeon ... | GPU | Moyen |  |
| X11 | Pow & PoS | Dash | ASICs | Faible |  |
| ECDSA | Consensus | Ripple | / |  |  |
| Pos | PoS | Waves | / |  |  |
| SHA3 | ... | IOTA | / |  |  |
| ... | ... | …. |  |  |  |

## 

## 

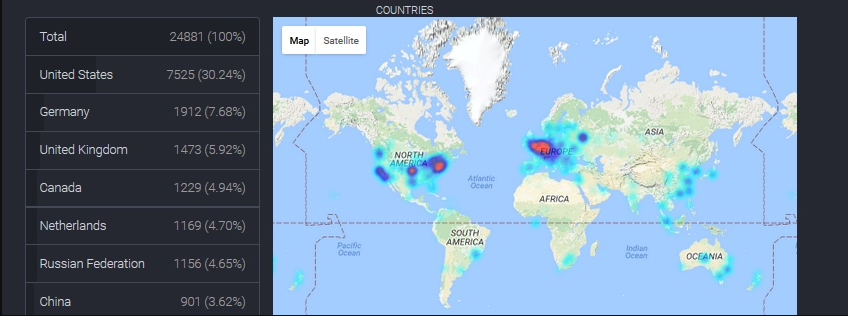
# 2 - FOCUS ETHEREUM

## 

## 2.1 - Présentation

Nous venons de voir que Bitcoin, basé sur la technologie blockchain, permet d’échanger une cryptomonnaie (le bitcoin, BTC) de pair-à-pair, et ce, de manière sécurisée et sans intervention d’un tiers (banque, centralisation). Quand Bitcoin a commencé à être attractif, plusieurs projets ont été développés afin d'améliorer certains points bloquants de Bitcoin et proposer d’autres types de transactions que des transferts de “token”. Ces projets, aussi appelés “AltCoins”, ont toujours ajouter leurs fonctionnalités sur des blockchain séparées. C’est ainsi que le fondateur d’Ethereum, Vitalik Buterin, a proposé son idée: au lieu de recréer une blockchain à chaque application, pourquoi ne pas créer une blockchain programmable et assez flexible pour satisfaire toutes ces applications?

L’objectif d’Ethereum tend à répondre à cette question. Ethereum est une plateforme qui, en plus d’avoir sa crypto-monnaie (l’Ether, ETH) pour fonctionner, permet la création d’application décentralisée, et d’avoir ainsi une blockchain publique qui s’adapte et flexible. C’est la vision de la blockchain de demain. Voici un aperçu du nombre de noeuds (au 11/10/17) du réseau Ethereum :



*Figure 12: Répartition des noeuds sur la carte mondiale*

*(source: trustnodes.com )*

## 2.2 - La machine virtuelle d’Ethereum

Ethereum est une blockchain programmable. Au lieu de donner aux utilisateurs un ensemble d'opérations à exécuter (comme le Bitcoin), Ethereum permet aux utilisateurs de créer leur propres opérations et applications. Mais ces opérations doivent être comprises par tous les noeuds du réseau. Ceci est assuré par l’EVM (Ethereum Virtual Machine). Ethereum est dit “Turing complet”, ce qui signifie que les applications qui tournent sur l’EVM peuvent être programmées avec des langages de programmation qui implémentent au moins toutes les fonctions de calculs au sens de Turing.

Tous les noeuds du réseau opèrent l’EVM et exécutent les mêmes instructions. Ethereum peut donc être vu comme un ordinateur décentralisé. Cette parallélisation sur tout le réseau Ethereum n’est pas fait accélérer les opérations, car au contraire Ethereum est beaucoup plus lent qu’un ordinateur classique. Chaque noeud du réseau exécute cette EVM dans le but de maintenir le consensus du réseau à travers la blockchain. Ainsi, Ethereum garantit un haut niveau de tolérance aux fautes, un stockage des données de la blockchain immuable (n’est pas sujet au changement) et une résistance à la censure / corruption.

## 2.3 - Les Comptes: notion majeure dans Ethereum

A la différence de Bitcoin qui tient un registre de transactions, Ethereum fonctionne en termes de comptes. Il existe 2 types de comptes :

* Externally Owned Account (EOA): compte “utilisateur” géré par une clé privée
* Contract Account: compte d’un contrat qui est géré par son code (instructions EVM). Ce code ne peut être activé que par un EOA.

Ces comptes sont des entités qui ont un état :

* Un EOA a un solde (Balance)
* Un Contract Account a un solde (Balance) et du stockage (du code, de l’information…)

L'état de tous les comptes est l'état du réseau Ethereum qui est mis à jour avec chaque bloc et sur lequel le réseau s’accorde selon le concept de consensus. Les comptes sont essentiels pour que les utilisateurs interagissent avec la blockchain Ethereum via des transactions.

La blockchain Ethereum suit l'état de chaque compte et toutes les transitions d'état sur la blockchain Ethereum sont des transferts de valeur et d'informations entre les comptes.

Si Ethereum était réduit aux EOA permettant seulement des transactions entre eux, Ethereum serait un AltCoin et servirait à transférer une cryptomonnaie, l’Ether.

Il faut donc bien mettre en évidence l’importance des Contract Account qui permettent de rendre la blockchain Ethereum “programmable”, à travers l'exécution de programmes, les smart contract.

Le terme “smart contract” représente le code stocké dans un Contract Account. Ce programme est exécuté seulement si une transaction est envoyée à ce compte. Cette transaction ne peut être envoyée que par EOA. Un smart contract ne peut donc pas s'exécuter en “tâche de fond”.

Comme pour Bitcoin, un compte est associé à une paire clé privée / clé publique. Un compte est indexé sur le réseau par son adresse qui est dérivée de la clé publique: il s’agit des 20 derniers octets.

Un compte est créé sur un noeud du réseau. Les clés associées à ce compte sont stockées en local dans le répertoire des données du noeud Ethereum. Il s’agit bien d’un répertoire dédié à Ethereum (ce répertoire contient aussi, entres autres, la base de donnée de la blockchain). Ces clés doivent être sauvegardées afin de ne pas perdre le(s) compte(s) et donc leur solde. Une autre alternative consiste à utiliser un Wallet matériel (voir Annexe 6.1 - Le Wallet).

## 2.4 - Contrats et Transactions

**En cours de rédaction.**

### 2.4.1 La transaction

Dans Ethereum, une transaction est définie par un paquet signé d’informations contenant un message envoyé d’un EOA vers un autre compte (EOA ou Contrat).

Ethereum implémente aussi des objets virtuels, les messages. Un message peut être déclenché seulement par un contrat et est destiné à un autre contrat. Les messages sont dédiés à l’interaction entre les contrats.

### 2.4.2 Le contrat

Le contrat fait référence au “Contract Account” de la section précédente. Un contrat :

* a un solde (Balance)
* a du code associé (exécuté sur l’EVM)
* exécute son code sur demande (transaction) d’un EOA ou sur un message d’un autre contrat

Toute action sur le réseau Ethereum est issue d’une transaction réalisée par un EOA. Quand un contrat reçoit une transaction, il exécute son code selon les paramètres d’entrée contenus dans la transaction. Le code du contrat est exécuté dans l’EVM de chaque noeud qui participe au réseau en vérifiant les nouveaux blocs. Comme un bloc est déterminé valide au bout du sixième bloc, on voit bien que les performances temporelles ne sont pas la force d’Ethereum.

Retenons ici qu’il ne faut pas faire ce pour quoi Ethereum n’est pas fait. Ethereum n’est pas une plateforme de parallélisation de calcul haute performance.

## 2.5 - Le minage dans Ethereum

Le minage permet de sécuriser et vérifier le réseau, ainsi que de créer la cryptomonnaie. Le minage dans Ethereum est le même principe que celui de Bitcoin. Néanmoins, il y a quelques différences inhérentes au fonctionnement et à l'idéologie d’Ethereum. Cette partie ne définit donc pas en quoi le minage consiste, puisqu’il a été détaillé dans le chapitre précédent. Cette section se focalise sur les fonctionnalités / modifications apportées par Ethereum.

### 2.5.1 - L’algorithme Dagger-Hashimoto

Avec l’utilisation intense des ASICS et des pool de minage, Bitcoin a vu apparaître une certaine centralisation allant alors à l’encontre de l'idéologie de décentralisation apportée par Bitcoin à l’origine.

Pour pallier à ce phénomène, Ethereum a combiné deux algorithmes dans le but d'éviter l’utilisation d’ASIC. L'idée est d'implémenter un algorithme de PoW (l’Ethash PoW) qui réponde aux 2 points suivant :

* *ASIC-resistant*: le bénéfice d'implémenter l’algorithme sur un ASIC doit être aussi minimal que possible. Ainsi, les mineurs sont contraints d’utiliser des CPU (éventuellement combiné à un GPU).
* Vérification par un client léger: étant donné que tous les noeuds du réseau vérifient un bloc, l’algorithme de vérification doit être efficace (nécessite peu de ressources CPU et mémoire) de manière à être possible sur un client léger (faible ressources).

### 2.5.2 - Les blocs *“oncles”*

Comme expliqué dans le chapitre précédent, dans Bitcoin, c’est toujours la chaîne la plus longue qui est acceptée par le réseau.

Dans Ethereum, étant donné que le temps de minage entre les blocs a été réduit (à 12 secondes, temps estimé de propagation d’un message sur tout le réseau), une telle stratégie impliquerait qu’un pool de mineurs qui se rapproche des 50% soit le seul à pouvoir miner.

La encore pour éviter le risque de centralisation, Ethereum a modifié la stratégie de minage en ne favorisant non plus la chaîne la plus longue, mais la chaîne ayant le plus de “poids”. Ainsi, lorsqu’une chaîne contient des “fork” (duplication), alors abandonnés (orphelins) dans Bitcoin, ces derniers apporte un “poids” et sont rémunérés. Ces blocs sont appelés des blocs “oncles”.

Ceci favorise les mineurs moins “puissant” et tend à conserver la décentralisation, idéologie principale dans Ethereum.

## 2.6 - Le modèle économique d’Ethereum

**En cours de rédaction.**

Ethereum, pour son fonctionnement, a établi un modèle économique. Une brève description est donnée dans cette section.

### 2.6.1 - C’est quoi l’Ether?

### 2.6.2 - Le WEI

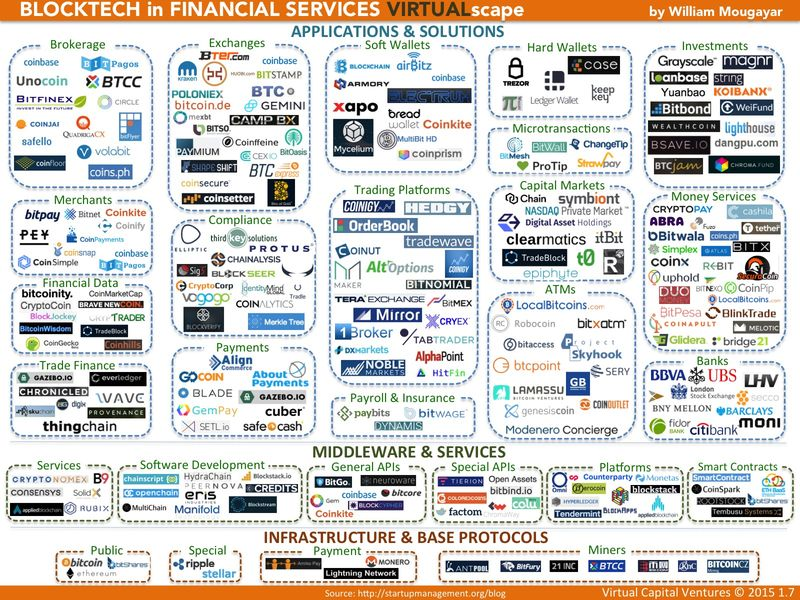
### 2.6.2 - Le GAS

# 3 - L'ÉCOSYSTÈME DE LA BLOCKCHAIN

**<PARTIE EN COURS DE RÉDACTION>**

## 3.1 - L’application “landscape”

2017 est une année faste pour le technologie de la blockchain. Aujourd’hui il y a beaucoup d’acteurs, cette infographie (figure 12) résume les différents domaines et acteurs:



*Figure 12: Application landscape*

*(source:http://startupmanagement.org/2015/12/08/update-to-the-global-landscape-of-blockchain-companies-in-financial-services/)*

## 3.2 - Quelques exemples

On peut déjà répertorié de nombreux cas utilisant la blockchain. Nous en avons sélectionné quelques uns pour leur application, ou pour les acteurs du projet. Cela montre la variété des domaines où la blockchain peut apporter une plus value, ou même être disruptive. Cette liste est bien sûr non exhaustive.

## 

*Figure 13:*

*(source: blockchain\_livre\_blanc\_20160204\_shared)*

|  |  |
| --- | --- |
| **ENERGIE** | **BROOKLYN MICROGRID**  Création d’un système de production et d’échange d’énergie en autonomie. La production d’énergie est solaire. L’échange est réalisé via une blockchain fonctionnant sous ethereum.    *Source(s):* [*https://www.wedemain.fr/A-Brooklyn-les-habitants-echangent-de-l-energie-solaire-locale-grace-a-la-blockchain\_a1780.html*](https://www.wedemain.fr/A-Brooklyn-les-habitants-echangent-de-l-energie-solaire-locale-grace-a-la-blockchain_a1780.html)  [*http://lo3energy.com/*](http://lo3energy.com/) |
| **SMARTGRID LYON CONFLUENCE**  Reprise du concept mis en place à Brooklyn à Lyon par Bouygues Immobilier, Energisme et Stratumn pour l'éco-quartier Lyon Confluence.  *Source(s): http://www.lemonde.fr/smart-cities/article/2017/09/27/la-blockchain-ouvre-le-champ-des-possibles-pour-la-smart-city\_5192463\_4811534.html* |
| **BORNE DE RECHARGE AUTOMOBILE AUTONOME**  Innology (filiale de l'énergéticien allemand RWE) implante des bornes de chargement chez les particuliers utilisable par toute personne ayant besoin de recharger sa voiture. Il est possible de définir des tarifs préférentiels pour une personne souhaité. La personne propriétaire de cette borne est donc rémunérée.  *Source(s): https://blog.slock.it/share-charge-launches-its-app-on-boards-over-1-000-charging-stations-on-the-blockchain-ba8275390309* |
|  | |
| **TRACABILITE** | **PRODUITS ALIMENTAIRES**  Prototype proposé par Intel pour suivre l'origine des poissons avec un capteur qui fixé à la cagette dès la pêche sur le bateau. Ce capteur envoi des informations (température, localisation, humidité etc..) tout au long des étapes du transport.  *source: etude blockchain partner* [*https://blockchainpartner.fr/wp-content/uploads/2017/06/Etude-supply-chain-tra%C3%A7abilit%C3%A9-blockchain.pdf*](https://blockchainpartner.fr/wp-content/uploads/2017/06/Etude-supply-chain-tra%C3%A7abilit%C3%A9-blockchain.pdf) |
| **MÉDICAMENTS**  Vérification de l'authenticité d’un médicament acheté grâce à une application mobile.  *source: https://www.blockpharma.com/* |
| **TRUST** | **VOTE EN LIGNE**   * Le parti “Nous Citoyens” en France a récemment utilisé la blockchain pour garantir la sécurité et la transparence des votes en ligne pour une de ses élections internes   *source:* [*https://www.frenchweb.fr/voter-via-la-blockchain-experimentations-et-retours-dexperience/240683*](https://www.frenchweb.fr/voter-via-la-blockchain-experimentations-et-retours-dexperience/240683)   * Expérimentation d’une solution de vote en ligne par Karpersky, nommée Polys.   *source: https://www.silicon.fr/telegrammes-dix-nouveaux-langages-pour-microsoft-translator-kaspersky-securise-le-vote-par-blockchain-facebook-travaille-avec-airbus-191055.html?inf\_by=59ed6931671db8686e8b484c* |
| **CADASTRE NUMÉRIQUE**  Au Ghana en permettant aux propriétaires d’arpenter leurs terres via GPS et d’enregistrer leurs actes fonciers sur une Blockchain.  *source:* [*https://www.info-afrique.com/cadastre-ghana-blockchain/*](https://www.info-afrique.com/cadastre-ghana-blockchain/) |
| **SANTÉ** | **REGISTRE MÉDICALE**  Enregistrement et sécurisation des données médicales en estonie et en chine utilisant la blockchain et développée par la société guardtime.  *source:*  [*https://cointelegraph.com/news/estonian-government-adopts-blockchain-to-secure-1-mln-health-records*](https://cointelegraph.com/news/estonian-government-adopts-blockchain-to-secure-1-mln-health-records)  [*https://cointelegraph.com/news/alibaba-deploys-blockchain-to-secure-health-data-in-chinese-first*](https://cointelegraph.com/news/alibaba-deploys-blockchain-to-secure-health-data-in-chinese-first) |
| **ASSURANCE** | **INDEMNISATION RETARD**  C’est une des applications phare des smart-contrats. Disposer de conditions de remboursement au moment d’un achat. C’est notamment le cas dans le domaine du tourisme. (exemple billet d’avion). Une société propose le concept sous ethereum.  *source:* [*https://etherisc.com/*](https://etherisc.com/) |
| **FINANCE** | **Transactions bancaires**  C’est bien sur le domaine de prédilection d’application de la blockchain qui permet d’envoyer de l’argent à n’importe qui sur terre sans un tier de confiance tel que les banques. Nous ne nous étalerons par ce sujet et laissons soin au lecteur de se renseigner sur les différentes crypto-monnaie existante. |
| **ARTISTES** | **Domaine de la musique**:  C’est un domaine prometteur pour la blockchain. En effet, la rémunération direct des artistes pourrait permettre de supprimer certains intermédiaires. De plus les smart-contrats pourraient s'avérer utile pour rediriger les revenus aux différents membres d’un groupe.  *source:* [*http://amp.weforum.org/agenda/2017/07/how-can-creative-industries-benefit-from-blockchain?utm\_medium=referral&utm\_campaign=amp&utm\_source=www.weforum.org-RelayMediaAMP*](http://amp.weforum.org/agenda/2017/07/how-can-creative-industries-benefit-from-blockchain?utm_medium=referral&utm_campaign=amp&utm_source=www.weforum.org-RelayMediaAMP) |
| **IOT** | **SLOCKIT**  C’est une entreprise fondée par un ancien collaborateur de Ethereum et qui a développé une technologie à orientation IOT reposant sur ce dernier. Elle a participé à la mise en place de bornes de recharges automobiles citées un peu plus tôt dans ce rapport.  *source:* [*https://slock.it/*](https://slock.it/) |
| **IOTA**  IOTA prône développer une prochaine génération de blockchain, dédiée à l’IOT et n’utilisant plus les notions de POW ou POS. De plus un accord a été signé avec sopra steria/  *source:* [*https://www.soprasteria.com/fr/media/communique/la-blockchain-au-service-de-l-iot-sopra-steria-noue-un-partenariat-avec-iota*](https://www.soprasteria.com/fr/media/communique/la-blockchain-au-service-de-l-iot-sopra-steria-noue-un-partenariat-avec-iota) |
| **DIVERS** | **STOCKAGE CLOUD DISTRIBUÉ**  La startup storj propose des espaces de stockages distribué en opposition au modèle centralisé actuel du cloud. N’importe quel utilisateur peut décider de dédier une partie de son disque dur au stockage. Il est rémunéré pour cette action. Cette application est basée sur Ethereum.  *source: https://storj.io* |

## 

# 

## 

## 

# 

# 

# 4 - Conclusion

**<EN COURS DE RÉDACTION>**

**UNE NOUVELLE TECHNOLOGIE**

A l’issue de cet état de l’art, nous sommes convaincu d’une chose, 2017 a été une année faste pour la blockchain. En effet nous avons pu remarquer par nos recherches que 90% des articles dataient de l’année 2017. (de nombreuses sources sur le bitcoin était en revanche plus ancienne)

Nous tirons ces quelques conclusions de cette “fraîcheur” de l’information:

* Au départ adossée et cantonnée au bitcoin, la blockchain montre son potentiel afin d’être appliquée à d’autres domaines
* C’est une technologie en émergence. Cela rime avec une multiplicité des acteurs qui se lancent dans l'aventure. Certains tirent déjà leur épingle du jeu mais nous ne sommes pas à l’abri qu’une jeune pousse innovante devienne un acteur incontournable dans les prochaines années. (le “tri” n’a pas encore été fait)
* Les informations sont récentes, les PoCs sont nombreuses, mais il n’y a pas de forte tendance à déterminer.
* Certaines sources sont donc à prendre avec des pincettes, difficile d’être affirmatif sur certains points avec si peu de recul.
* Des acteurs tels que Microsoft ou IBM proposent aujourd’hui de déployer des blockchains as-a-service afin que les entreprises déploient leur propre blockchain privée.
* Cet état de l’art est nécessairement non exhaustif et plusieurs informations seront surement déjà obsolètes d’ici un an.

**LA GOUVERNANCE**

Point d’ordre que nous avons pu relever, sans gouvernance la place de la gouvernance reste importante.

**ETHEREUM ET LES SMART-CONTRACTS**

Ethereum est aujourd’hui une des solutions les plus fiables pour développer des applications décentralisées. Nous avons fait le choix de développer une application ethereum afin de démontrer l’intérêt d’un smart contrat. Toutefois nous pouvons remarquer qu’aujourd’hui d’autres acteurs sont présent dans ce domaine. Ethereum a une longueur d’avance car il y a déjà de nombreux tutoriels disponibles sur internet et elle dispose déjà d’une certaine notoriété pour les entreprises, mais il n’est pas dit que ce soit la solution adaptée à tous les besoins.

Viabilité des smart contracts ?

**QUELQUES EXEMPLES D’INFOS EN MOUVEMENT**

Lorsque nous avons commencé cet état de l’art, nous avions eu une information toute fraîche du désir de l’Estonie de se lancer dans la crypto-monnaie qui à été botté en touche par la BCE (Banque Centrale Europpéene)

<https://www.businessbourse.com/2017/09/12/bce-interdit-a-lestonie-de-lancer-propre-crypto-monnaie-toute-concurrence-a-leuro-interdite/>

Aujourd’hui, seulement deux mois après, les décisions des banques centrales de la Russie ou la Chine par exemple ont amené la BCE à revoir leur position et à étudier de plus près la réglementation de la cryptomonnaie. <https://f-lys.com/2017/11/18/la-banque-centrale-europeenne-envisage-de-reglementer-le-bitcoin-selon-les-membres-du-conseil/>

Autre exemple, lors de nos recherches nous avions vue une nouvelle technologie de blockchain dédiée à l’IOT, IOTA, qui n’avait pas forcément retenue notre attention. Après parcours du livre blanc nous n’avions pas été convaincu par cette solution. Aujourd’hui cette entreprise a signer un accord avec sopra-steria <https://www.silicon.fr/iot-securite-sopra-steria-iota-blockchain-190559.html> nul doute que cela va booster cette technologie.

**NOTRE AVIS**

Pour notre part nous sommes particulièrement convaincu de l’avenir de la technologie pour des utilisations du quotidien. Le couplage avec les domaines de l’écologie, de

# 

# 5 - Acronymes, Définitions & Sources

|  |  |
| --- | --- |
| ACRONYMES | |
| P2P | Peer to peer |
| POW | Proof Of Work (preuve du travail) |
| POS | Proof Of Stake (preuve de l’état) |
| ETH | Ether, monnaie de l’ethereum |
| BTC | Bitcoin, monnaie du bitcoin |
| EOA | Externally Owned Account |
| DAG | Directed Acyclic Graph |
| ASIC | Application Specific Integrated Circuit |
| OMC | Organisme Mondial du Commerce |
| SWIFT | Society for Worldwide Interbank Financial Telecommunication |
| CERN | Conseil européen pour la recherche nucléaire |
| **DEFINITIONS** | |
| Peer To Peer | Egalement nommé P2P ou réseau pair à pair, est un modèle de [réseau informatique](https://fr.wikipedia.org/wiki/R%C3%A9seau_informatique) proche du modèle [client-serveur](https://fr.wikipedia.org/wiki/Client-serveur) mais où chaque [client](https://fr.wikipedia.org/wiki/Client_(informatique)) est aussi un [serveur](https://fr.wikipedia.org/wiki/Serveur_informatique). Les termes « [pair](https://fr.wikipedia.org/wiki/Pair) », « [nœud](https://fr.wikipedia.org/wiki/N%C5%93ud) », et « utilisateur » sont généralement utilisés pour désigner les entités composant un réseau P2P[1](https://fr.wikipedia.org/wiki/Pair_%C3%A0_pair#cite_note-1). |
| hash | hachage. Méthode de cryptage d’une donnée en lui donnant une signature unique. Il impossible de revenir sur la donnée de base depuis le hachage généré. |
| AltCoins | Cryptomonnaie alternative au bitcoin |
| Seed | Graine. Phrase mnémotechnique de minimum 12 mots permettant de générer/regénérer une clé privée. |
| Wallet | Portefeuille permettant de détenir une crypto-monnaie. Créer avec un jeu de clé privée/publique. |
| **SOURCES** | |
| La Blockchain en détail (Benoît Lafontaine - Yann Rouillard) - DEVOXX | https://www.youtube.com/watch?v=J0MgFQ-j6nE |
| “Comprendre la Blockchain” - uchange | https://www.uchange.co/ |
| Wikipedia |  |
|  |  |

# 

# 

# 6 - Annexes

Ces annexes nous permettent d’aller plus loin dans le détail sur des aspects sortant un peu du cadre de cet état de l’art.

## 6.1 - Focus sur le wallet

Toutes transactions effectuées sur une blockchain pour échanger de la crypto-monnaie nécessitent un wallet. Autrement dit, un portefeuille électronique.

Rapidement, un wallet se créer simplement avec la génération d’un jeu de clé asymétrique privée/public. La clé privée sert à confirmer et payer des transactions. La clé publique sert comme adresse de destination pour recevoir les transactions.

Il existe plusieurs types de wallet:

**HOT WALLET\***

* **EN LIGNE**
  + Le portefeuille et la privée clé associée sont stockés en ligne. C’est le cas des wallets sur les plateformes de trading par exemple.
* **MOBILE**
  + Il s’agit d’applications permettant d’effectuer facilement des transactions depuis son mobile. Le jeu clé peut être stocké sur son mobile ou en ligne.
* **ORDINATEUR DE BUREAU**
  + client complet: l’intégralité de la blockchain est téléchargée. L’ordinateur est alors un noeud participant à la consolidation de la blockchain.
  + client léger: l’ordinateur interroge un serveur distant pour accéder à la blockchain. (moins sécurisé que la première solution...)

**COLD WALLET\***

* **PHYSIQUE** 
  + paper wallet: il s’agit de générer un jeu de clé privée et publique et de l’imprimer avec un QRcode afin de réutiliser facilement cette dernièer lorsqu’on le souhaite.
  + hardware wallet: les clefs privées sont conservés sur une puce embarquée. (ledger, trezor ou keepkey)

\*Par définition, nous entendons souvent parlé de “cold wallet”, plus sécurisé et utilisé pour un stockage à long terme. Et les “hot wallet”, moins sécurisé mais permettant déchanger rapidement sur des sites en lignes.

Remarques diverses:

* Pour le Bitcoin, une application référence semble être Electrum. Créer en 2011, cette application est open source. C’est un facteur à ne pas négliger. Un logiciel propriétaire pourrait en effet cacher une backdoor afin d’usurper votre wallet. Electrum propose plusieurs type d’authentification
* Attention lorsque vous télécharger ces différents logiciel, assurez-vous de bien le faire sur le site officiel. En effet, différents site de scam/hameçonnage peuvent vous faire croire que vous avez généré un wallet qui peut être utilisable par une personne mal intentionnée.
* On peut remarquer des procédés original afin de générer une clé aléatoirement. Ce site par exemple <https://walletgenerator.net/> créer la clé en prenant aléatoirement la position de la souris.

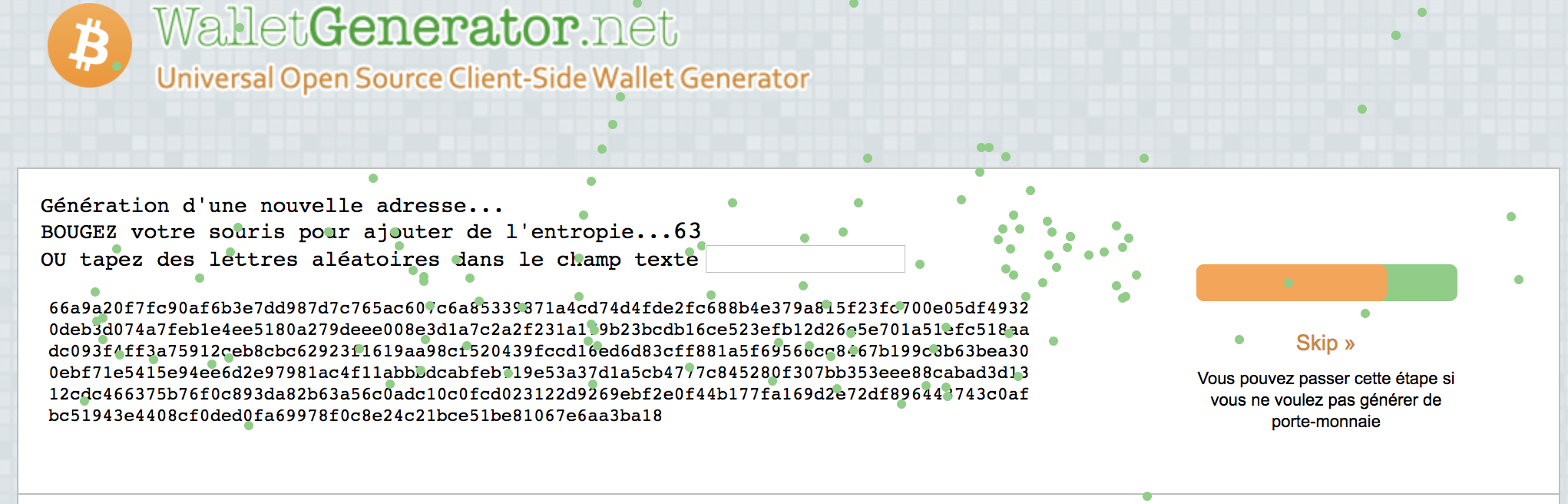


figure: génération d’un paper wallet

* La seed, ou en francais “graine” est un moyen mnémotechnique que l’on peut écrire sur un bout de papier afin de générer une clé privée à partir d’une série de 12 mots minimum.



figure: “seed” ou graine d’un wallet

* Le QRcode. On peut noter son utilisation accru dans les différents wallet. En effet il est aisé de générer un QRcode avec son adresse publique ainsi que le montant pour effectuer une transation.

sources: <https://www.acheter-bitcoin.info/portefeuille-bitcoin-wallet/> & <https://bitconseil.fr/wallets-bitcoin-altcoins/>

## 

## 

## 6.2 - Focus sur l’achat et le trading des crypto-monnaies

**ACHAT**

Le Bitcoin reste la monnaie centrale dans l’univers des crypto-monnaies . Afin d’acheter ou de trader une crypto-monnaie “alternative”, il sera surement nécessaire de passer par le Bitcoin. Voici des exemples non exhaustifs pour se procurer des Bitcoins.

**Vente d’un bien en échange de Bitcoin**. Cela peut être une bonne option étant donné qu’une fois la transaction effectuée, il n’est pas possible de revenir en arrière. Un gage de sécurité donc pour le vendeur.

|  |  |
| --- | --- |
| figure: localbitcoins | **Achat auprès directement à une personne**. Cela est possible nottament sur ce site <https://localbitcoins.com/fr/> qui est un peu “le bon coin” du bitcoin |

|  |  |
| --- | --- |
| **Achat sur une plateforme d’échange.**  Il est aisé de trouver les plateformes disponibles, il faut prendre en considération différent critères comme, Réputation, frais, méthodes de paiement, niveau de sécurité, taux de change. | figure: tableau compratif plateformes d’achat de Bticoin source: https://www.acheter-bitcoin.info/ |

**TRADING**

Il existe également de nombreuses plateformes comparables à ce que l’on peut trouver le trading en bourse. Sachez toutefois que c’est un marché extrêmement volatile.



figure: exemple de plateforme d’échange

Note: Attention toutefois, ces plateformes sont la cible préféré des hackeurs. Il est préférable de transférer par la suite la monnaie sur un portefeuille local.

source: <https://www.cryptos-monnaies.fr/acheter-bitcoin/>

## 

## 6.3 - Focus sur le minage

Dans le monde de la blockchain, le minage est un monde à part entière qui génère beaucoup d’argent. Les monnaies sujettent aux minages sont celles utilisant des algorithme POW (Proof Of Work). Cela prend une telle importance que l’on peut voir un effet sur le prix des GPU qui augmente ou des constructeurs qui développent des cartes mères dédiées au minage. (<https://www.developpez.com/actu/157311/Asus-devoile-une-carte-mere-dediee-au-minage-de-cryptomonnaies-qui-supporte-jusqu-a-19-GPU-compatible-avec-les-processeurs-Intel-KabyLake/>)

**Les mineurs**

Un mineur est rémunéré suivant le pourcentage de la puissance de calcul qu’il va finir dans le réseau.

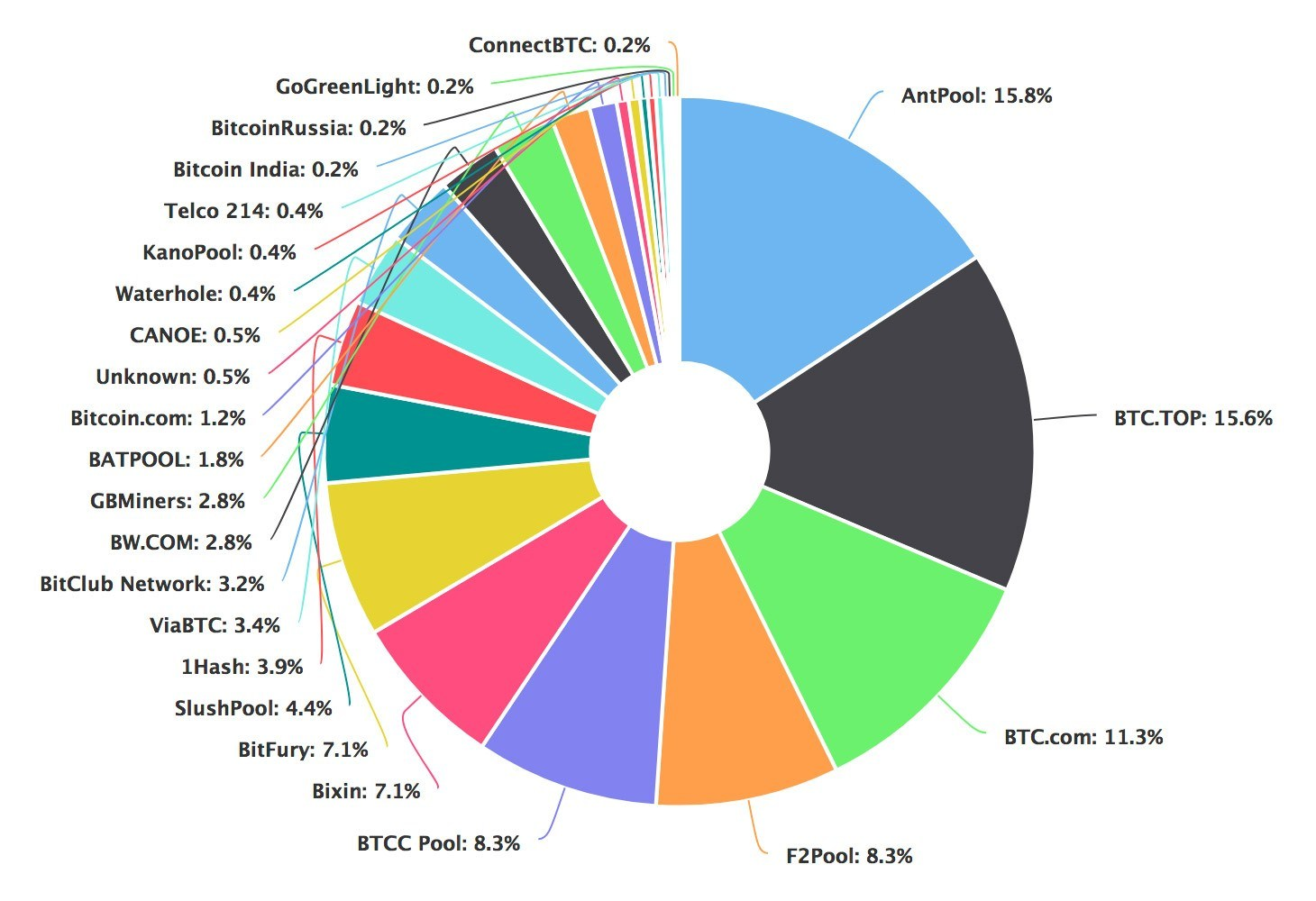
Dans cette activité lucrative, nous pouvons différencier différents type de mineur, l’amateur ou le “professionnel”, avec des installations pouvant prendre des proportions assez importantes.

Nous pourrons noter que des ascis ont été développés spécifiquement pour cette activité. Réduisant la consommation électrique et donnant des performances décuplées. (<https://www.bitmain.com>)

|  |  |  |
| --- | --- | --- |
| Un mining rig amateur | Un entrepôt mining rig en chine | Un asics dédié |

**Les pools de minage**

La rémunération dépend du nombres de blocs trouvés. Un mineur indépendant disposant d’une petite installation a peu de chance de trouver un bloc tout seul. C’est pourquoi il existe des pools de minage qui regroupe plusieurs mineurs indépendants. Statistiquement, il n’y pas de différence de rémunération entre un petit pool et un gros pool. Un petit pool trouvera des blocs moins souvent, mais la rémunération est plus élevé car votre pourcentage sera plus élevé. Inversement pour les gros pools.



**Minage dans le cloud**

Des société se sont également spécialisées afin de miner dans le “cloud” via un investissement de départ de votre part.

**Et la consommation électrique?**

**< EN COURS DE RÉDACTION> -> CONTROVERSE, certains chiffres seraient exagérés**

D’après cet article, en juillet 2017, les activités de minage du bitcoin et d’Ethereum réunit consomme plus de 19.23 Térawatts par heure, soit plus que la consommation de l’Islande.

La consommation moyenne d’une habitation francaise est de 6 937.86 kwh par an. La consommation de 19.23 Twh représente alors l’équivalent de 2 772 091 ménages!?

<http://www.clubic.com/antivirus-securite-informatique/cryptage-cryptographie/crypto-monnaie/actualite-833314-crypto-monnaie-minage-consomme-islande.html>

## 

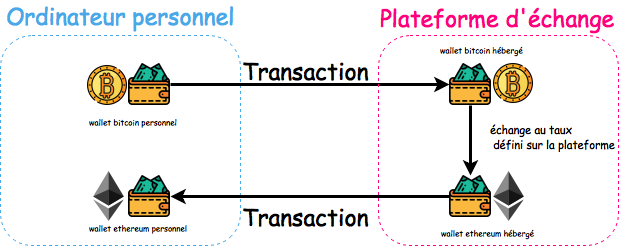
## 

## 6.4 - Focus sur les cas de hacking

Bien que la technologie de la blockchain en elle-même soit un système sécurisé et éprouvé, l’écosystème applicatif permettant d'interagir avec elle l’est moins. Voici quelques exemples **non exhaustifs** des cas de piratages intervenant à différents points d'interactions avec la blockchain.

**Les plateformes d’échanges**

Ce sont des cibles privilégiées. En effet, elles regroupent et stock plusieurs wallets en lignes pour permettre aux utilisateur d’échanger leur crypto-monnaie.

[](https://www.draw.io/#G0BxYwN-yW1kTbaEVMU3NhRVBBM2M)

Quelques exemples...

|  |  |  |  |
| --- | --- | --- | --- |
| **Année** | **Qui** | **Montant** | **Comment** |
| 2014 | Mt.Gox | 850 000 BTC | Cold wallet compromised/inside job |
| 2016 | Bitfinex ( | 119 756 BTC | User wallet |
| 2012 | Linode (web hosting) | 46 703 BTC | Inside job/8 bitcoin wallets were compromised |
| 2015 | Bitstamp | 19 000 BTC |  |
| 2014 | Polionex | 12.3% de la plateforme |  |

sources: <https://coins.newbium.com/post/655-the-10-biggest-bitcoin-hacks-in-history>

<https://www.coindesk.com/poloniex-loses-12-3-bitcoins-latest-bitcoin-exchange-hack/>

**ETHEREUM, les smarts contracts et DAO**

Quelques exemples de l’ETHER

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Année** | **Qui** | **Montant** | **Comment** | **Solution** |
| 2017 | Parity (start up dévelpant un smart contract) | 377 000 ETH | bug in a multi sign wallet wallet.sol |  |
|  |  |  |  |  |
|  |  |  |  |  |

sources: <http://uk.businessinsider.com/report-hackers-stole-32-million-in-ethereum-after-a-parity-breach-2017-7>

**ICO**

Pour rappel les ICO sont des “levées de fond” lors du lancement d’une nouvelle crypto-monnaie. En supportant un projet, vous pouvez obtenir un bonus immédiat entre 5% et 25% de votre investissement sur cette nouvelle crypto-monnaie. Les hackers remplacent simplement l’adresse d’envoi par une fausse adresse. Ceci permet de dérober les investissements effectués par les investisseurs. (dashcoin: 2000 investisserus on envoyés 37 000 ETH à une fausse adresse, source: <https://www.coindesk.com/coindash-ico-hacker-nets-additional-ether-theft-tops-10-million/>)

**Divers**

Il y a également eu des cas de piratage suite à une faille sur une hébergeur web. (exemple Linode en 2012, 46 703 BTC)

Bien sur il reste également le piratage “simple” de votre ordinateur personnel afin de récupérer votre clé privée.

**Que déduire de ces cas? Quelles peuvent être les parades?**

Tout d’abord, nous pouvons noter qu’il est important de bien se renseigner avant de se lancer dans l'aventure de la crypto-monnaie, et d’agir avec prudence.

Les plateforme d’échanges sont des points faibles et des cibles pour le hacking. C’est pour cela qu’a été introduite les notions de “cold wallet” et “hot wallet” (voir annexe… “Focus sur les wallets)

Pour ethereum, il faut développer avec la plus grande prudence les smarts contract .

De plus, il est recommandé d’utiliser des logiciels open sources, permettant de vérifier qu’il n’y est pas de backdoor.

## 

## 

## 6.4 - REX: participation à une conférence midi minatec

**" QUAND L'ÉCONOMIE DU PARTAGE, LE DIGITAL ET LA FINANCE S'INVITENT DANS LE SECTEUR DE L'ÉNERGIE"**

Intervenante: Anne-Lorène VERNAY - Professeure assistante à GEM

Lieu: Grenoble

Date: 13/10/2017

Cette conférence tomba à pic. Elle a permis d’enrichir notre recherche sur les cas d’utilisations de la blockchain dans le secteur de l’énergie.

La production d’énergie est actuellement un modèle hypercentralisé. Des grandes compagnies produisent et offrent peu d’interactions avec le consommateur qui se retrouve perdu et peu intéressé. Des start-up proposent de nouveaux “business models” afin d’impliquer le consommateur dans cette production d’énergie.

C’est en Hollande et en Allemagne que l’interlocutrice a choisi 5 exemples afin de nous exposer les futures solutions:

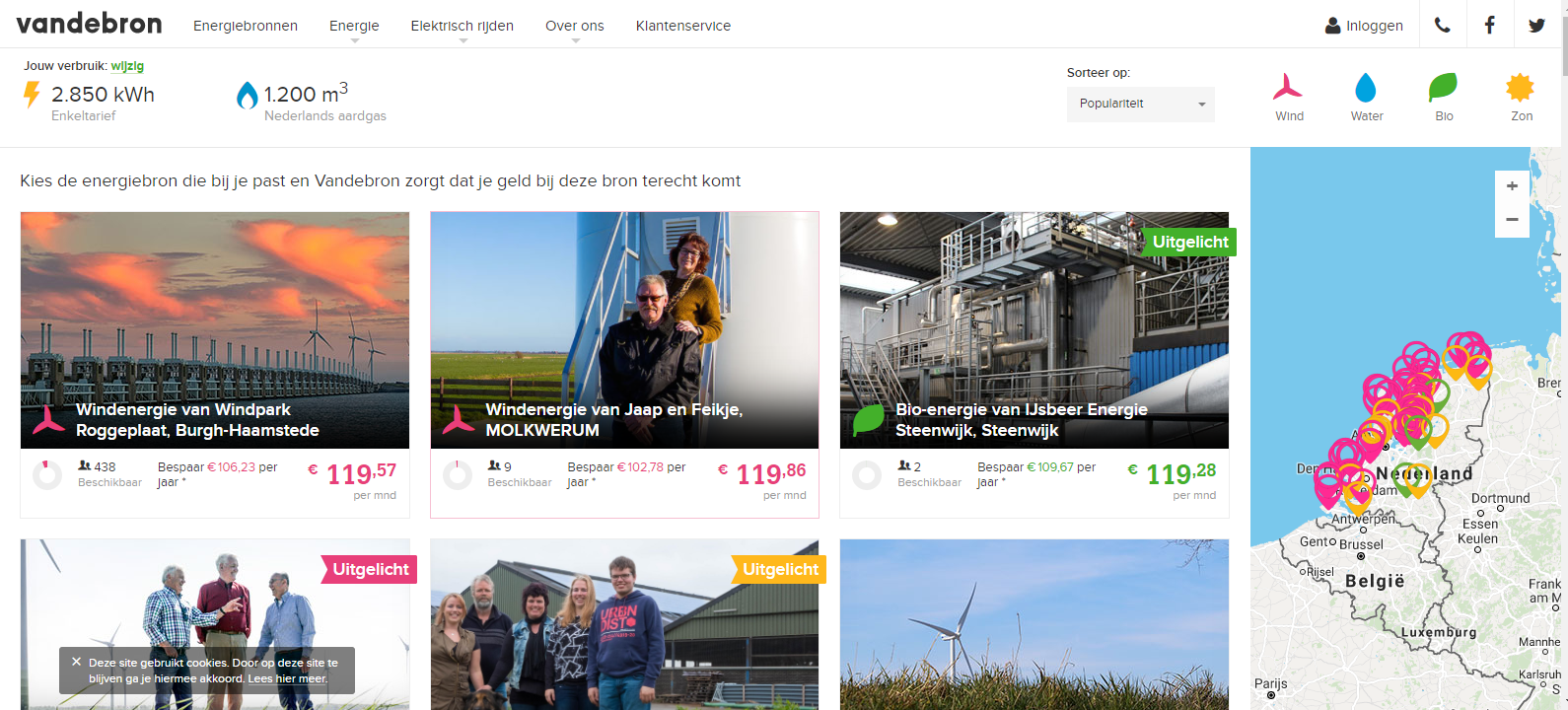
**Windcentrale :** Entreprise néerlandaise proposant d'acheter les parts d’une éolienne. La participation s’élève à environ 250€ pour une part. Une réelle coopérative est créée autour de l'éolienne à laquelle l'acheteur participe. La coopérative négocie la distribution d’énergie directement avec les fournisseurs.

Une application est disponible pour vérifier la conso de son éolienne et d’autres paramètres.

https://www.windcentrale.nl/

**Vandebron** Plateforme qui permet de “colorer” l'électron en mettant un nom et une personne derrière son achat d’électricité. Il est possible de choisir en ligne à quel producteur nous achetons directement notre électricité.

<https://vandebron.nl/>



**Powerpeers :** Place de marché permettant d’acheter et de vendre de l'électricité entre particuliers. Un algo calcule combien on produit et combien on a consommé. Utilisation d’une crypto monnaie nommée “**solarcoins**”.

https://www.powerpeers.nl/

**Beegy :** Box murale reliée à des panneaux solaires et/ou une batterie Tesla. Gère et donne des conseils au particulier pour économiser près de 50% de son électricité. Mise en lien de tous les possesseurs de Beegy afin que chacun puisse s’échanger et consommer de l'électricité 100% Beegy.

http://www.beegy.com/

**Jedlix**: Application permettant de gérer la recharge de sa voiture en vendant l'électricité de la batterie lorsque nous n’en avons pas besoin.

https://jedlix.com/

**Divers**:

* Modèle Enercoop (France) qui est une scope et qui met en place des panneaux solaires sur les toits des collectivités etc… Cela permet d’acheter de l'électricité verte.
* Problèmes liés à la stabilité du réseau. En effet, les énergie vertes sont difficiles à gérer sur le réseau. Qui sera garant de cette stabilité? Les auto-producteurs devront-ils payer un abonnement conséquent pour utiliser ce réseau?

**Conclusion**

Tous les exemples évoqués mettent en oeuvre des transactions financières. Il n’y a pas d’échange d'électrons… le modèle se cherche encore. L’Allemagne qui était partie sur un modèle 100% autonome en se passant du réseau est actuellement en train de faire marche arrière.

Au final l’interlocutrice n’a que peu évoqué la blockchain. Elle a par contre mis en avant que c’est grâce à ces nouvelles technologies que les applications de demain vont pouvoir exister.

<https://en.bitcoin.it/wiki/Secp256k1>

# Références

Pour un site:

[X] auteur, “nom”, [Online]. Disponible: <http://www.domain.name/page/web>.

Pour livre/document:

[X] auteur, *titre*, universite/entreprise/institut, année.

[1] Blog Developpez, “Hachage n’est pas cryptage” [Online]. Disponible: <https://blog.developpez.com/sqlpro/p12496/langage-sql-norme/hachage-nest-pas-cryptage-de-la-securite-des-donnees-chiffrees-dans-les-sgbdr>

[2] Satoshi Nakamoto, *“Bitcoin: A Peer-to-Peer Electronic Cash System”*, <https://bitcoin.org/bitcoin.pdf>, 2008.

[3]