**Transaction en crypto-monnaie vs standard**

**Illustration paiement standard**

Etapes

1. Transfert au vendeur

Parties concernées

* Acheteur
* Banque acheteur (A)
* Banque vendeur (V)
* Vendeur

*Etape 1*

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Actifs** | **Passifs** | **Rôle** |
| Acheteur A | - 50 |  | Ordre de pmt à banque A |
| Banque A | - 50 | - 50  *+ 50* | Débit compte A  Virement à banque V (cptes BNS)  *Virement à banque correspondant, pour le compte de banque V\** |
| *Correspondant US (banque)\** | *+ 50*  *- 50* |  | *Si pmt via bque correspondante, p.ex. virement en USD* |
| Banque V | + 50 | *- 50*  + 50 | Virement de banque A (cptes BNS)  *Virement reçu sur banque correspondant\**  Crédit compte de V |
| Vendeur V | + 50 |  | - |

*\* Cas avec pmt via banque correspondante (ex. pmt US)*

*Hypothèse : correspondant US créancier envers banque A et banque B (avant et après pmt)*

Fondamentalement : échange de créances sur des banques

**Illustration paiement crypto-monnaie (illustration bitcoin)**

Etapes

1. Achat cryptomonnaie via compte bancaire
2. Transfert au vendeur

Parties concernées

* Acheteur (également acheteur crypto)
* Banque acheteur (A)
* Banque vendeur crypto (V)
* Vendeur crypto
* *Intermédiaire crypto (Wallet)*
* *Blockchain*
* *Mineurs*
* Vendeur

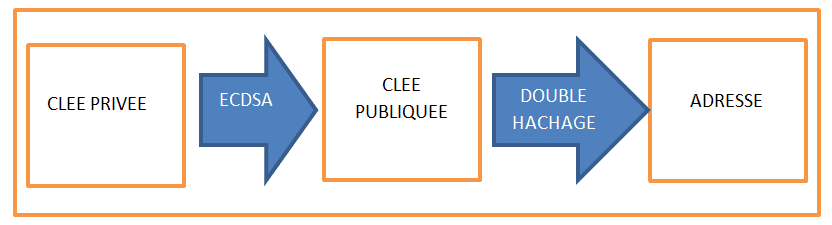
Identification

* + clé publique (*~ no de compte = adresse[[1]](#footnote-2)*) => historique de toutes les transactions (apparaît dans blockchain)
  + clé privée (*~ mot de passe = signature transaction*) => permet identification pour exécuter transaction

Lien clé privée – clé publique – adresse $crypto

* clé publique : version hashée de la clé privée
* adresse $crypto : version hashée de la clé publique

A VOIR DE PLUS PRES



*Etape 1 : achat cryptomonnaie*

Préliminaire : création *wallet* bitcoin = 3 fonctions

* conservation clés privées
* création clés publiques
* lien avec réseau (blockchain)

Types de *wallet[[2]](#footnote-3)* :

* online (*hot storage* : clés privées et publiques stockées sur le site d’un prestataire de service)
* installation logiciel sur PC (*cold storage*, sauvegarde clés privées peut être faite sur des clés USB sécurisées)
* Hierarchical Deterministic (HD) wallet : génération de clés publiques aléatoirement à partir de clé publique principale et seed fixé … pour plus tard…

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Actifs** | **Passifs** | **Rôle** |
| **Partie monnaie standard** | | | |
| Acheteur A | - 50 |  | Ordre de pmt à banque A |
| Banque A |  | - 50  + 50 | Débit compte A  Virement à banque V (via cptes correspondant US) |
| Banque V |  | - 50  + 50 | Virement de banque A (via cptes correspondant US)  Crédit compte de Vendeur crypto |
| Vendeur crypto | + 50 |  | Réception pmt |
| *Intermédiaire crypto (wallet)* | *-* | *-* | *Rôles ?*   * *Gestion coordonnées bancaires**?* * *Validation que pmt reçu pour envoyer transaction crypto ?* |
| **Partie crypto** | | | |
| Vendeur crypto | - $Crypto |  | Transfert crypto |
| *Intermédiaire crypto (wallet)* | *-* | *-* | *Rôles :*   * *Conservation clés* * *Accès blockchain, transmission infos transaction crypto-monnaie* |
| *Blockchain* |  |  | *Rôles :*   * *Conservation historique transactions* * *Réseau vérifie*   *1) validité transaction (clé privée <> clé publique)*  *2) disponibilité des $Crypto (selon clé publique)*   * *Stocké où ? Distribué => chez qui ? Qui participe ?* |
| *Mineurs* |  |  | *Rôles :*   * *Participants à blockchain* * *Stockage ledger distribué ?* * *Validation des transactions ?* * *Constitution de blocs, vérification bloc => intégration dans blockchain* |
| Acheteur A | + $Crypto |  | Réception crypto |
| Questions |  |  | Questions :   * Rôle mineurs ? * **Crypto = créances envers qui ? Nature de la monnaie ?** * Provenance $Crypto : actifs intermédiaires , autres détenteurs de $Crypto, nouvelle émission ? * Blockchain ? * ProofOfWork, ProofOfStake ? * **Quel lien entre pmt en USD et transfert crypto ? Intermédiaire pour synchroniser ?** |

*Etape 2*

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Actifs** | **Passifs** | **Rôle** |
| Acheteur A | - $Crypto |  | Achat vs paiement en crypto |
| *Intermédiaire crypto (wallet)* | *-* | *-* | *Rôles :*   * *Conservation clés* * *Accès blockchain, transmission infos transaction crypto-monnaie* |
| *Blockchain* |  |  | *Rôles :*   * *Conservation historique transactions* * *Réseau vérifie*   *1) validité transaction (clé privée <> clé publique)*  *2) disponibilité des $Crypto (selon clé publique)*   * *Stocké où ? Distribué => chez qui ? Qui participe ?* |
| *Mineurs* |  |  | *Rôles :*   * *Participants à blockchain* * *Stockage ledger distribué ?* * *Validation des transactions ?* * *Constitution de blocs, vérification bloc => intégration dans blockchain* |
| Vendeur V | + $Crypto |  | Vente vs paiement en crypto |

Qq notions :

* algorithme de hashage

Liens divers :

* Transactions crypto

<https://www.blockchains-expert.com/portefeuille-bitcoin-comment-conserver-vos-cryptomonnaies/>

<https://www.blockchains-expert.com/4-etapes-pour-comprendre-une-transaction-bitcoin/>

https://en.bitcoin.it/wiki/Main\_Page

<https://pouruneautreeconomie.fr/comment-fonctionne-transaction-bitcoin/>

<https://www.les-crises.fr/approfondir-le-bitcoin-deroulement-dune-transaction-23/>

* Clé privée / publique

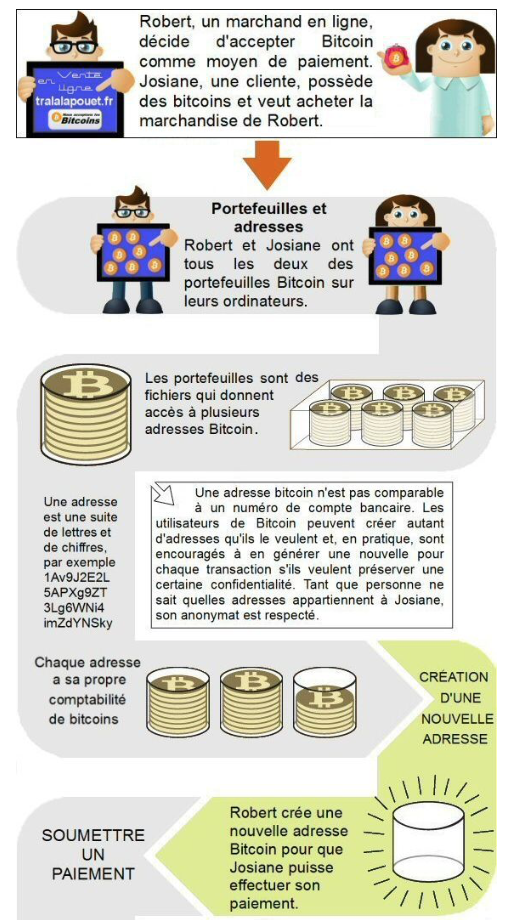
[https://medium.com/@JB\_Pleynet/le-chiffrage-%C3%A0-cl%C3%A9s-publiques-priv%C3%A9s-expliqu%C3%A9-aux-non-initi%C3%A9s-1a0eed15934f](https://medium.com/@JB_Pleynet/le-chiffrage-à-clés-publiques-privés-expliqué-aux-non-initiés-1a0eed15934f)

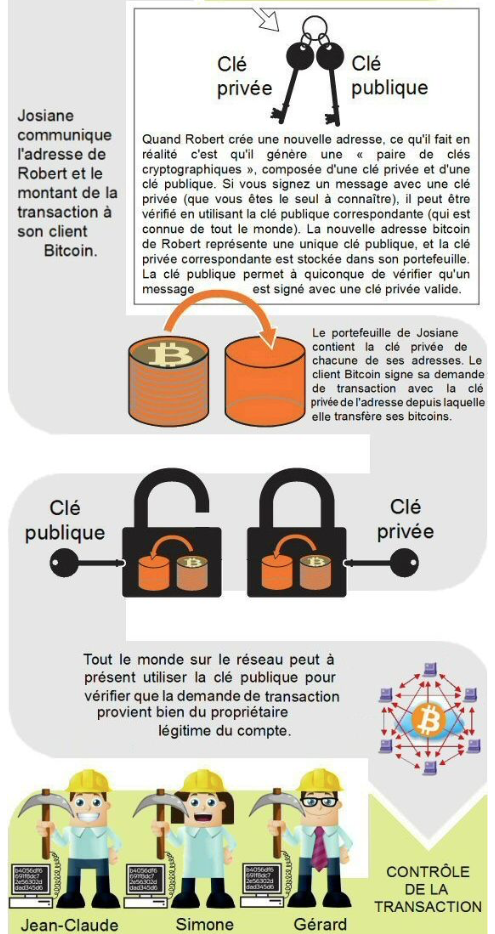
* Licences bancaires

<https://www.bilan.ch/finance/la-finma-elargit-la-voie-a-la-crypto-avec-deux-licences-bancaires>

[https://www.allnews.ch/content/r%C3%A9glementation/fintech-le-conseil-f%C3%A9d%C3%A9ral-concr%C3%A9tise-la-licence-bancaire-%C2%ABlight%C2%BB](https://www.allnews.ch/content/réglementation/fintech-le-conseil-fédéral-concrétise-la-licence-bancaire-)

* Divers





1. Différence fondamentale : une nouvelle adresse peut être créée pour chaque nouvelle transactions (conseillé !) [↑](#footnote-ref-2)
2. NB : wallet cryptée ! accès via mot de passe [↑](#footnote-ref-3)