Arrigo Jordan
Carbonnier Mathieu

La Cryptomonnaie

I - La Cryptomonnaie :

1-) Introduction :

Actuellement pour pouvoir donner de l'argent à quelqu'un, on est obligé de passer par un "tiers de confiance" qui réalise la transaction (banque…). Cela représente plusieurs inconvénients :

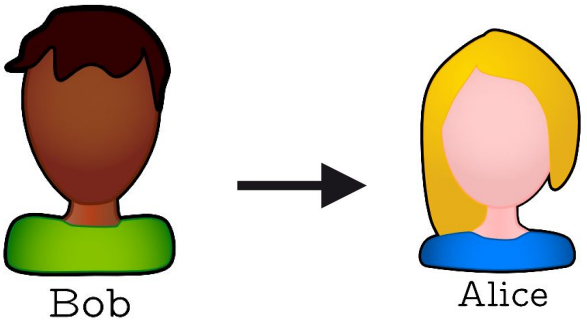
- Ce service tiers ne fait rien gratuitement, nous avons donc une dépense supplémentaire.
- Nous avons très bien vu la crise financière de 2007-2008, où le service tiers peut à n'importe qu'elle moment partir avec notre argent.

Exemple de transfert :

Banque

Mais en 2008, un développeur du nom de Satoshi Nakamoto développe un moyen de paiement électronique entièrement décentralisé.
Le 9 janvier 2009, Satoshi annonce le lancement du Bitcoin sur SourceForge.

Exemple de transfert avec cryptomonnaie :



Grâce à la cryptomonnaie, on peut envoyer directement de l'argent sans passer par un tier de confiance.

2-) Caractéristiques de la cryptomonnaie :

Personne ne contrôle la cryptomonnaie, puisque le transfert n'utilise aucun tiers de confiance. C'est vous qui gérez vos portefeuilles (on peut comparer ça à un compte bancaire) et donc votre agent. La cryptomonnaie, est donc entièrement décentralisé, c'est un transfert peer-to-peer, personne ne la contrôle.

L'anonymat est aussi une caractéristique de la cryptomonnaie. Etant donné que seules vos adresses de portefeuille sont visible et hashé. Si vous ne divulguez pas l'information que l'adresse vous est associé, alors votre anonymat sera conservé.

II - Clé privée ,clé public et adresse :

1-) Clé privée :

Une clé privée est un code alphanumérique et crypté donnant accès à vos fonds en cryptomonnaie.
Il s'agit de la seule manière de prouver que vous en êtes le propriétaire.
Les clés privées sont usuellement représentées en base 58 sous la forme d'une chaîne de caractères.
Elles commencent toujours par un 5, un K ou un L.
Exemple d'une clé privée :

```
Kzczf8E4oq8MLakhRS479gpZpSe2e6u2xErKHQNqpeFMPEK4irtc
```

La clé privée est calculé à partir d'un algorithme de cryptographie asymétrique appelé ECDSA(*Elliptic Curve Digital Signature Algorithm*) que l'on détaille dans la partie :
"Pair Clé Privée/Public".

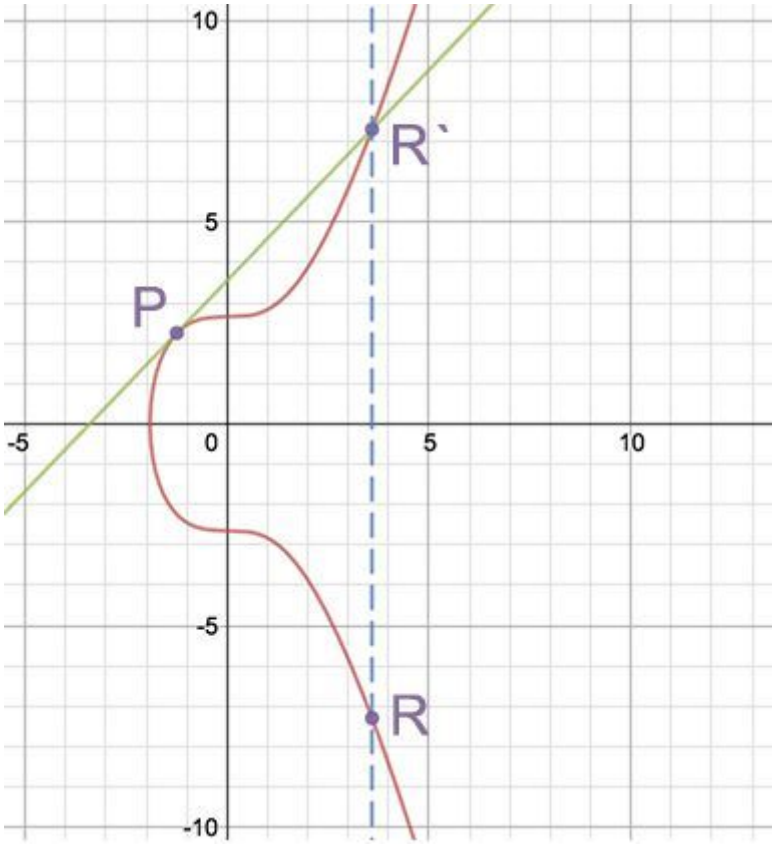
2-) Clé public :

Une clé publique va toujours de paire avec une clé privée.
Dans le cas de Bitcoin, la clé publique est calculée à partir de la clé privée et elle aussi de l'algorithme de cryptographie asymétrique ECDSA.
Cette opération se fait à sens unique, de sorte qu'il est impossible de retrouver la clé privée à l'aide de la publique.
La clé publique est un élément qui sert d'adresse sur une blockchain.
Elles sont usuellement représentées sous forme hexadécimale.
Par exemple, la clé publique associée à la clé privée donnée plus haut est :

```
02f5e25778dcee9539b25799831277eb8e731ffcbdcd9e68f79f8ca43c570b94ba
```

3-) Pair Clé Privé/Public :

Comme dit plus haut, les clés sont calculé à partir d'ECDSA.
L'opération est réalisée à l'aide de la courbe elliptique secp256k1 représentée ci-dessous :



- La clé privée est le nombre de fois qu'il faut multiplier le générateur de la courbe elliptique pour avoir la clé publique.
- La clé publique est un point sur une courbe elliptique qui correspond à la clé privée.

La paire clé privée / clé publique intervient dans la signature des transactions. L'utilisateur signe sa transaction avec sa clé privée et les autres acteurs du réseau vérifient cette signature à l'aide de la clé publique.
Si la clé publique correspond à la signature, la transaction est validée et ajoutée à la chaîne de blocs.
Sinon elle est refusée par le réseau.
Dans ce processus, la clé privée n'est donc pas dévoilée et seule la clé publique est connue de tous, d'où son nom de clé « publique ».

4-) Adresse :

Tout comme la clé privée, l'adresse est usuellement représentée à l'aide de la base 58 sous-forme de chaîne de caractères.
Elle commence toujours par un 1.
L'adresse correspondant à notre exemple paire de clés ci-dessus est :

`1KMnRF6NbRnLg8KkqBGorSyLGM14BVR2LS`

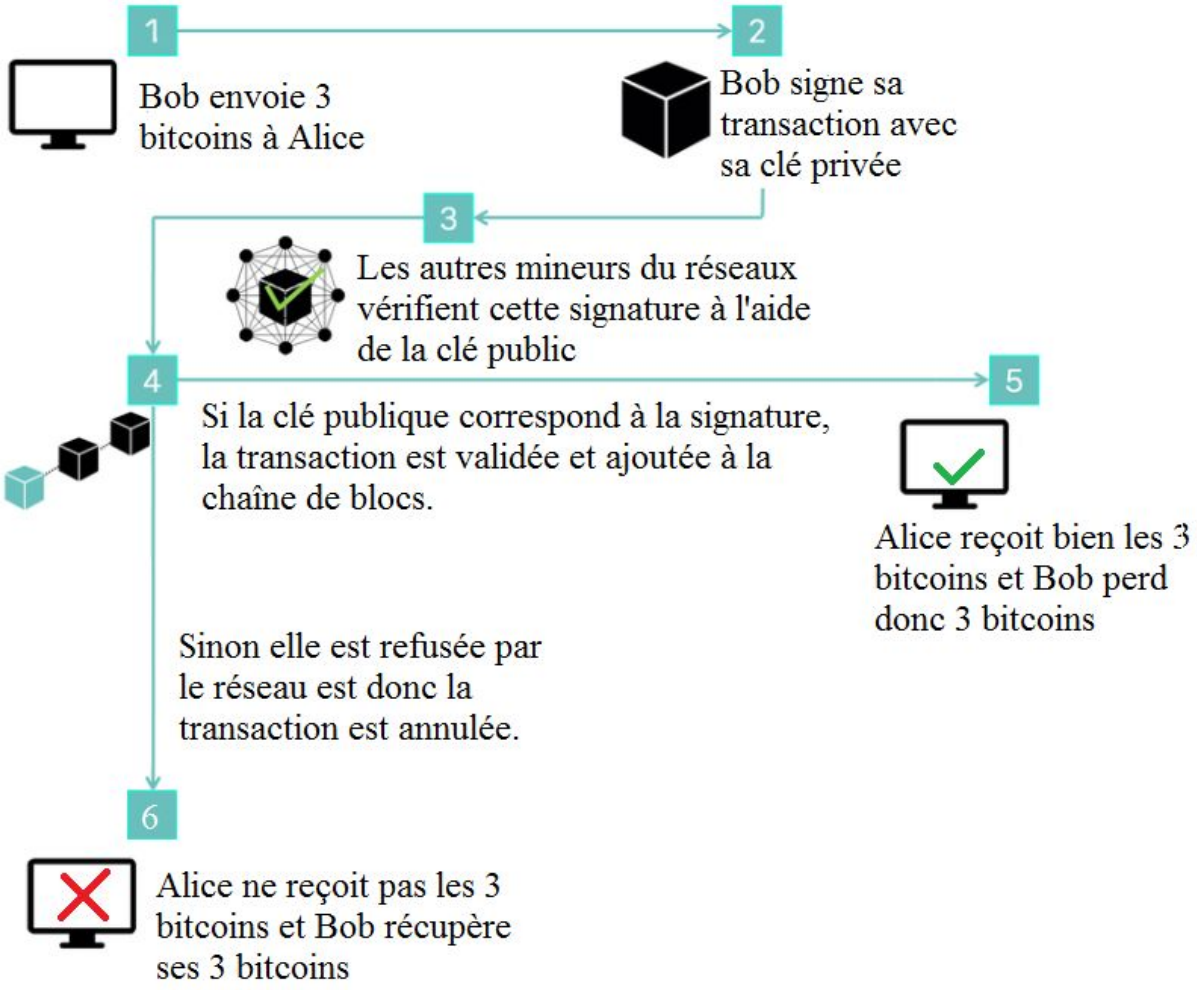
Une adresse est en quelque sorte un compte appartenant à un utilisateur dont il se sert pour :

- conserver ;
- recevoir ;
- échanger ses cryptomonnaies.

5-) Comment obtenir l'adresse :

Une adresse est calculée à partir de la clé publique à l'aide de fonctions de hachage.
La clé publique est d'abord hachée par la fonction SHA-256, puis le résultat est haché par la fonction RIPEMD-160.
Les deux fonctions de hachage sont des fonctions irréversibles et il est donc impossible de retrouver la clé publique à partir de l'adresse.
Ainsi, l'adresse est calculée à partir de la clé publique, qui est elle-même calculée à partir de la clé privée.
Ces opérations sont à sens unique, si bien que personne ne peut retrouver votre clé privée (ni même votre clé publique si vous n'avez pas réalisé de transaction) à partir de votre adresse !

III - Validation des transactions dans la blockchaine :



IV - Conclusion :

V - Référence :

Voici les références que l'on a utilisées :

- https://cryptoast.fr/cles-privees-cles-publiques-et-adresses-dans-bitcoin/
- https://bitcoin.fr/qu-est-ce-qui-relie-la-cle-publique-a-la-cle-privee/
- https://blockgeeks.com/guides/fr/quest-ce-que-la-crypto-monnaie/
- https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/