# Fondamentaux de la blockchain

Éric BERTHOMIER
eric.berthomier@free.fr

20 mars 2022

Version 1.2 - Version Stagiaire

Ce cours est une adaptation libre de la page web :

# Building a Minimal Blockchain in Python

## Understanding blockchain by coding

# BlockChain : Idées reçues

- Utilisée uniquement pour les Bitcoins ou autres cryptomonnaies.

# BlockChain : Idées reçues

- Utilisée uniquement pour les Bitcoins ou autres cryptomonnaies.
- Utilisée comme une base de données.

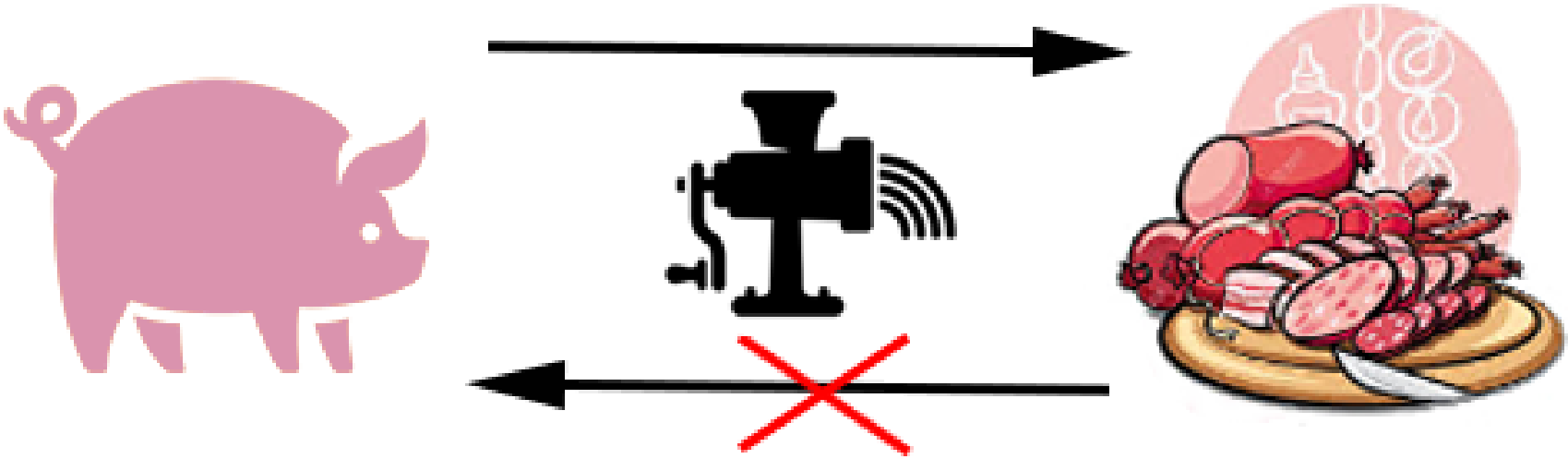
# BlockChain : Idées reçues

- Utilisée uniquement pour les Bitcoins ou autres cryptomonnaies.
- Utilisée comme une base de données.
- Liée à un chiffrement des données.

# BlockChain : Idées reçues

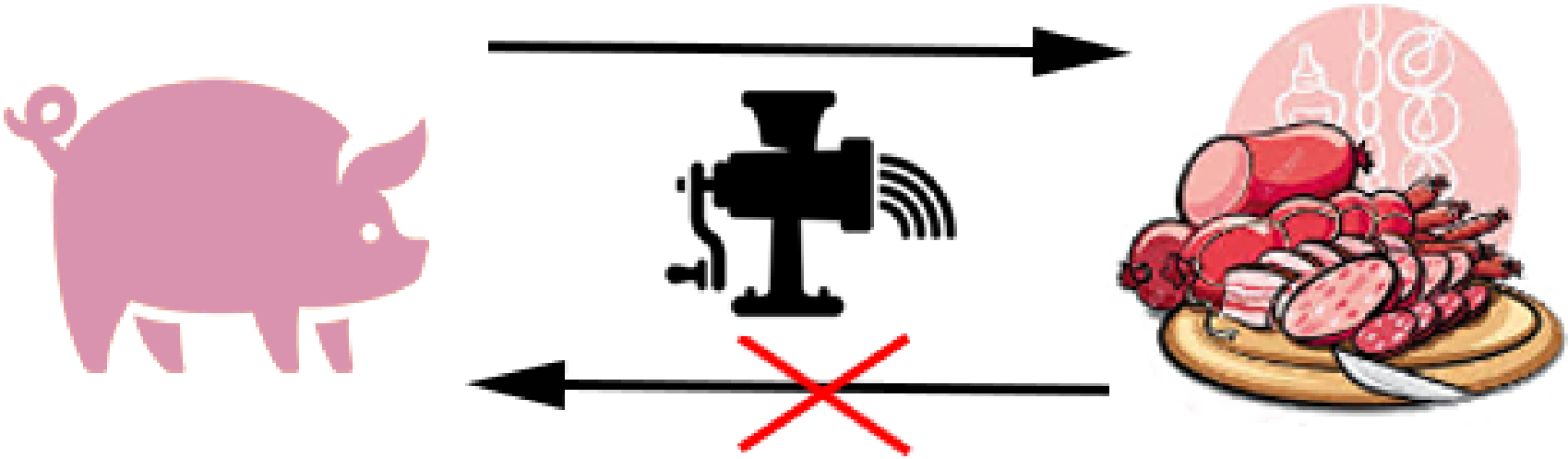
- Utilisée uniquement pour les Bitcoins ou autres cryptomonnaies.
- Utilisée comme une base de données.
- Liée à un chiffrement des données.
- Transparence des données.

# Notion informatique : le hashage



À une donnée entrée ne correspond qu'une seule et unique donnée en sortie.

# Notion informatique : le hashage



À une donnée entrée ne correspond qu'une seule et unique donnée en sortie.
Il est impossible de partir du haché pour revenir à la source.

# Exemple d'utilisation

| | |
|---|---|
| Buzz Lightyear | 2d22f600ae506961d2d8499bdec964385781bb0d79e40d4626fac232ed0bd792 |
| Rex the T-Rex | 070ed46f35be29ffd4578453f50fc9997b6b1e78b2fc9664ee6b9a415d032364 |
| Bo the Peep | 7a6aa8bbdb0f6094355397d68f67b197752c633cdfe4406ca7d52af2a88fa0e5 |
| Hamm the pig | 4bc7d8a4889c951c207988757e9a599bde8b8e3df13d0606d9c3622372a6975e |

# Notion informatique : Horodatage

Chaque élément de la block-chain contient un champs d'horodatage afin de pouvoir estampillé chaque action.

exemplehorodatage.txt

```
2022-03-12 19:33:19.927564
```

# Autres éléments d'un maillon de chaîne

Nous disposons maintenant de quelques éléments pour construire notre premier maillon de chaîne :

- Un hash
- Un horodatage

# Autres éléments d'un maillon de chaîne

Nous disposons maintenant de quelques éléments pour construire notre premier maillon de chaîne :

- Un hash
- Un horodatage

Nous allons pouvoir ajouter ce qui nous intéresse : la data

- Une donnée

# Autres éléments d'un maillon de chaîne

Nous disposons maintenant de quelques éléments pour construire notre premier maillon de chaîne :

- Un hash
- Un horodatage

Nous allons pouvoir ajouter ce qui nous intéresse : la data

- Une donnée

Et enfin lier les maillons entre eux par 3 éléments :

- Un contrôle du maillon précédent : son hash
- Un index pour connaître le numéro du maillon
- La chaîne : un tableau dynamique de maillons

# Structure d'un maillon

| | |
|---|---|
| index | Numéro de maillon / de transaction |
| timestamp | Horodatage |
| data | Données |
| previous_hash | Le hash du précédent maillon |
| hash | Le hash du maillon actuel |


Schématisation d'une blockchain

# Contrôle interne d'une BlockChain

- Les index doivent être croissants

# Contrôle interne d'une BlockChain

- Les index doivent être croissants
- Le hash du maillon précédent doit bien être égal au previous_hash du maillon actuel

# Contrôle interne d'une BlockChain

- Les index doivent être croissants
- Le hash du maillon précédent doit bien être égal au previous_hash du maillon actuel
- Le hash du maillon actuel doit bien être égal au hash enregistré dans ledit maillon

# Contrôle interne d'une BlockChain

- Les index doivent être croissants
- Le hash du maillon précédent doit bien être égal au previous_hash du maillon actuel
- Le hash du maillon actuel doit bien être égal au hash enregistré dans ledit maillon
- Les maillons doivent avoir un ordre chronologique dans leurs horodatages

# Pourquoi tous ces contrôles ?

- Un disque dur quelque soit sa technologie n'est pas inusable et certains éléments peuvent être détruits du fait de l'usure du disque. On parle de secteurs défectueux.

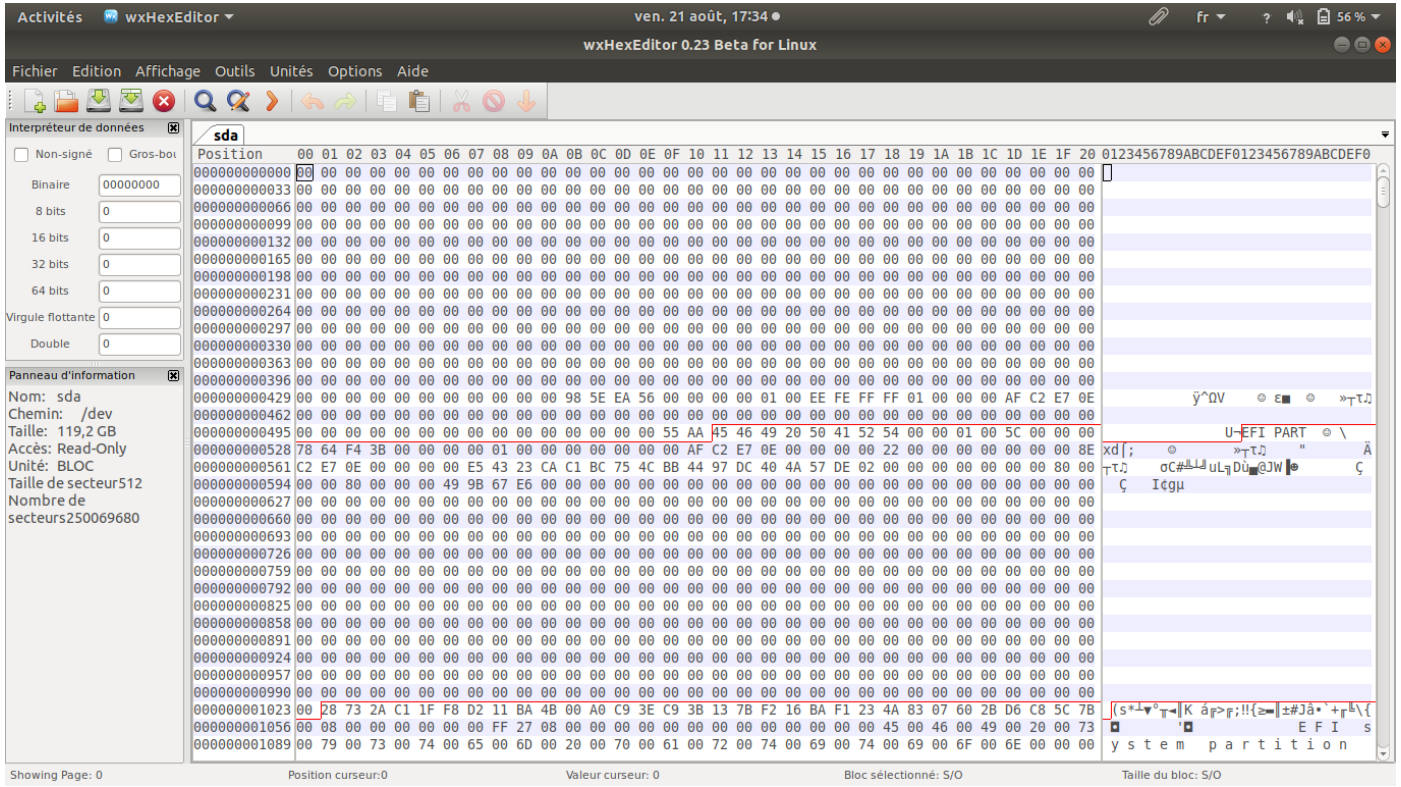
# Pourquoi tous ces contrôles ?

- Un disque dur quelque soit sa technologie n'est pas inusable et certains éléments peuvent être détruits du fait de l'usure du disque. On parle de secteurs défectueux.
- Volonté de nuire. Il pourrait être intéressant de modifier le contenu d'un maillon pour effacer une information ou la modifier.

# Pourquoi tous ces contrôles ?

- Un disque dur quelque soit sa technologie n'est pas inusable et certains éléments peuvent être détruits du fait de l'usure du disque. On parle de secteurs défectueux.
- Volonté de nuire. Il pourrait être intéressant de modifier le contenu d'un maillon pour effacer une information ou la modifier.
- L'horodatage permet d'établir une chronologie des actions effectuées sur la chaîne et ainsi permet une traçabilité de ces actions.

# Démonstration - Visuel d'un disque dur




```
sudo wxHeditor /dev/sda
```

# Notions SSI

Quelles seraient les actions à réaliser pour modifier la donnée contenue dans un maillon ?

- Sur le maillon lui-même :

# Notions SSI

Quelles seraient les actions à réaliser pour modifier la donnée contenue dans un maillon ?

- Sur le maillon lui-même :
  - la donnée

# Notions SSI

Quelles seraient les actions à réaliser pour modifier la donnée contenue dans un maillon ?

- Sur le maillon lui-même :
  - la donnée
  - le hash

# Notions SSI

Quelles seraient les actions à réaliser pour modifier la donnée contenue dans un maillon ?

- Sur le maillon lui-même :
  - la donnée
  - le hash
- Sur le maillon suivant :

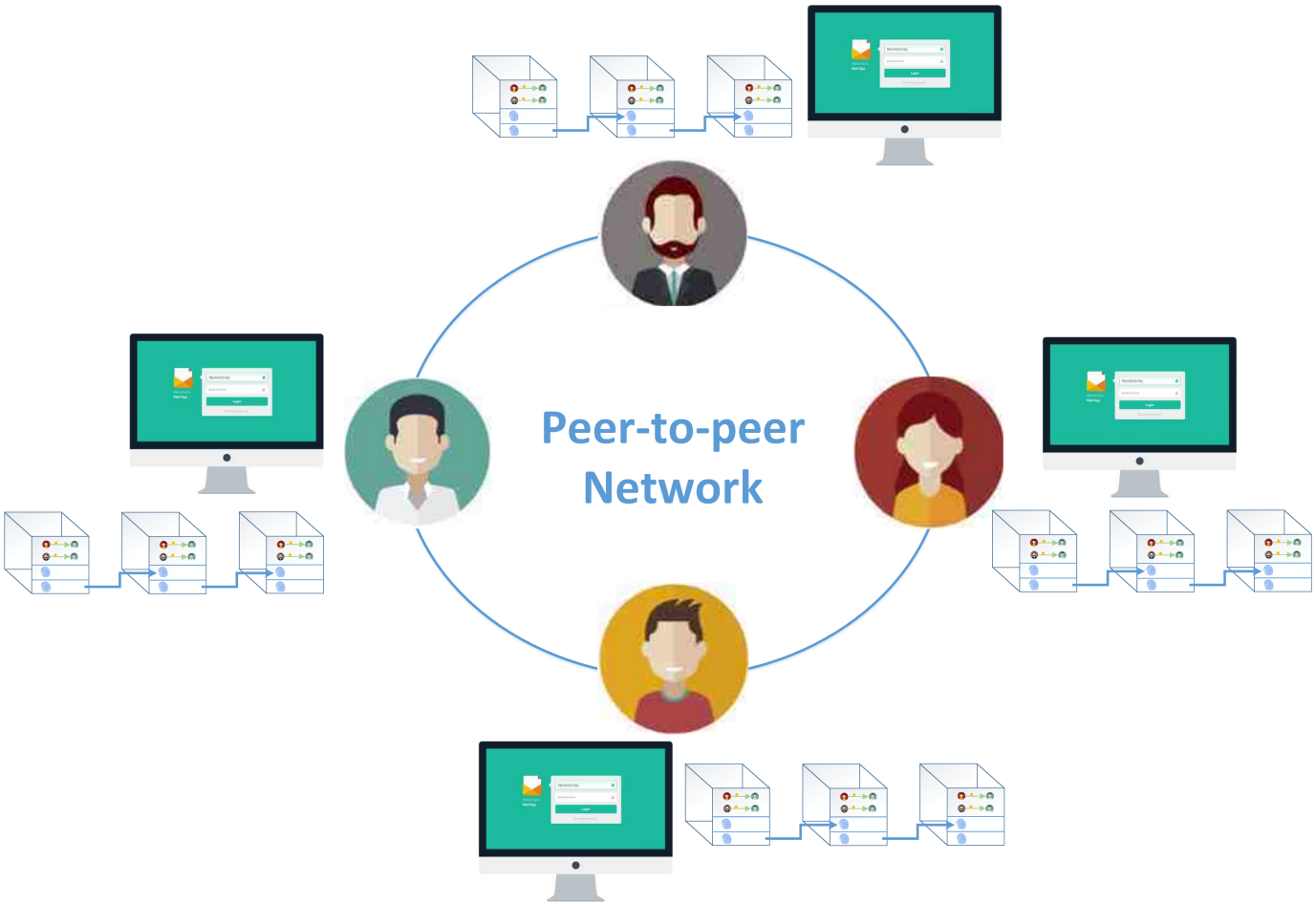
# Notions SSI

Quelles seraient les actions à réaliser pour modifier la donnée contenue dans un maillon ?

- Sur le maillon lui-même :
  - la donnée
  - le hash
- Sur le maillon suivant :
  - le previous_hash

# Un réseau partagé

La blockchain est définie au travers d'un réseau partagé.
Chacun possède en fait une copie de la blockchain.




# L'ajout d'un élément : une décision partagée

Chacun recevant l'ensemble des ordres sur la blockchain il est nécessaire de créer des règles pour valider l'ajout d'un block dans la blockchain.
On en distingue principalement deux :

La preuve de travail (Proof-of-work (PoW)) : Moyennant rémunération pour les meilleurs, les mineurs doivent résoudre un challenge informatique pour indiquer leur validation de la demande.

# L'ajout d'un élément : une décision partagée

Chacun recevant l'ensemble des ordres sur la blockchain il est nécessaire de créer des règles pour valider l'ajout d'un block dans la blockchain.
On en distingue principalement deux :

La preuve de travail (Proof-of-work (PoW)) : Moyennant rémunération pour les meilleurs, les mineurs doivent résoudre un challenge informatique pour indiquer leur validation de la demande.

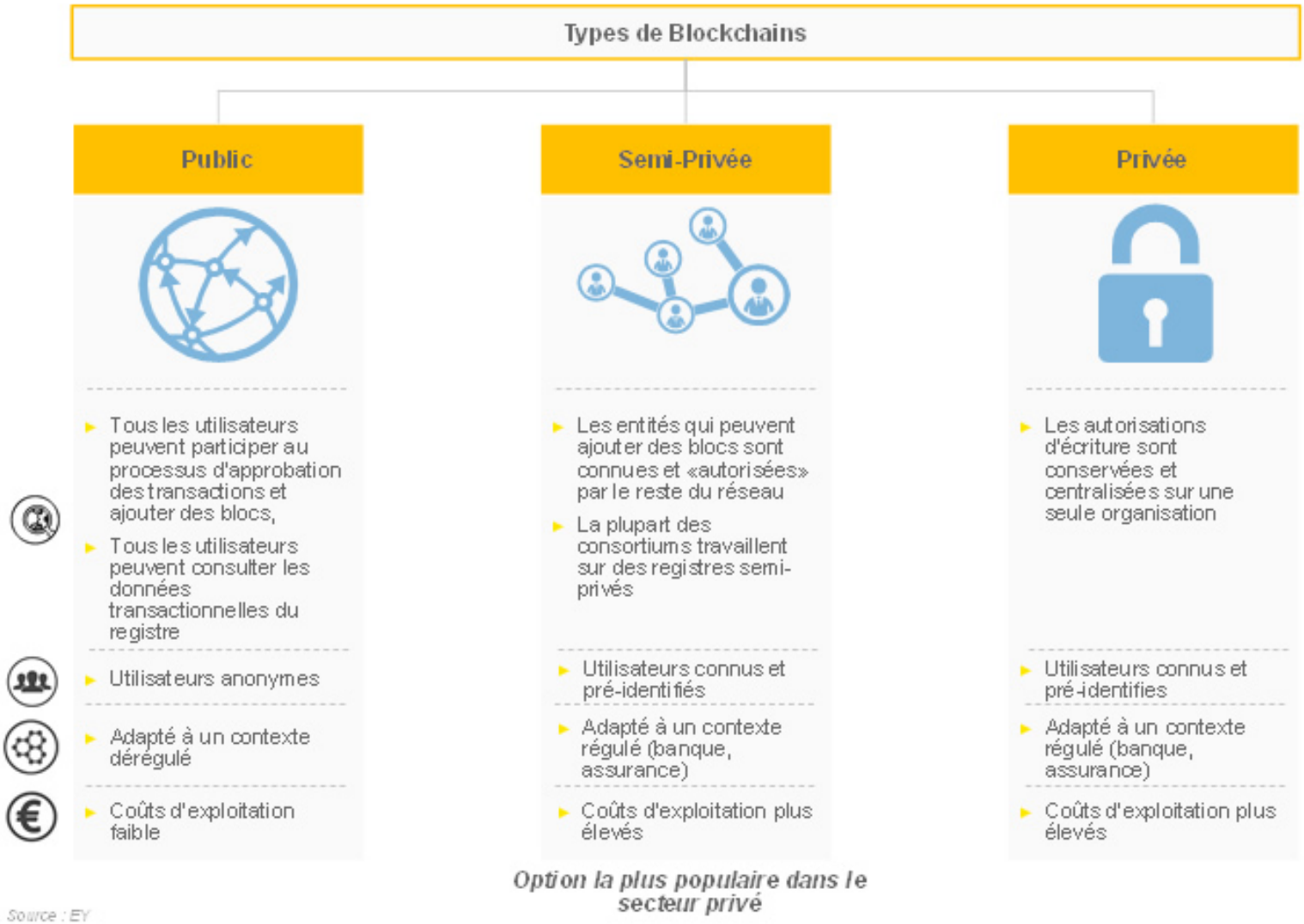
La preuve d'enjeu (Proof-of-stake (PoS)) : La preuve d'enjeu demande à l'utilisateur de prouver la possession d'une certaine quantité de jetons (leur " participation ") pour prétendre à pouvoir valider des blocs supplémentaires dans la chaîne de bloc et de pouvoir toucher la récompense, s'il y en a une, à l'addition de ces blocs.

# L'ajout d'un élément : une décision partagée

| PROOF OF WORK | PROOF OF STAKE |
| --- | --- |
|  The probability of mining a block is determined by how much computational work is done by the miner. |  The probability of validating a new block is determined by how large of a stake a person holds (how many coins they possess). |
|  A reward is given to the first miner to solve the cryptographic puzzle of each block. |  The validators do not receive a block reward, instead they collect network fees as their reward. |
|  Network miners compete with one another using computational power. Mining communities tend to become more centralized over time. |  Proof of Stake systems can be much more cost and energy efficient than Proof of Work systems, but are less proven. |

*3iQ Research Group*

# Différents types de blockchains




*Option la plus populaire dans le secteur privé*

Source : EY

# Logistique - BabyGhost

# Logistique - Récemment - StarBucks


Les clients des magasins américains de Starbucks peuvent désormais connaître la provenance du café quils consomment.

# Logistique - Récemment - StarBucks


Les clients des magasins américains de Starbucks peuvent désormais connaître la provenance du café quils consomment. Grâce à la technologie blockchain fournie par Microsoft, les producteurs de café savent eux aussi où sont consommés leurs grains de café.

# Économie - Cryptomonnaie


# Économie - Cryptomonnaie


Vidéo : *"La blockchain expliquée en émojis"*