

Les chaines de blocs

Le Bon, la Brute et le Truand

Louis Martin
Professeur – Département d'informatique
Université du Québec à Montréal



31 mai 2018



Le Bon, la Brute et le Truand



Les chaines de blocs et non les cryptomonnaies

- Les cryptomonnaies font les manchettes des médias depuis plusieurs mois — déjà plus de 3000 cryptomonnaies
- La présente présentation se concentre sur les chaines de blocs, la technologie derrière la majorité des cryptomonnaies
- Objectif visé : appréhender les chaines de blocs pour en saisir les opportunités et les risques
- Il s'agit d'une entrée en matière

Bitcoin énergivore



Bitcoin énergivore

- Visa peut traiter 60 000 transactions par seconde
- Bitcoin est actuellement limité à 7 transactions par seconde
- Bitcoin consomme actuellement 35 fois plus d'énergie que Visa
- Si Visa fonctionnait sur le même principe que Bitcoin, l'équivalent de 5 000 centrales atomiques serait nécessaires



Définition

La chaîne de blocs est une technologie qui permet de stocker et transmettre des informations de manière transparente, sécurisée et **sans organe central de contrôle**. Elle ressemble à une grande base de données qui contient l'historique de tous les échanges réalisés entre ses utilisateurs depuis sa création. La chaîne de blocs peut être utilisée :

- pour du transfert d'actifs (monnaie, titres, actions...)
- pour une meilleure traçabilité d'actifs et produits
- pour exécuter automatiquement des contrats (des "smart contracts")

— *tiré du Journal du Net*

Fonction de hachage I

Petit éditeur

Liège est une ville magnifique et accueillante.

Calculer le hash

Hash courant : **dd7f4eaf835d649472a871cc05cbf43e50008958fd0142ce3ff0d65fb10eecd1**

Hash précédent :

Fonction de hachage II

- SHA256 est une fonction de hachage de la famille SHA-2 — *Secure Hash Algorithm* — conçue par la National Security Agency — *NSA* — des États-Unis
- $1,15^{77}$ combinaisons possibles
- Probabilité d'une collision équivalente à gagner 10 fois consécutives le gros lot de la lotto
- Il est impossible de reconstruire le message de base à partir de son hash

Fonction de hachage III

Petit éditeur

Liège est une ville magnifique et accueillante

Calculer le hash

Hash courant : **b1c4e88d4d08deba9f0c8f4e0719286602bae62b626fbab5bd4dad938da209fb**

Hash précédent : **dd7f4eaf835d649472a871cc05cbf43e50008958fd0142ce3ff0d65fb10eecd1**

Une chaine de blocs simple I

Bloc genèse

```
'contenu':  
  { 'bloc_numero': 0,  
    'hash_parent': None,  
    'horodateur': '2018-04-25 18:49:39.319246',  
    'nbre_transactions': 1,  
    'nonce': 88,  
    'transactions': [{'Compte_A': 50, 'Compte_B': 50}]}  
'hash': '0008fd96d0e824331f770f883ab2a0f3  
          943391c7d5a8aaa6d293d7fcbfd12fbf'
```

Une chaine de blocs simple II

'contenu':

```
{ 'bloc_numero': 1,  
  'hash_parent': '0008fd96d0e824331f770f883ab2a0f3  
                  943391c7d5a8aaa6d293d7fcbfd12fbf',  
  'horodateur': '2018-04-25 18:49:39.321375',  
  'nbre_transactions': 5,  
  'nonce': 11042,  
  'transactions': [{ 'Compte_A': 2, 'Compte_B': -2},  
                    { 'Compte_A': 2, 'Compte_B': -2},  
                    { 'Compte_A': -2, 'Compte_B': 2},  
                    { 'Compte_A': 3, 'Compte_B': -3},  
                    { 'Compte_A': -2, 'Compte_B': 2}]]},
```

```
'hash': '0000dfa7645bcbae283a202888d75a30  
        277fee762016ad0e1a00a36332af2814'
```

Une chaine de blocs simple III

'contenu':

```
{ 'bloc_numero': 2,  
  'hash_parent': '0000dfa7645bcbae283a202888d75a30  
                  277fee762016ad0e1a00a36332af2814',  
  'horodateur': '2018-04-25 18:49:39.588213',  
  'nbre_transactions': 5,  
  'nonce': 5423,  
  'transactions': [{ 'Compte_A': 2, 'Compte_B': -2},  
                    { 'Compte_A': 2, 'Compte_B': -2},  
                    { 'Compte_A': -3, 'Compte_B': 3},  
                    { 'Compte_A': 1, 'Compte_B': -1},  
                    { 'Compte_A': 1, 'Compte_B': -1}]]},
```

```
'hash': '00016eeca4a60c0bf8e41c9efec157af  
        02db70674ba199c2850f92f82d04017a'
```

Types de chaine de blocs

	Publique	Consortium	Semi-privée
Accès	Aucune permission requise	Membres seulement	Utilisateurs qualifiés (inscription en ligne)
Innovation visée	Nouveau modèle d'affaires	Nouveau processus au sein d'une relation existante	En soutien à l'existant ou un nouveau service
Gouvernance	Consensus public	Poids égal pour tous les participants	Contrôle par le propriétaire
Nombre d'utilisateurs	$1\ 000\ 000 < x$	$10 < x < 500$	$500 < x < 10\ 000$

Le pour

« Blockchain is still one of the most promising technologies to help with the lack of trust of consumers in institutions, government, Tech companies and the like. »

— Michael K. Spencer

- Archive numérique, décentralisée et publique
- Indépendance d'un tiers de confiance
- Libération des Uber, AirBnB, etc.
- Révolution comparable à celle d'Internet à ses débuts — Web 3.0
- Potentiel de sauver la vie de plus d'un million de personnes par année

Cas d'utilisation



Les DAO

« Une Decentralized Autonomous Organization (DAO ou en français « Organisation Autonome Décentralisée ») est une organisation fonctionnant grâce à un programme informatique qui fournit des règles de gouvernance à une communauté. Ces règles sont transparentes et immuables, car inscrites dans la blockchain, une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle »

— Wikipédia

■ Le cas de *TheDAO*

6 idées fausses sur les chaines de blocs

- 1 Le mythe de l'immuabilité
- 2 Le mythe de la désintermédiation et de la décentralisation
- 3 Le mythe de la confiance zéro
- 4 Le mythe selon lequel les chaines de blocs sont « des machines de vérité »
- 5 Le mythe de la transparence
- 6 Le mythe des « contrats intelligents »

— tiré de Byron Connolly dans *Everything you think you know about blockchain is wrong : 6 common myths*

Le contre I

« La technologie n'est jamais neutre. C'est un terrain de conflit influencé par les imaginaires et les intérêts des personnes en charge de son design. La blockchain dérive ainsi d'une vision de l'homme très particulière : des individus autonomes passent des contrats entre eux. Ils n'ont pas besoin de collectif, de communauté. Et les contrats sont fondés sur une forme de propriété. »

— Michel Bauwens, théoricien de l'économie collaborative et fondateur de la Peer-to-peer Foundation, règle son compte à la Blockchain sur Le Monde.fr 2016-04-18

Le contre II

- La présence d'un tiers de confiance assure un meilleur fonctionnement
- Le tiers de confiance a une responsabilité
- La technologie est complexe à comprendre et à en évaluer les limites
- Les « contrats intelligents » sont des programmes informatiques avec leurs aléas
- Le domaine est loin d'être mature
- Les recours légaux absents

L'approche du projet pilote

- Choix crucial pour la suite
- Si une base de données classique ne peut répondre aux besoins
- Si les parties prenantes n'ont pas établi une relation de confiance entre eux
- Si un tiers de confiance ne peut répondre aux besoins
- S'il existe une relation entre les transactions inscrites dans la base de données partagée
- Déterminer le mécanisme de validation : un seul acteur, un groupe déterminé d'acteurs ou tous les acteurs ; le protocole de validation doit empêcher les manipulations malveillantes ; les règles d'établissement du consensus doivent être établies
- Identifier qui sera garant des actifs inscrits dans une chaîne de blocs, par exemple, qui émettra les crédits de carbone ; dans plusieurs cas, l'entité garante assume une responsabilité légale.

Sur le site *Platform.coop*

- Arcade City — Blockchain-based ridesharing
- ARK — "provides users, developers, and startups with innovative blockchain technologies"
- Backfeed — "develops governance schemes and economic models for decentralized organizations, enabling a true collaborative economy using blockchain technologies"
- Bank of the Commons — "Global and Cooperatively Owned Banking system. Supports Cryptocurrencies and Fiat. Is developing Blockchain based credit system without interest."
- BitHouse — "A blockchain infrastructure project to tokenize property"
- Plus une dizaine d'autres organisations

Importance de la gouvernance

Dans la pratique, les mécanismes de sécurité et de gouvernance qui s'appliquent au réseau permettent de maîtriser le risque. « Les participants de l'écosystème doivent comprendre que ce n'est pas la technologie en tant que telle qui protège les enregistrements de la chaîne de blocs contre les modifications, mais la façon dont le réseau est conçu, mis en œuvre et exploité. Cela s'applique aux réseaux dotés de mécanismes de consensus qui offrent plus d'évolutivité, mais qui, à eux seuls, apportent peu ou pas de protection contre les attaques malveillantes », ont encore expliqué les chercheurs.

