Enjeux numériques du monde contemporain

La blockchain

Fabien Tarissan

CNRS – ENS Paris Saclay – ISP

ENUM

La blockchain

Technologie de registres distribués (*Distributed Ledger Technology*, DLT)

Une technologie de registres distribués est une base de données de transactions :

- transparente $\mapsto$ tout le monde a accès aux registres
- fiable $\mapsto$ on ne peut pas falsifier les registres
- décentralisée $\mapsto$ sans organe de contrôle central

La blockchain

La blockchain est une DLT particulière ayant les charactéristiques suivantes :

- les transactions sont *validées* par l'ensemble des participants (les mineurs)
- les transactions validées sont enregistrées dans des blocs
- chaque bloc contient la signature du bloc précédent (les blocs sont chaînés)

La blockchain

Technologie de registres distribués (*Distributed Ledger Technology*, DLT)

Une technologie de registres distribués est une base de données de transactions :

- transparente ↦ tout le monde a accès aux registres
- fiable ↦ on ne peut pas falsifier les registres
- décentralisée ↦ sans organe de contrôle central

La blockchain

La blockchain est une DLT particulière ayant les charactéristiques suivantes :

- les transactions sont *validées* par l'ensemble des participants (les mineurs)
- les transactions validées sont enregistrées dans des blocs
- chaque bloc contient la signature du bloc précédent (les blocs sont chaînés)

Qu'est-ce qu'une blockchain

Fonction de hachage

Le principe

Une *fonction de hachage* est une fonction qui

- à toute entrée (suite de symbole), de taille quelconque
- attribue une *empreinte* (un hash) de taille fixe

La sortie est une signature de taille fixe de l'entrée

Fonction de hachage

Le principe

Une *fonction de hachage* est une fonction qui

- à toute entrée (suite de symbole), de taille quelconque
- attribue une *empreinte* (un hash) de taille fixe

La sortie est une signature de taille fixe de l'entrée

Caractéristiques des fonctions de hachage

Une fonction de hachage est

- déterministe $\mapsto$ 1 entrée = 1 hash
- irréversible $\mapsto$ connaissant le hash, impossible d'identifier l'entrée
- résistante aux *collisions* $\mapsto$ 2 entrées différentes = 2 hash différents

Chaîne de caractère	SHA256
Bonjour	9172e8eec99f144f72eca9a568759580edadb2cfd154857f07e657569493bc44
Bonjour !	083de31ac1fa14f95671a6e39cc6c72d8fed1590b2a51759bc3f54a76b4169c4

Fonction de hachage

Le principe

Une *fonction de hachage* est une fonction qui

- à toute entrée (suite de symbole), de taille quelconque
- attribue une *empreinte* (un hash) de taille fixe

La sortie est une signature de taille fixe de l'entrée

Caractéristiques des fonctions de hachage

Une fonction de hachage est

- déterministe $\mapsto$ 1 entrée = 1 hash
- irréversible $\mapsto$ connaissant le hash, impossible d'identifier l'entrée
- résistante aux *collisions* $\mapsto$ 2 entrées différentes = 2 hash différents

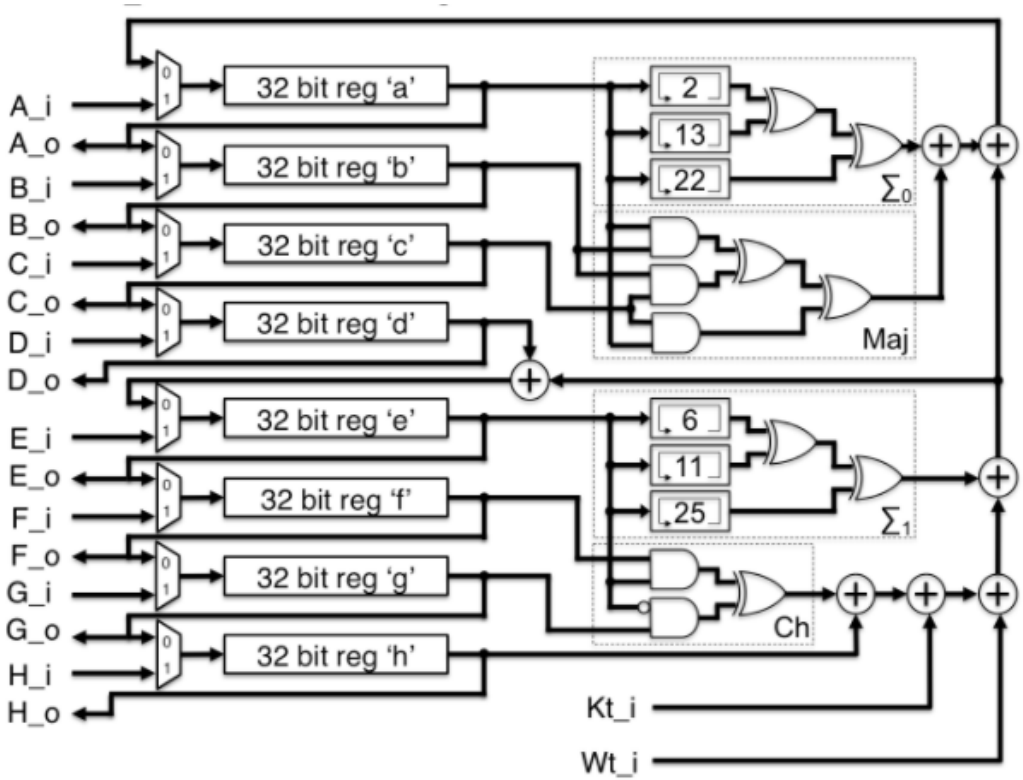
Chaîne de caractère	SHA256
Bonjour	9172e8eec99f144f72eca9a568759580edadb2cfd154857f07e657569493bc44
Bonjour !	083de31ac1fa14f95671a6e39cc6c72d8fed1590b2a51759bc3f54a76b4169c4

Utilité

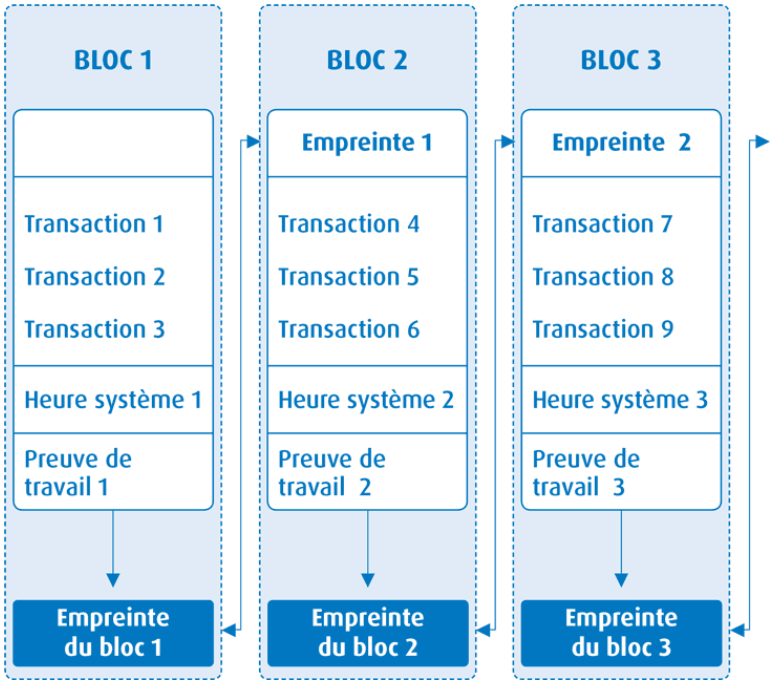
- Signature électronique
- Vérifier d'intégrité des données
- Sockage des mots de passe
- Fournir une preuve de calcul

Fonction de hachage

Calcul du SHA256 : `https://andersbrownworth.com/blockchain/hash`

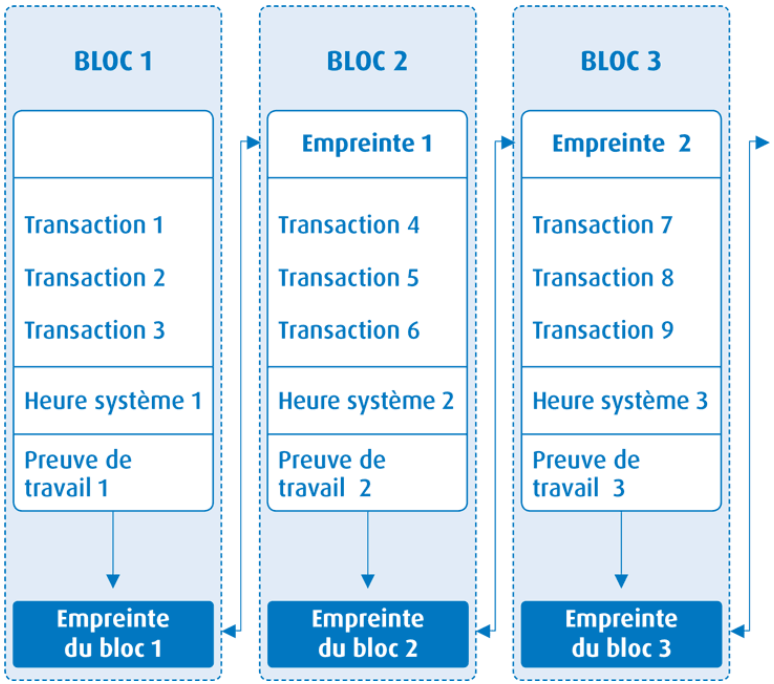


Principe de la Blockchain



La vie d'une blockchain

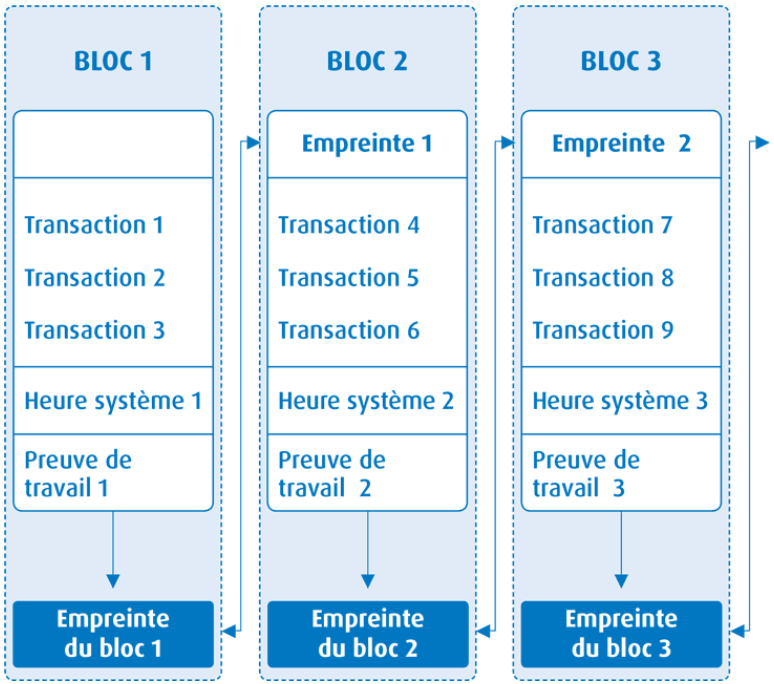
Principe de la Blockchain



La vie d'une blockchain

1. Sélection de transactions en attente de validation

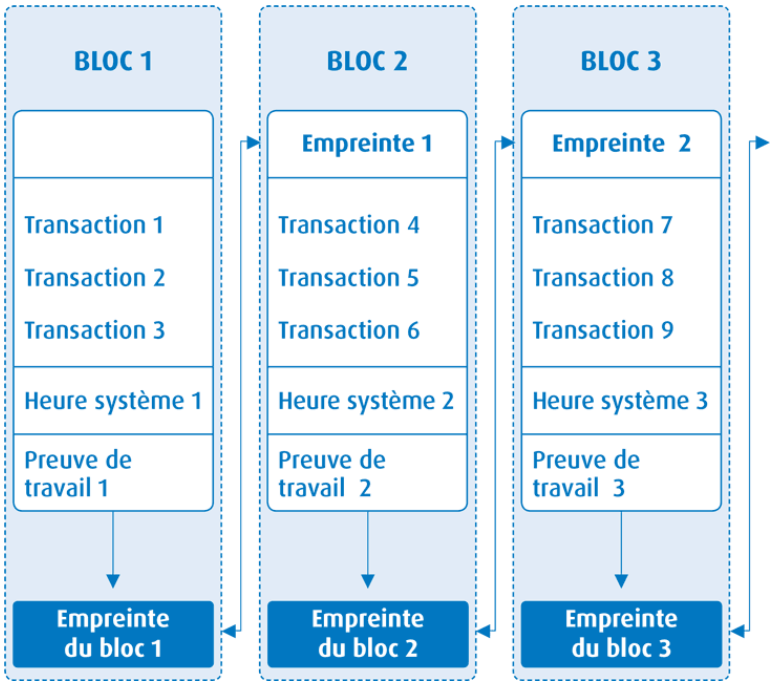
Principe de la Blockchain



La vie d'une blockchain

1. Sélection de transactions en attente de validation
2. Validation des transactions à l'aide d'une preuve de travail (*miner*)

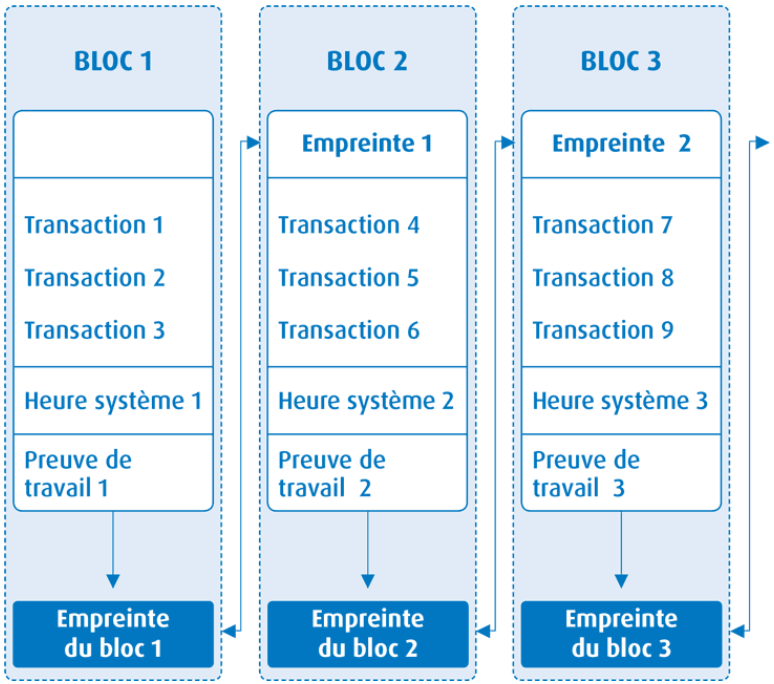
Principe de la Blockchain



La vie d'une blockchain

1. Sélection de transactions en attente de validation
2. Validation des transactions à l'aide d'une preuve de travail (*miner*)
3. Création d'un nouveau bloc ajouté à la chaîne (empreinte du bloc précédent)

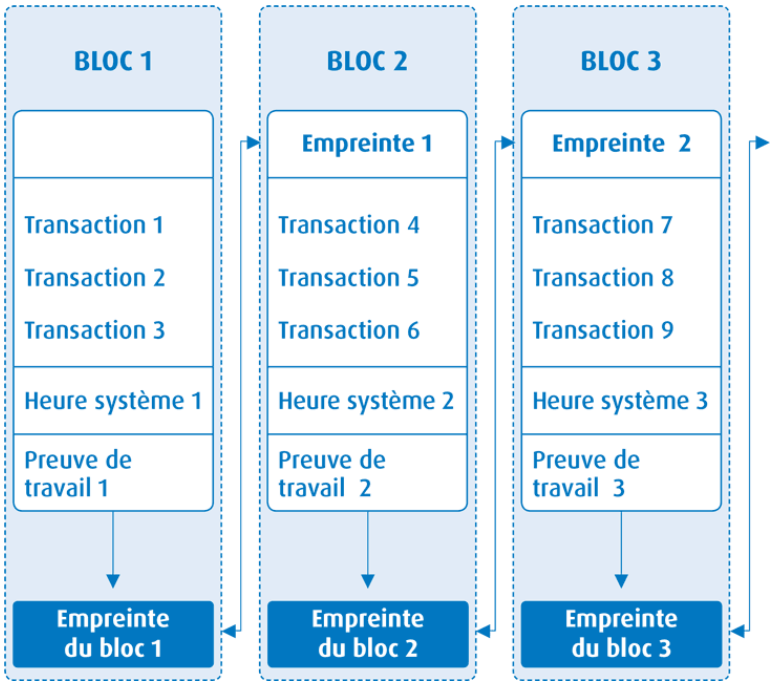
Principe de la Blockchain



La vie d'une blockchain

1. Sélection de transactions en attente de validation
2. Validation des transactions à l'aide d'une preuve de travail (*miner*)
3. Création d'un nouveau bloc ajouté à la chaîne (empreinte du bloc précédent)
4. Propagation de l'ajout du nouveau bloc à tout le réseau

Principe de la Blockchain



La vie d'une blockchain

1. Sélection de transactions en attente de validation
2. Validation des transactions à l'aide d'une preuve de travail (*miner*)
3. Création d'un nouveau bloc ajouté à la chaîne (empreinte du bloc précédent)
4. Propagation de l'ajout du nouveau bloc à tout le réseau

Questions

- Qu'est-ce que la preuve de travail ?
- Que se passe-t-il si plusieurs transactions sont validées en même temps (*ie.* plusieurs blocs sont créés en même temps)
- Que se passe-t-il si on modifie une information dans un bloc antérieur (tentative de falsification) ?

La preuve de travail

La cible (*Target Hash*)

Le Nonce (*number only used once*)

La preuve de travail

La cible (*Target Hash*)

- Contrainte posée sur la valeur du *hash* du bloc (ex : $< 2^{56}$)

Le Nonce (*number only used once*)

- Miner : trouver une chaîne de caractère tel que l'empreinte du bloc vérifie la contrainte

La preuve de travail

La cible (*Target Hash*)

- Contrainte posée sur la valeur du *hash* du bloc (ex : $< 2^{56}$)
- Pour Bitcoin, calibrée pour être trouvée toutes les 10 minutes
- Réactualisée tous les 2016 blocs

Le Nonce (*number only used once*)

- Miner : trouver une chaîne de caractère tel que l'empreinte du bloc vérifie la contrainte
- Pour le Bitcoin, cela génère de la rémunération (en bitcoin)

La preuve de travail

La cible (*Target Hash*)

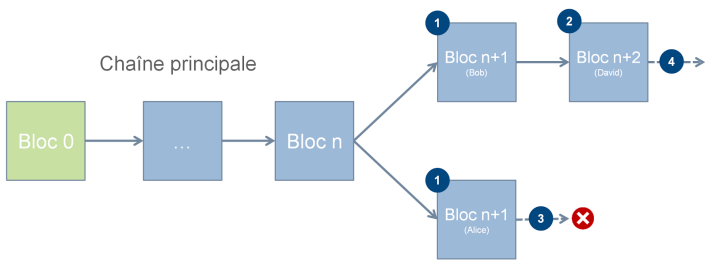
- Contrainte posée sur la valeur du *hash* du bloc (ex : $< 2^{56}$)
- Pour Bitcoin, calibrée pour être trouvée toutes les 10 minutes
- Réactualisée tous les 2016 blocs

Le Nonce (*number only used once*)

- Miner : trouver une chaîne de caractère tel que l'empreinte du bloc vérifie la contrainte
- Pour le Bitcoin, cela génère de la rémunération (en bitcoin)

Pourquoi ajouter cette difficulté ?

- Pour faciliter le consensus (quelle blockchain est valide ?) :
  - la blockchain la plus longue est celle qui est valide pour le réseau ($\sim 10min.$ pour créer un bloc)



La preuve de travail

La cible (*Target Hash*)

- Contrainte posée sur la valeur du *hash* du bloc (ex : $< 2^{56}$)
- Pour Bitcoin, calibrée pour être trouvée toutes les 10 minutes
- Réactualisée tous les 2016 blocs

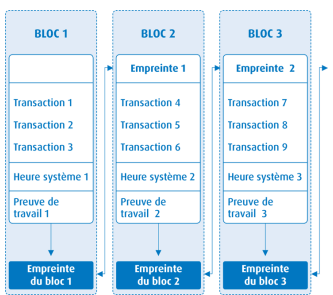
Le Nonce (*number only used once*)

- Miner : trouver une chaîne de caractère tel que l'empreinte du bloc vérifie la contrainte
- Pour le Bitcoin, cela génère de la rémunération (en bitcoin)

Pourquoi ajouter cette difficulté ?

- Pour faciliter le consensus (quelle blockchain est valide ?) :
  - la blockchain la plus longue est celle qui est valide pour le réseau ($\sim 10min.$ pour créer un bloc)
- Pour empêcher une falsification des registres
  - Modification d'une transaction du bloc 1 $\Longrightarrow$ modification du hash du bloc 1 ...
  - $\Longrightarrow$ modification du hash du bloc 2 ... $\Longrightarrow$ modification du hash du bloc n

$\Longrightarrow$ Il faut plus de puissance de calcul que l'ensemble des autres mineurs ! !



Les besoins de chiffrement

Il reste encore quelques problèmes ...

N'importe qui peut émettre une transaction.

- Comment s'assurer de l'authenticité de la personne ?
- Comment s'assurer que la personne possède une somme d'argent ?

Pas d'organe central (banque) pour ces deux taches

Les besoins de chiffrement

Il reste encore quelques problèmes ...

N'importe qui peut émettre une transaction.

- Comment s'assurer de l'authenticité de la personne ?
- Comment s'assurer que la personne possède une somme d'argent ?

Pas d'organe central (banque) pour ces deux taches

Cryptographie

Ensemble de techniques visant à protéger le contenu d'un message

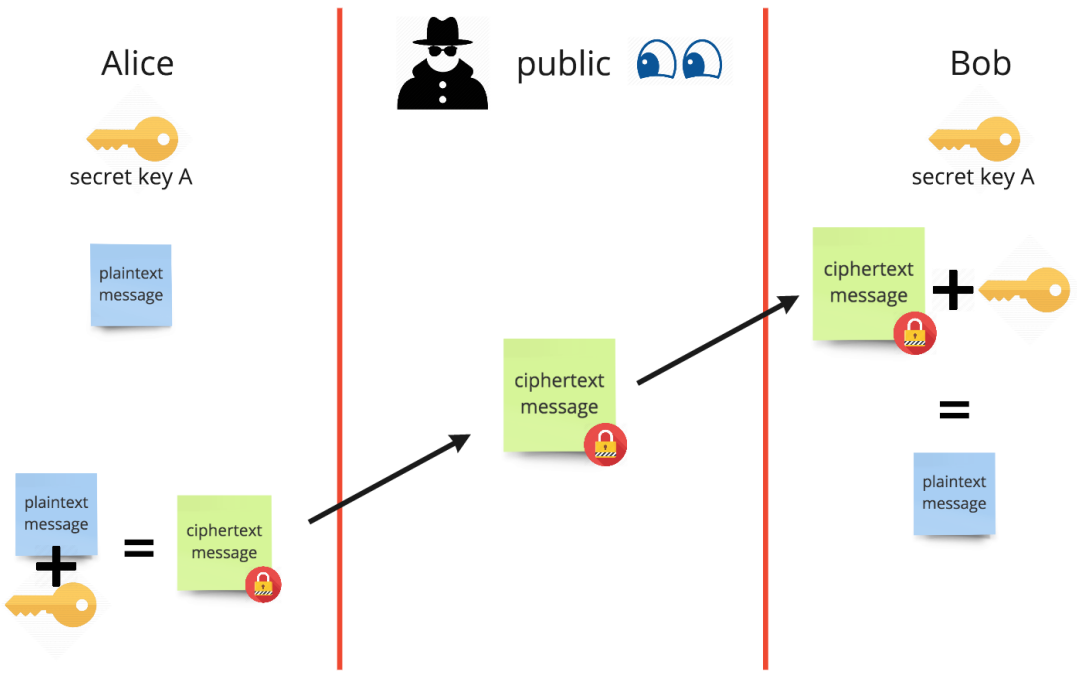
2 techniques principales

- cryptographie symétrique
- cryptographie asymétrique

Les techniques de chiffrement

Cryptographie symétrique

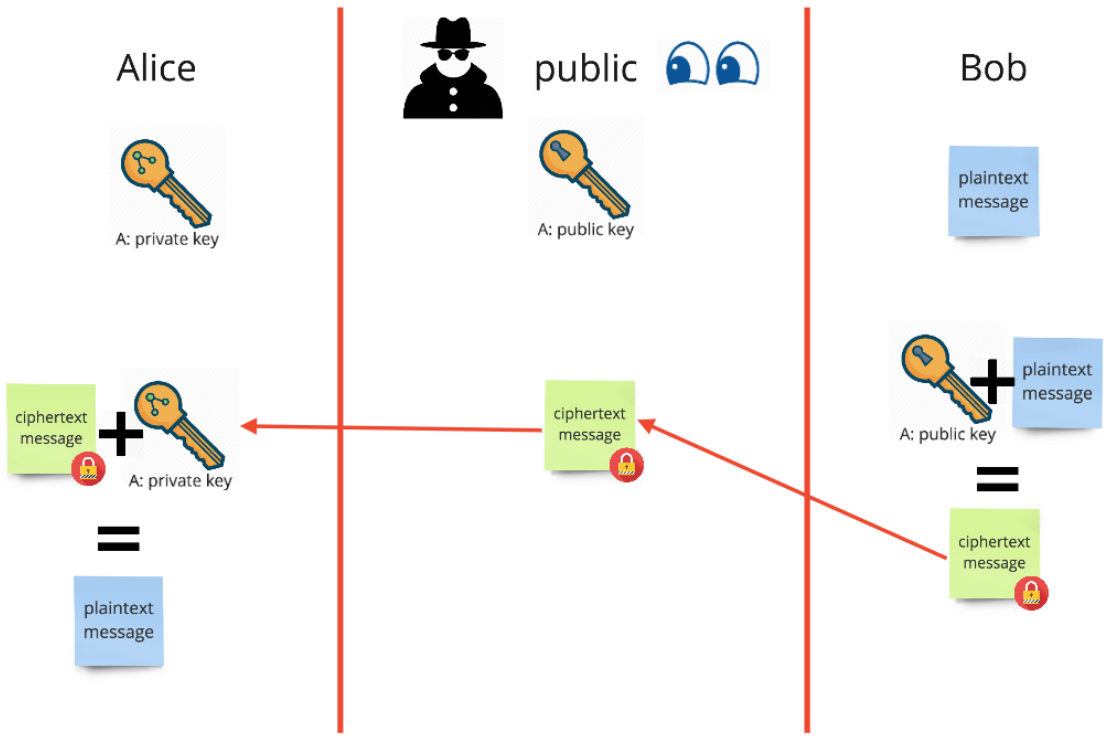
1 clé secrète et unique pour un coupe d'individus (Alice, Bob)



Cryptographie asymétrique

Chaque individu possède une clé publique et une clé privée

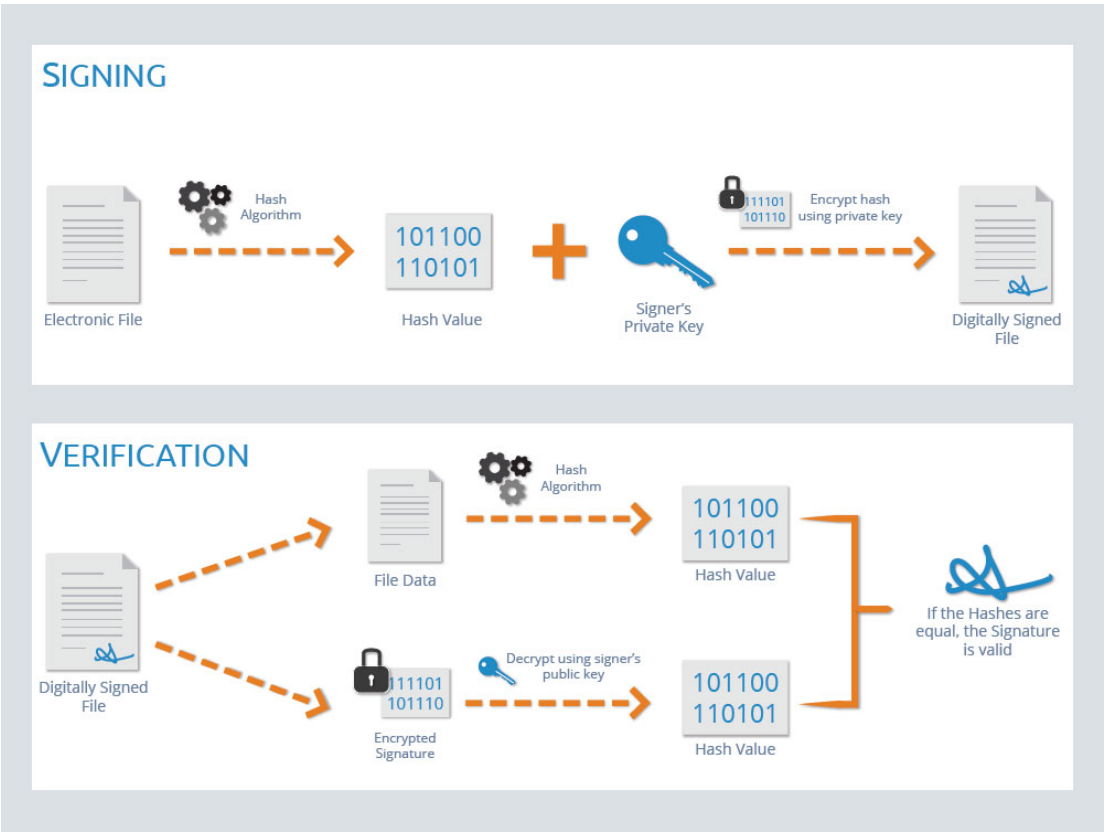
- ma clé publique pour que les autres chiffrent leur message
- ma clé privée pour que je déchiffre les messages



Signature électronique

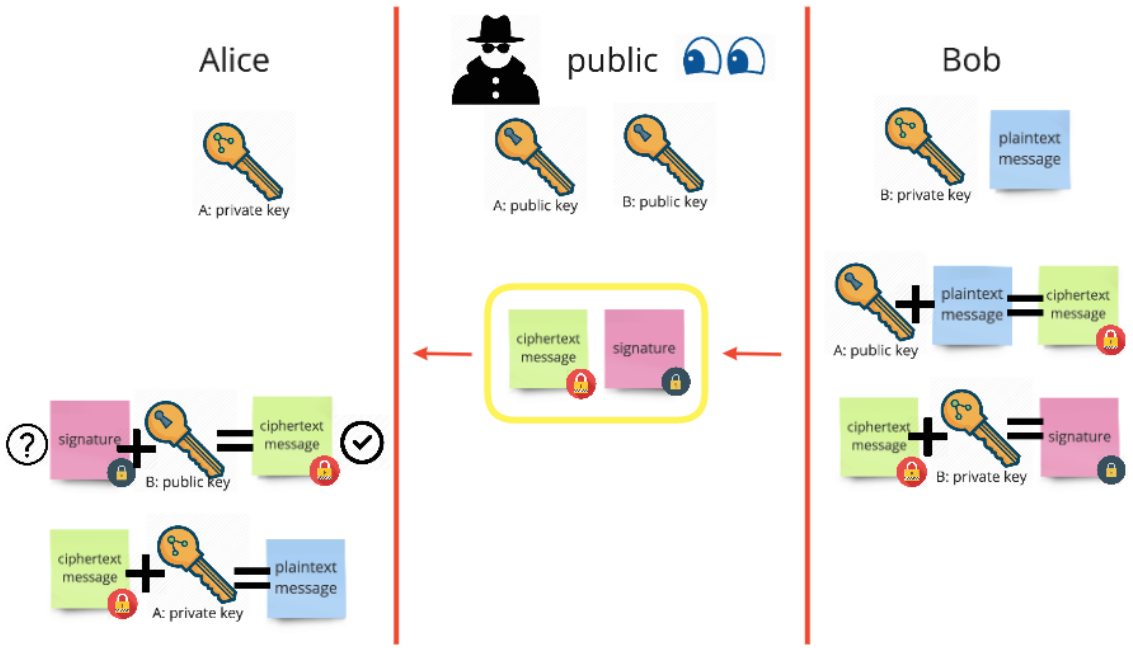
Chaque individu possède une clé publique et une clé privée

- ma clé privée pour que je signe mon message
- ma clé publique pour que les autes puissent authentifier mon message



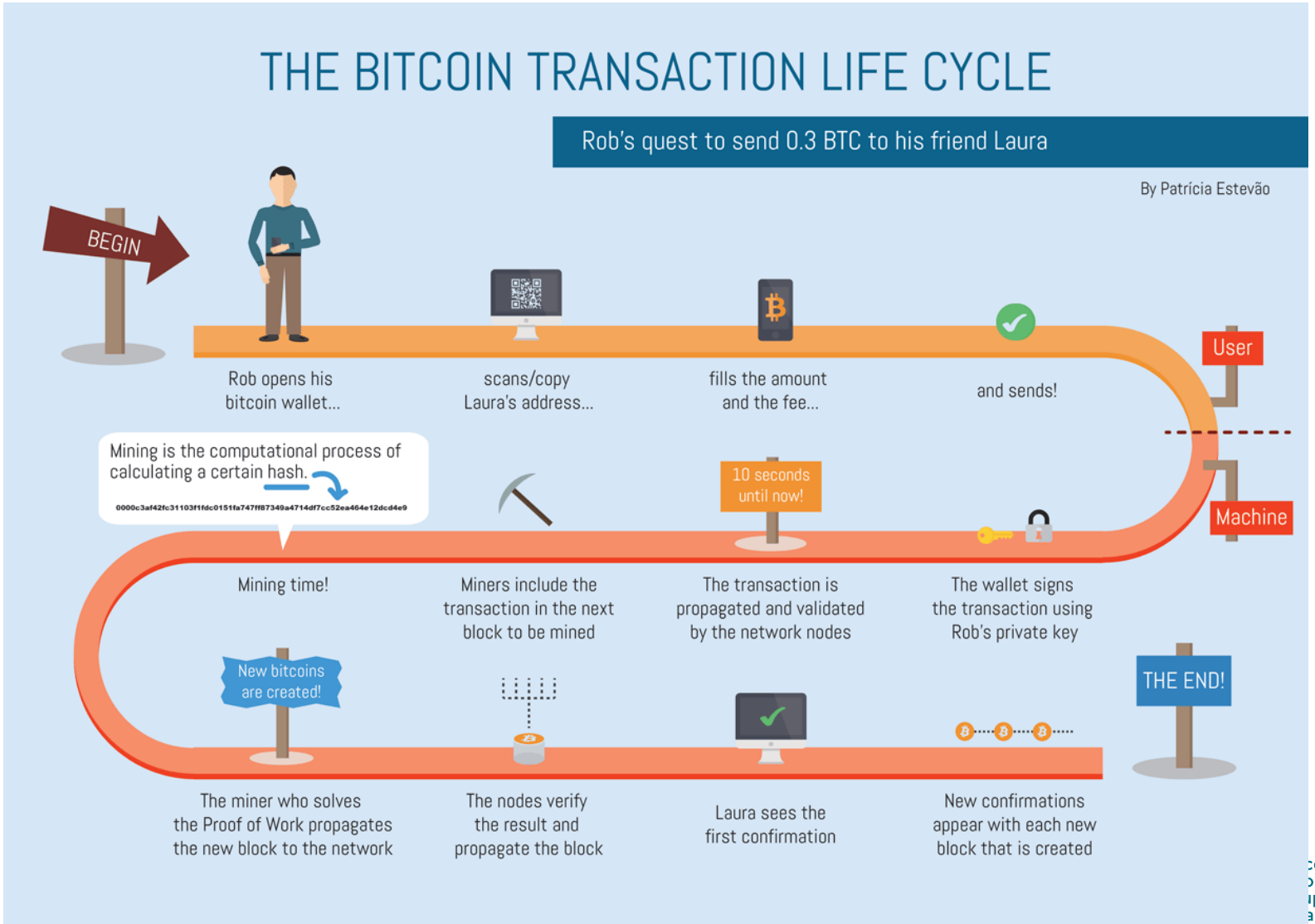
Chiffrement & signature

Chaque individu possède une clé publique et une clé privée



Le cas du bitcoin

Le cas du Bitcoin



Le cas du Bitcoin

Quelques propriétés, problématiques et enjeux autour du Bitcoin

- Importance de la clé privée

Cas de James Howells

Perd son ordinateur avec sa clé privée $\Longrightarrow$ perd 7 500 bitcoins

Le cas du Bitcoin

Quelques propriétés, problématiques et enjeux autour du Bitcoin

- Importance de la clé privée
- Question de l'anonymat

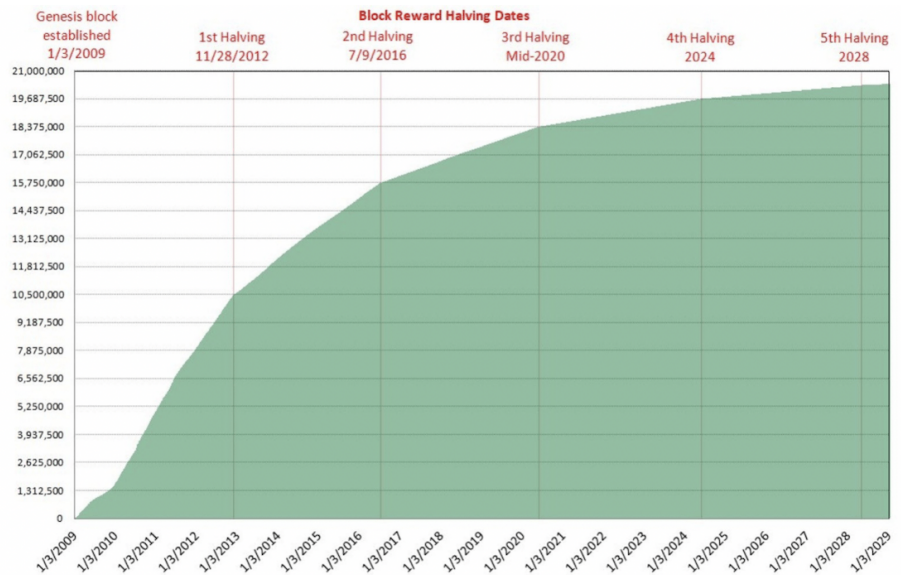
Cas de James Howells

Perd son ordinateur avec sa clé privée $\Longrightarrow$ perd 7 500 bitcoins

Le cas du Bitcoin

Quelques propriétés, problématiques et enjeux autour du Bitcoin

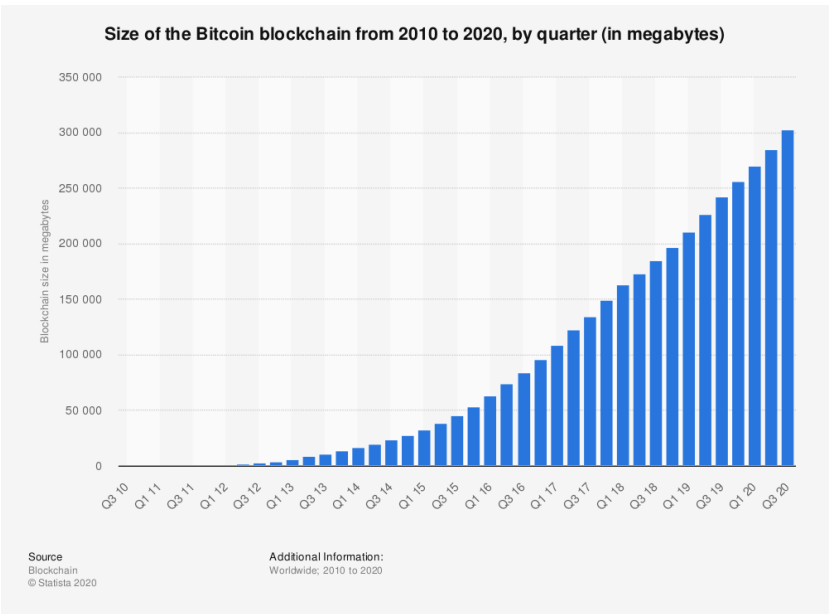
- Importance de la clé privée
- Question de l'anonymat
- Création de monnaie bitcoin connue et transparente



Le cas du Bitcoin

Quelques propriétés, problématiques et enjeux autour du Bitcoin

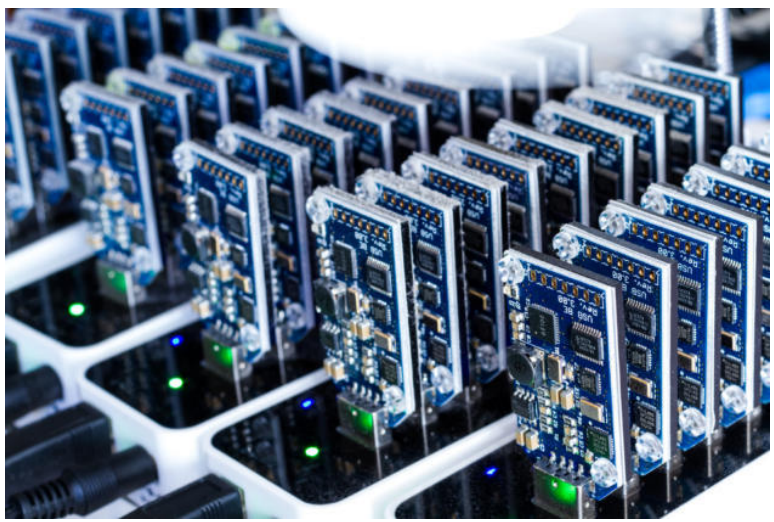
- Importance de la clé privée
- Question de l'anonymat
- Création de monnaie bitcoin connue et transparente
- Taille de la blockchain



Le cas du Bitcoin

Quelques propriétés, problématiques et enjeux autour du Bitcoin

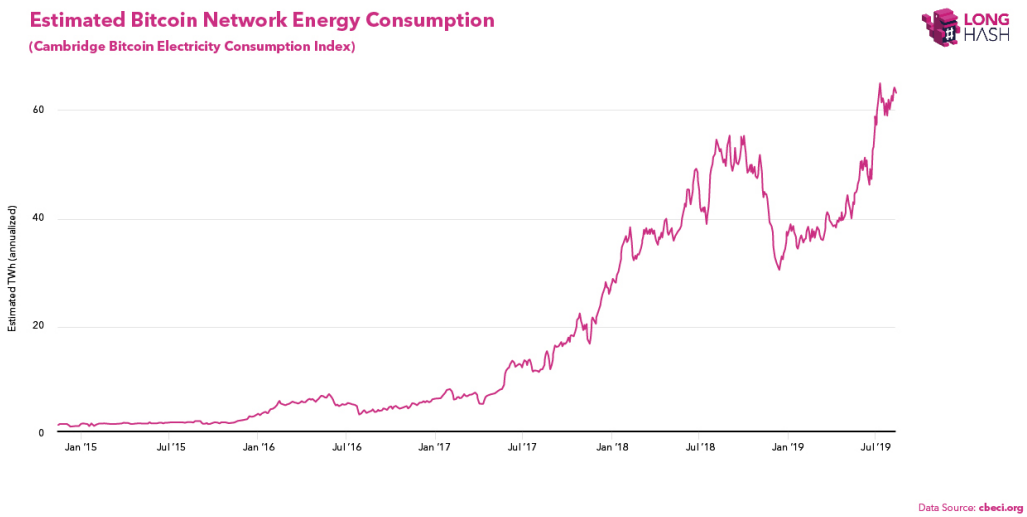
- Importance de la clé privée
- Question de l'anonymat
- Création de monnaie bitcoin connue et transparente
- Taille de la blockchain
- Concurrence entre les mineurs



Le cas du Bitcoin

Quelques propriétés, problématiques et enjeux autour du Bitcoin

- Importance de la clé privée
- Question de l'anonymat
- Création de monnaie bitcoin connue et transparente
- Taille de la blockchain
- Concurrence entre les mineurs
- Coût énergétique de la preuve de travail



Questions ?

http://tarissan.complexnetworks.fr/