La Blockchain

Concepts et implémentation

Patrick Valduriez

Objectif

- Problème
  - Comment échanger des actifs entre deux agents qui ne se connaissent pas sans que la transaction ne doive être sécurisée et validée par une autorité centrale (ex. tiers de confiance)?
- Solution
  - Un registre public des transactions, infalsifiable par construction, et partagé par tous
  - Techniques: réseau P2P, réplication des données, protocole de consensus, chiffrement à clé publique

Historique

- Bitcoin: A Peer-to-Peer Electronic Cash System
  - Satoshi Nakamoto (pseudo), 31/10/2008 (Halloween)
  - Cryptomonnaie et système de paiement P2P
  - Implémentation en logiciel libre
- 3 Janvier 2009
  - Satoshi Nakamoto crée le premier block source avec une transaction unique de 50 bitcoins à "lui-même"
- Depuis
  - D'autres blockchains et crytomonnaies
    - Etherum en 2013, Ripple en 2014
  - Des scandales : achats illégaux, blanchiment d'argent, vols, malwares
    - Détournement de +700000 bitcoins à Mt. Gox en 2014
  - Mises en garde (autorités de marché) et début de régulation (Chine, Corée du Sud, Japon, ...)

Capitalisation (21 février 2018)

- Plus de 180 milliards de $ (coinmarketcap.com)

#	Name	Market Cap	Price	Volume (24h)
1	Bitcoin	$182 572 095 510	$10 817,10	$10 084 100 000
2	Ethereum	$85 263 694 504	$872,23	$2 626 560 000
3	Ripple	$40 717 819 492	$1,04	$885 956 000
4	Bitcoin Cash	$22 914 734 833	$1 349,55	$678 512 000
5	Litecoin	$11 872 073 565	$214,62	$1 368 250 000

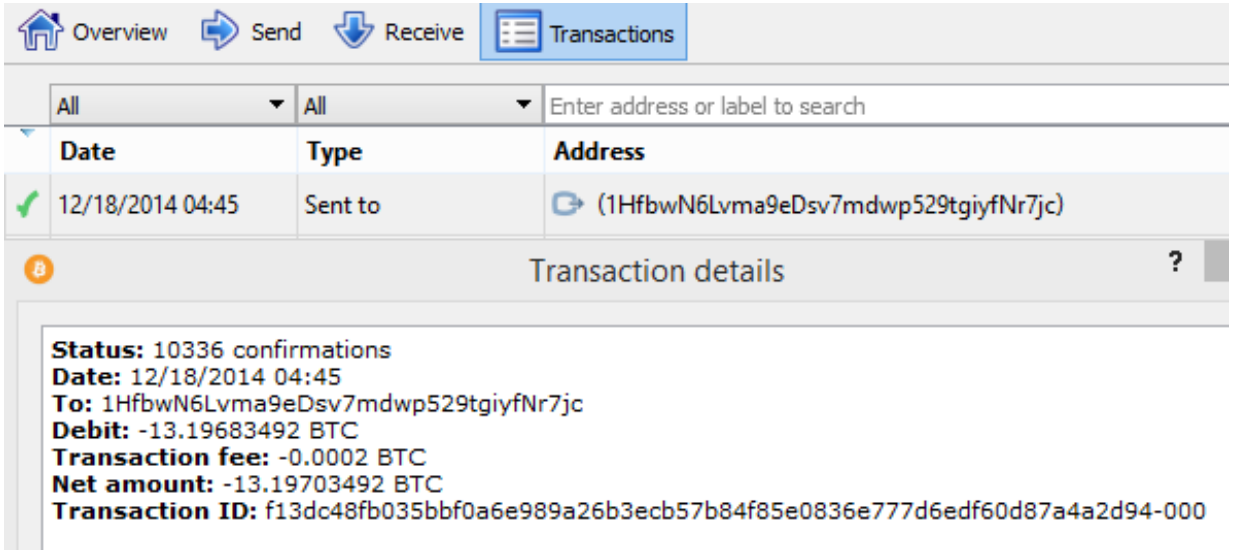
La blockchain : concepts

- Chaine de blocs
  - Un journal distribué et sûr
  - Répliqué sur tous les nœuds du réseau (les *full nodes*)
- Un bloc
  - Conteneur numérique pour transactions, contrats, titres de propriétés, etc.
- Le code de chaque nouveau bloc est construit sur celui du bloc qui le précède
  - Impossible de modifier à posteriori
- La blockchain est consultée par tous
  - Pour pouvoir valider les inscriptions dans les blocks
  - Confidentialité: les utilisateurs sont pseudonymisés

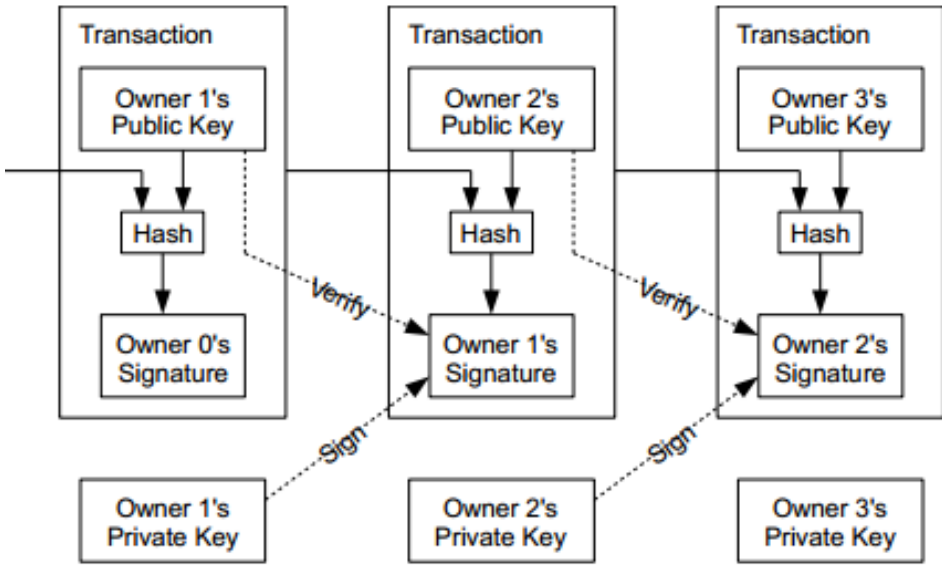
Implémentation

0. Initialisation (d'un *full node*)
   - Synchronisation avec le réseau pour récupérer la blockchain (160 GB au 20/2/2018)
1. Deux utilisateurs s'accordent sur une transaction
   - Echange d'information: adresses de portefeuille, clés, ...
2. Regroupement avec d'autres transactions dans un bloc et validation du bloc
   - Consensus par "mining"
3. Ajout du bloc validé dans la blockchain et réplication dans tout le réseau
4. Confirmation de la transaction

Transaction

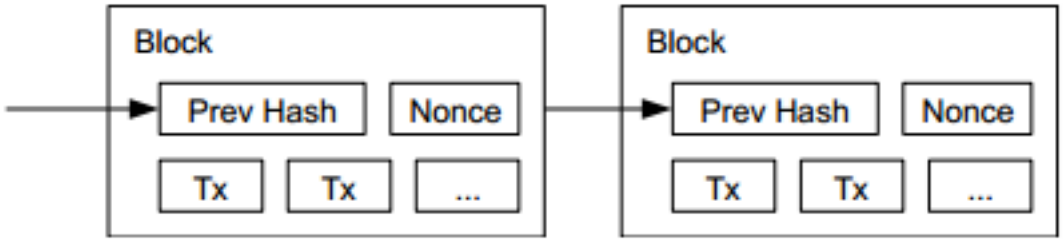


- Signature par l'émetteur à partir
  - D'un hash code de la transaction précédente
  - De sa clé privée



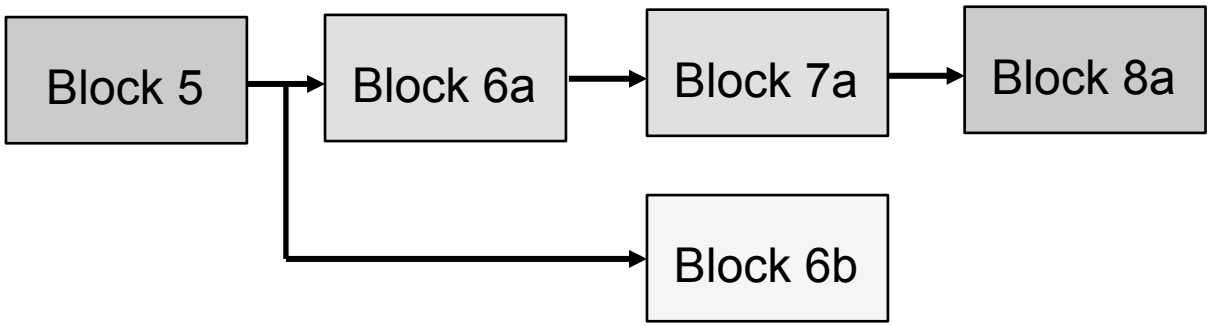
Gestion de blocs

- Les transactions sont diffusées dans le réseau, qui vérifie leur viabilité
- Les transactions viables sont placées dans des blocs, reliés par leurs adresses
  - Taille d'un bloc bitcoin = 1 MB



Validation par le réseau

- Chaque bloc est validé par des nœuds du réseau, les *mineurs*, par un protocole de consensus
- Comme différents blocs sont validés en parallèle, à tout moment, on peut voir plusieurs chaînes candidates
- *Longest chain rule*: prendre la chaîne la plus longue



Les transactions dans un bloc validé sont provisoirement validées; il faut attendre une confirmation

Protocole de consensus : le *mining*

- Pour valider un bloc, les nœuds mineurs concourent (comme à la loterie) pour produire une valeur numérique appelée *nonce* (number used once)
  - Une des solutions concurrentes est sélectionnée
    - Ex. celle qui inclut le plus grand nombre de transactions
  - Le mineur sélectionné est rémunéré
    - Ex. 12,5 bitcoins aujourd'hui (50 à l'origine)
    - Augmentation de la masse monétaire

Calculer du *nonce*: PoW versus PoS

- PoW (Proof of Work), utilisé dans Bitcoin
  - Très sûr, à l'origine pour empêcher les attaques de déni de service
  - Difficile à calculer (il faut une très grande puissance de calcul) mais facile à vérifier
  - Avantage les nœuds puissants
- PoS (Proof of Stake), annoncé dans Etherum
  - Facile à calculer: la preuve d'enjeu demande au mineur de prouver la possession d'une certaine quantité de crypto-monnaie
  - Avantage les nœuds riches

L'attaque des 51% (bitcoin)

- Appelée aussi attaque *Goldfinger*
  - Permet de bloquer les validations de transactions ou bien dépenser ses bitcoins plusieurs fois
- Comment
  - En détenant plus de 50% de la puissance totale de calcul pour le mining
    - Coalition de mineurs
  - Il devient alors possible de modifier une chaîne reçue (par ex. en enlevant une transaction) et produire une chaîne plus longue qui sera sélectionnée
- Solution
  - Surveillance par la communauté Bitcoin
  - En janvier 2014, Ghash.io a atteint 42%, puis a chuté à 9% après l'alerte de la communauté

Confirmation de transaction

- Une transaction provisoirement validée dans un bloc candidat qu'elle a été vérifiée et est viable
- Chaque nouveau bloc accepté dans la chaîne après la validation de la transaction est considéré comme une confirmation
- Bitcoin
  - Une transaction est considérée comme mature après 6 confirmations (1 heure en moyenne)
  - De nouveaux bitcoins (produits du mining) ne sont valides qu'après 120 confirmations, pour éviter l'attaque des 51%

Temps moyen d'une transaction

De 10mn à plusieurs jours

Limites de la blockchain

- Complexité
  - Evolution des règles de fonctionnement difficile
  - Taille croissante de la chaine
  - Consommation énergétique importante (avec PoW)
- Pseudonymisation des utilisateurs
  - Faire une transaction avec un utilisateur nous dévoile toutes ses autres transactions
  - On sait aussi que Satoshi Nakamoto est milliardaire en bitcoins
- Durée imprévisible des transactions
  - De qqs minutes à qqs jours
- Pas de standard
  - Différentes blockchains, non interopérables
- Absence de contrôle et de régulation

Blockchain 2.0

- Technologie disruptive
  - *The blockchain will do to the financial system what the internet did to media*. Harvard Business Review, mars 2017
  - Pour toutes sortes d'activités d'enregistrement (événements, contrats, identité, etc.)
  - Validation de transaction très efficace si les participants sont connus et de confiance
    - Pas besoin de produire une PoW
- Tous les grands acteurs s'y intéressent
  - Finance: Mastercard, Visa, …
  - Cabinets d'audit: EY, KPMG, PwC, Deloitte
  - Sociétés de conseil: Accenture, Capgemini, IBM
  - Géants du web: Amazon, Google
  - Editeurs de logiciels: IBM, Oracle, Microsoft, SAP
    - Projet Hyperledger (Linux Foundation)