NRC·CNRC

NRC.CANADA.CA

Chaîne de blocs et autres technologies de registres distribués : coup d'œil sous le capot

Stephen Downes

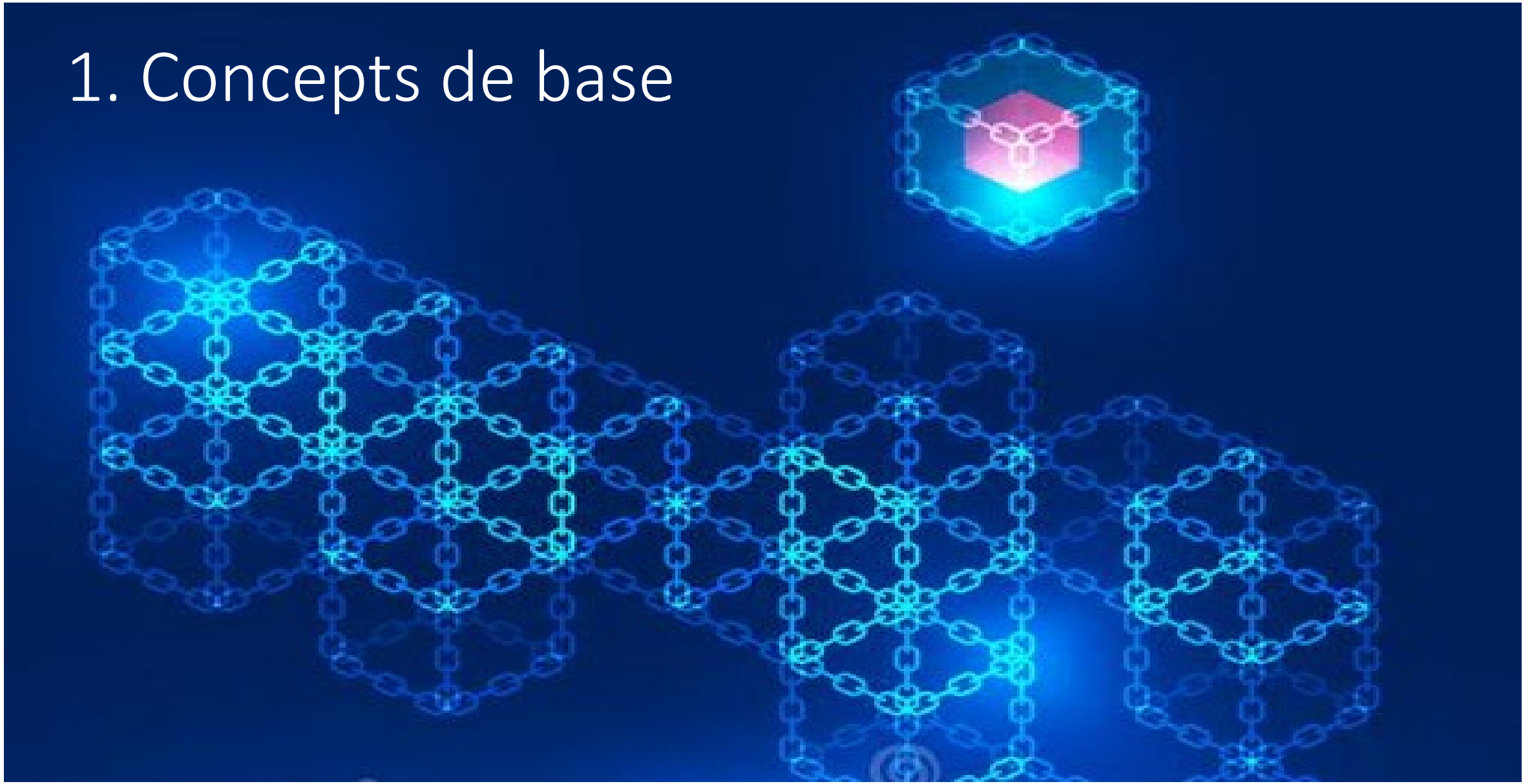
Centre de recherche en technologies numériques

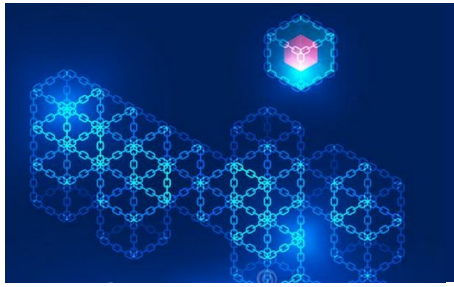
23 novembre 2017

Pourquoi recourir à la chaîne de blocs?

- Confiance
- Consensus
- Provenance
- Immutabilité et Finalité
- Équité?

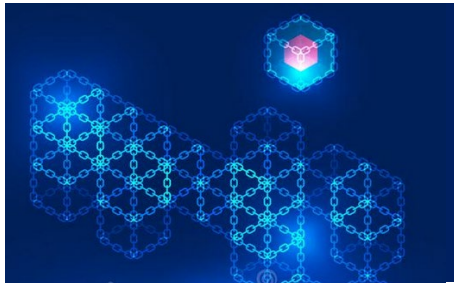
1. Concepts de base





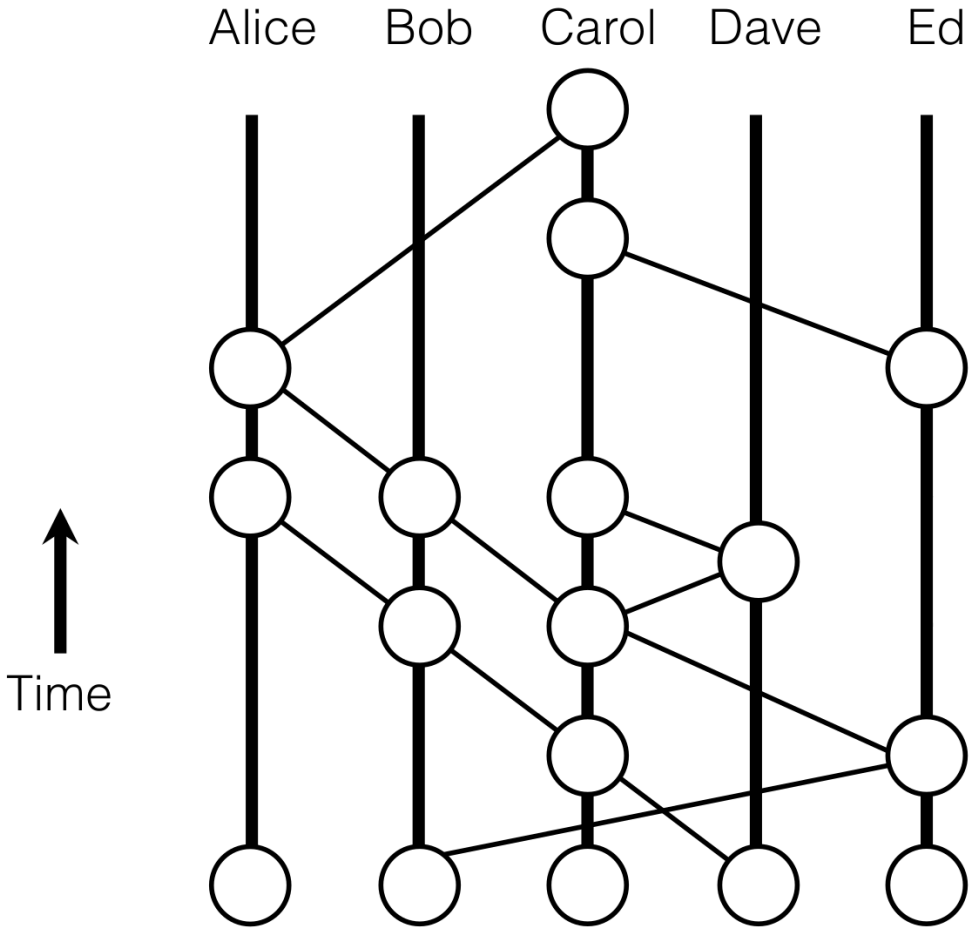
1.1 Biens, registres

- Le registre contient :
  - Transactions : *P* donne *x* à *Q*
  - États : *P* a *n* occurrences de *x*
  - Conditions :
    - Contrat : si <transaction> alors <transaction>
    - Inférences : si <état> alors <état>

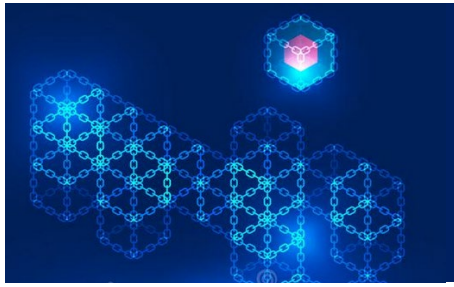


1.2 Registres distribués

« Une technologie basée sur un registre distribué est un système nous permettant de partager des données sans avoir à nous faire nécessairement mutuellement confiance, mais en faisant confiance au groupe lui-même. Ce type de technologie permet de parvenir à un consensus sur l'ordre des transactions et des horodatages. » [Traduction]



https://hackernoon.com/an-overview-of-hashgraph-b0900a1fd7bf



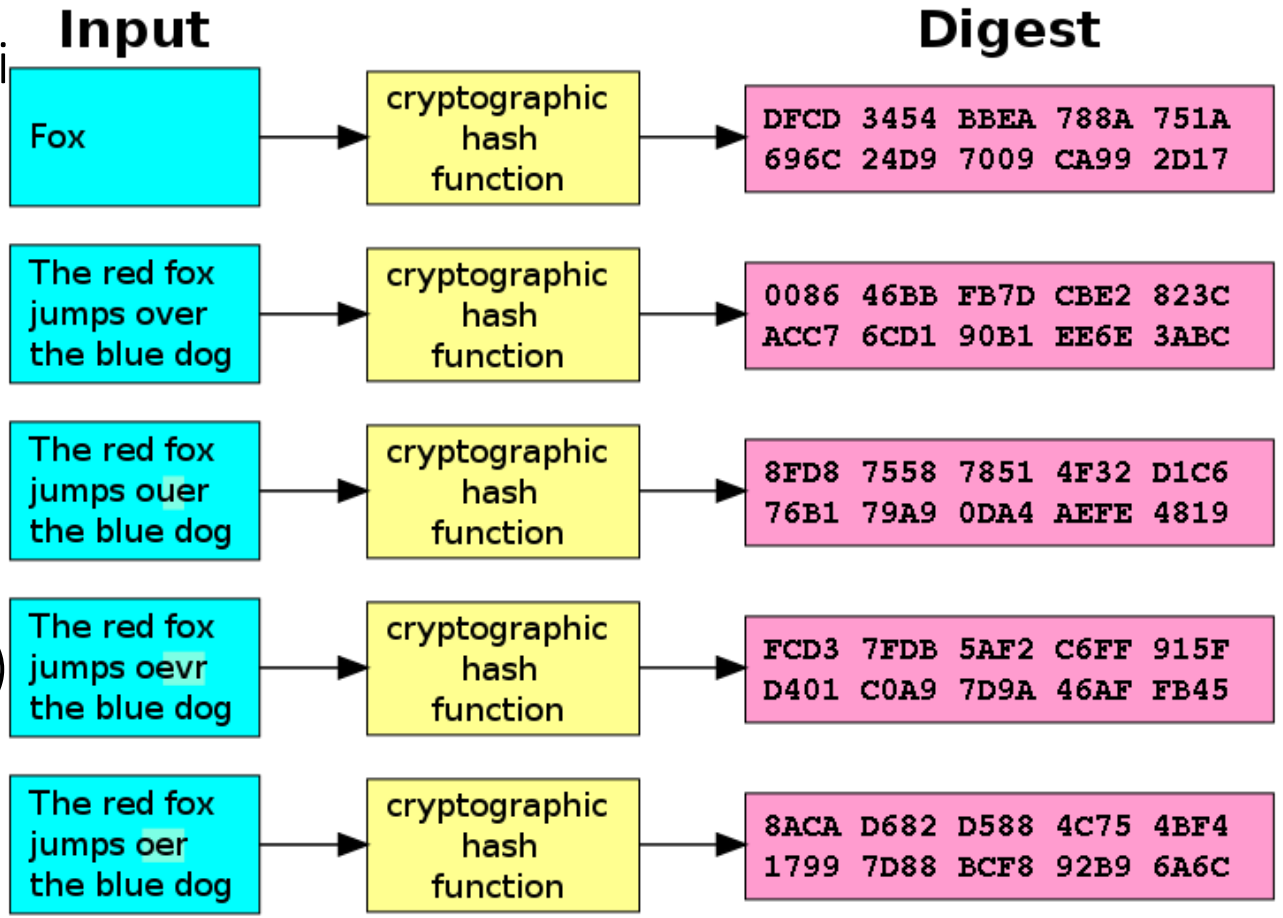
1.3 Fonctions de hachage cryptographique

« Un algorithme mathématique qui associe à un ensemble de données une chaîne de bits de taille fixe (le hachage), et ce de manière non inversible (algorithme à sens unique) » [Traduction].-

Algorithmes:

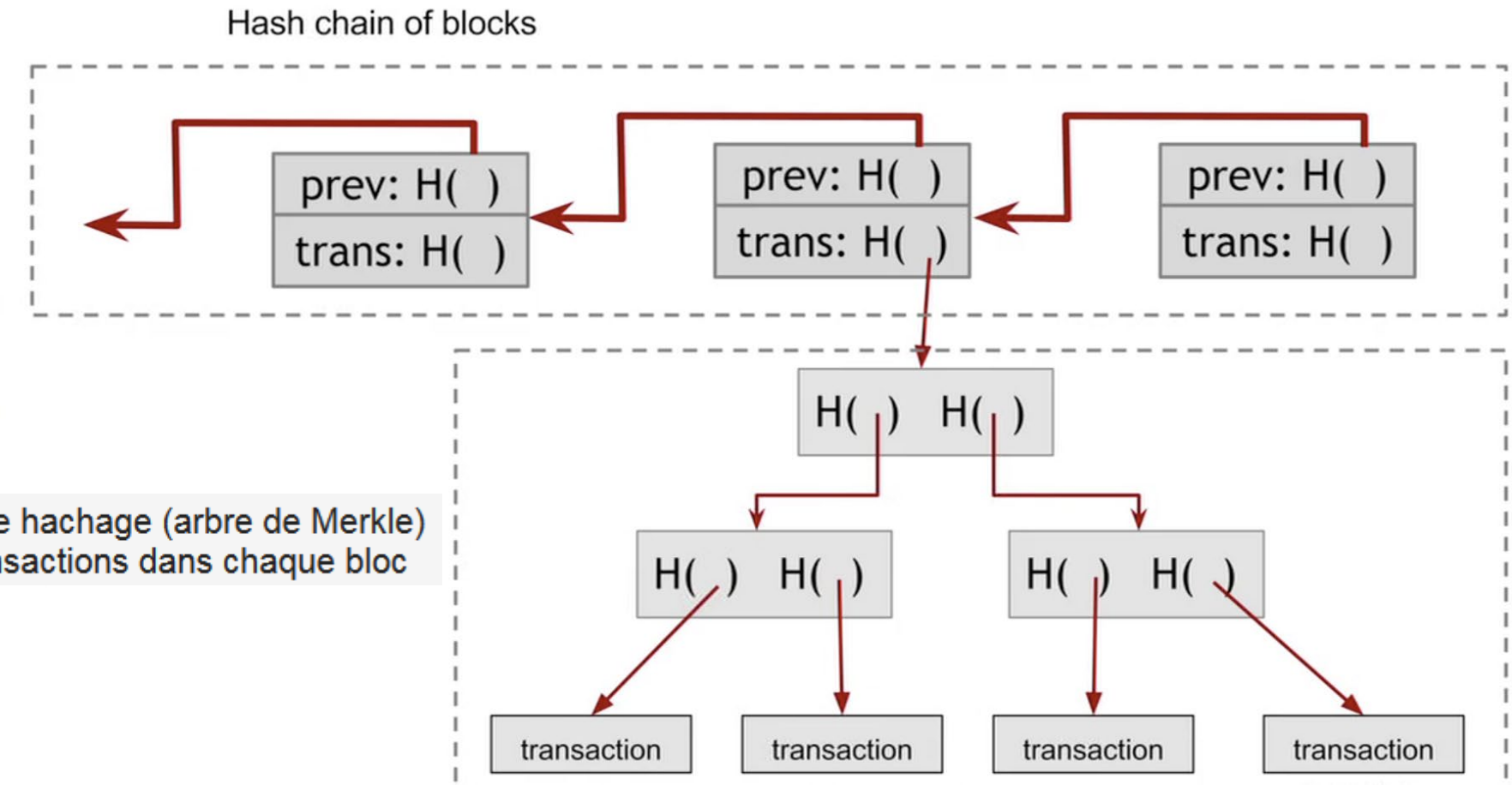
- MD5, SHA1 (non approprié)
- SHA2 (SHA-256 and SHA-512)
- SHA3, BLAKE2

- Signatures



https://en.wikipedia.org/wiki/Cryptographic_hash_function

1.4 Construction d'une chaîne de blocs

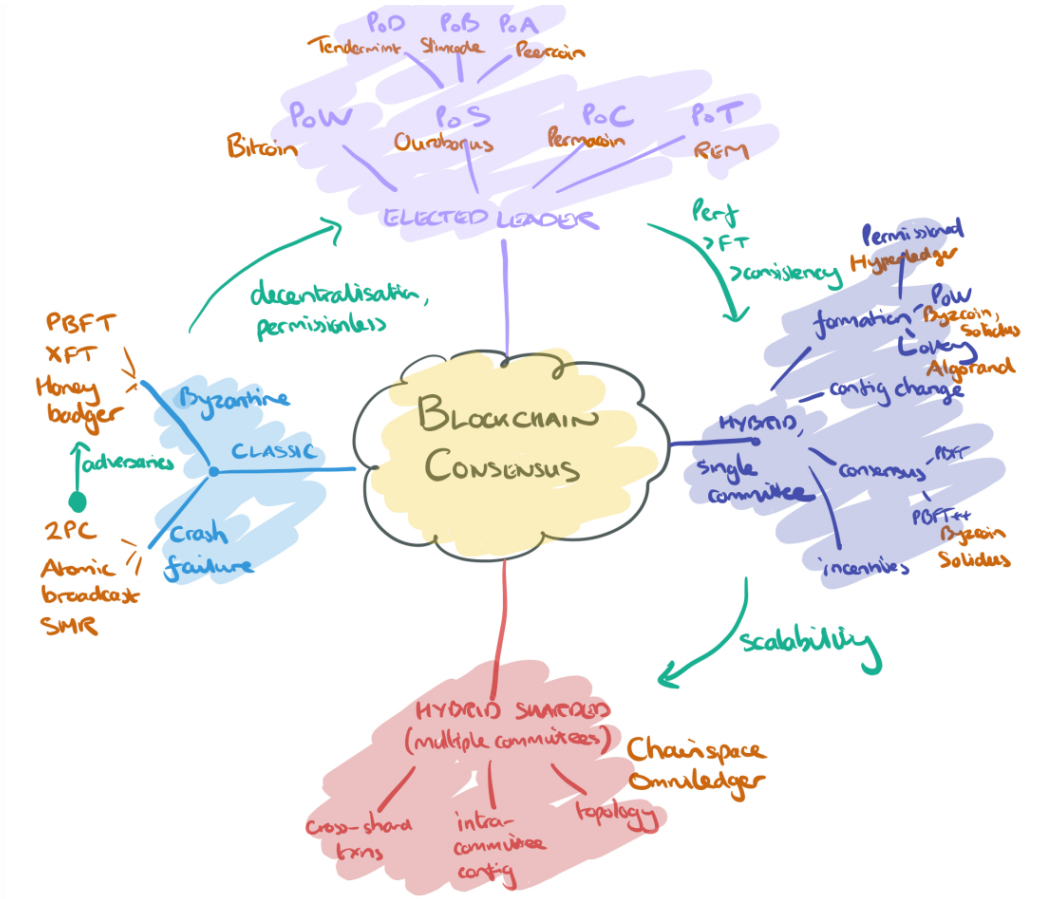


Arbre de hachage (arbre de Merkle) des transactions dans chaque bloc

https://hackernoon.com/how-does-blockchain-technology-work-ceeeee47eaba

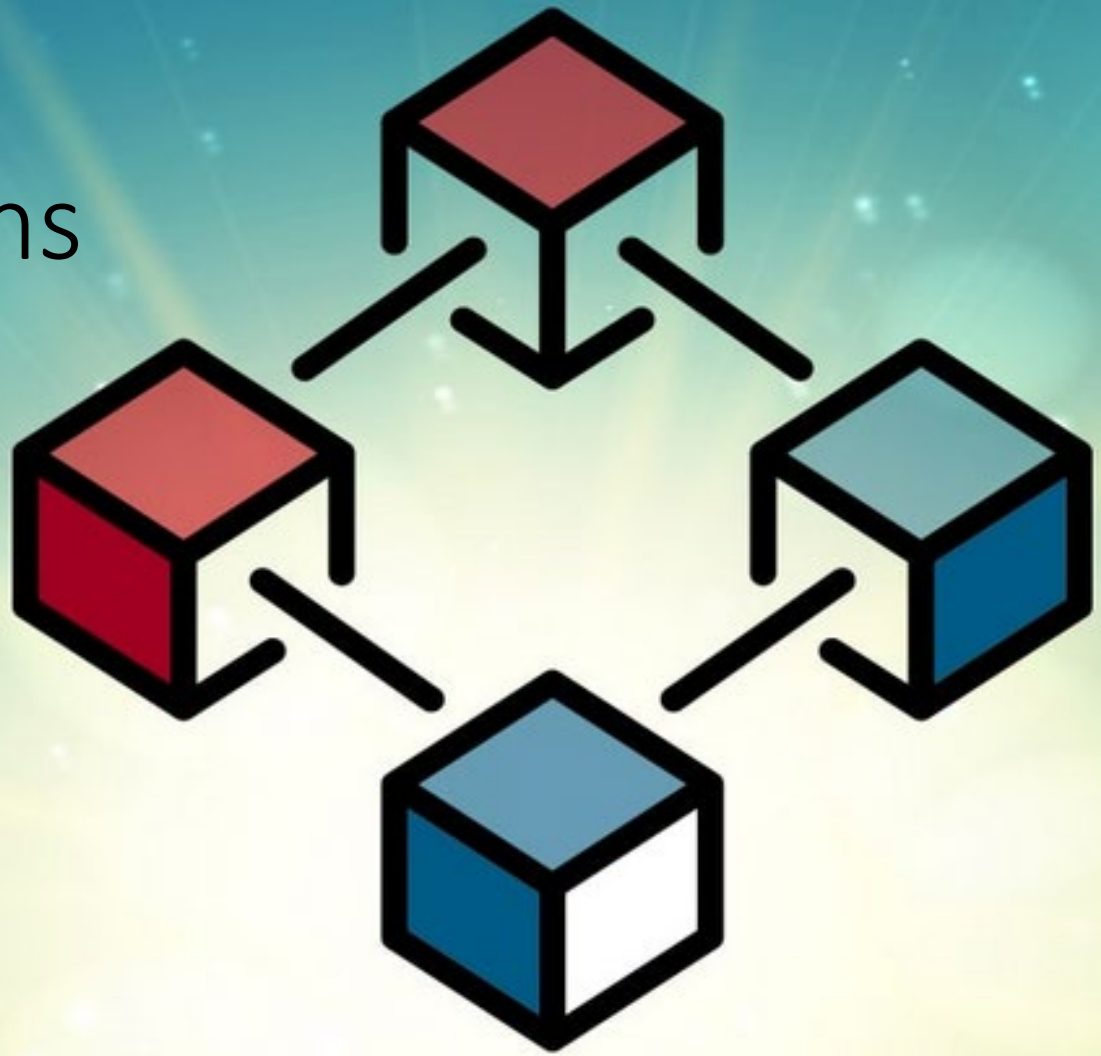
1.5 Consensus

« Le mécanisme le plus connu et le plus souvent mis en œuvre est évidemment la “preuve de travail” (ou consensus de Nakamoto). Des embranchements pouvant se présenter, le consensus de la preuve de travail permet de les discriminer en choisissant celui qui donnera le plus de travail accumulé. » [Traduction]



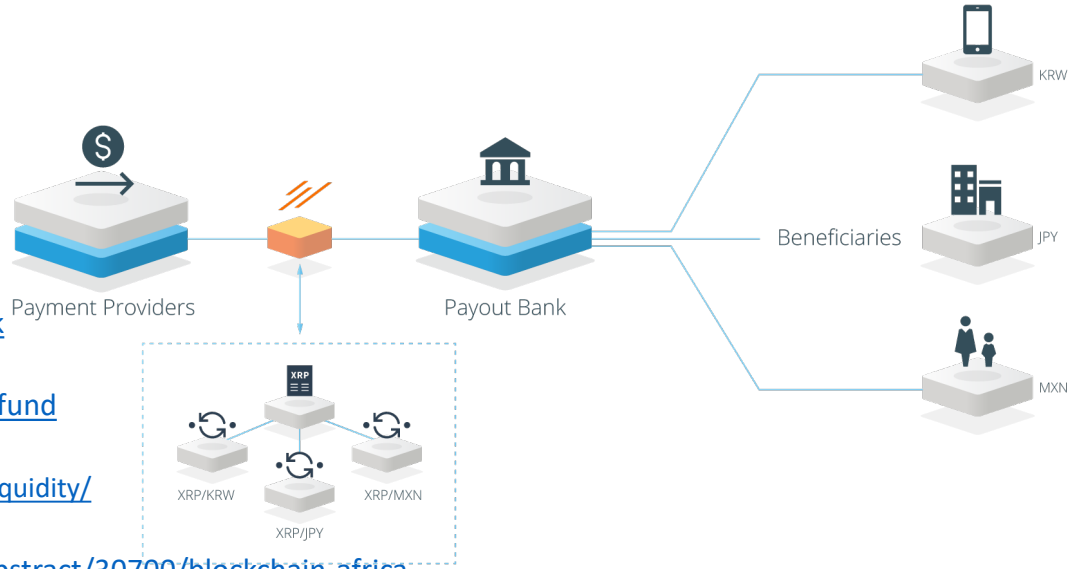
https://blog.acolyer.org/2018/02/12/sok-consensus-in-the-age-of-blockchains/

2. Exemples d’applications



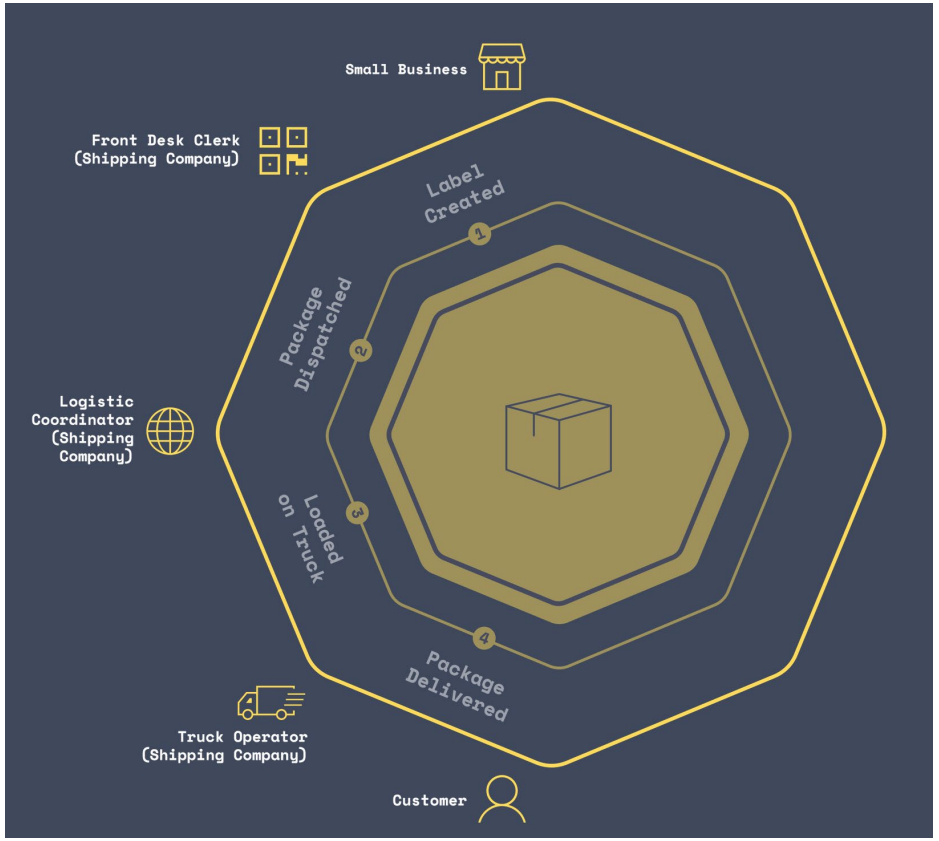
2.1 Monnaie et services financiers

- Paiements
  - Square - https://www.coindesk.com/square-gets-a-bitlicense-new-york-crypto/
- Cartes-cadeaux
  - eGifter, Gyft - https://www.gyft.com/bitcoin/ , https://www.egifter.com/
- Services financiers
  - Banques - https://www.ethnews.com/gmo-internet-group-creates-a-bank
  - Fonds de couverture - https://www.bitwiseinvestments.com/fund
  - Obligations et liquidité - https://ripple.com/solutions/source-liquidity/
  - Financement collectif - https://www.idgconnect.com/blog-abstract/30700/blockchain-africa



2.2 Affaires, audits, conformité

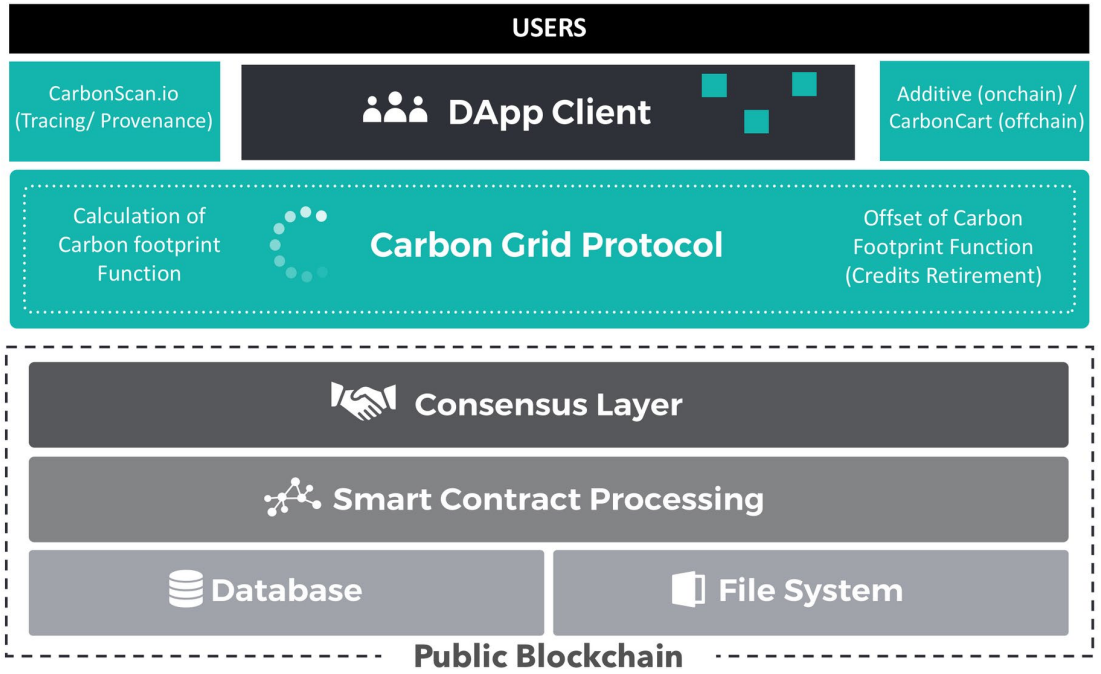
- Loi et contrats - https://agreements.network/
- Marchés - https://techcrunch.com/2017/04/11/bext360-is-using-robots-and-the-blockchain-to-pay-coffee-farmers-fairly/
- Gestion d'actifs - https://www.coindesk.com/td-bank-considers-public-blockchain-for-asset-tracking/
- Chaîne d'approvisionnement - https://peerledger.com/mimosi/ gives companies a trusted, immutable record of all track-and-trace transactions across supply chains, https://viant.io/ Supply chain mgmt. built on Ethereum
- Expédition - 94 organizations have joined blockchain trade platform https://www.reuters.com/article/us-shipping-blockchain-maersk-ibm/maersk-ibm-say-94-organizations-have-joined-blockchain-trade-platform-idUSKBN1KU1LM



https://viant.io/

2.3 Ressources et industrie

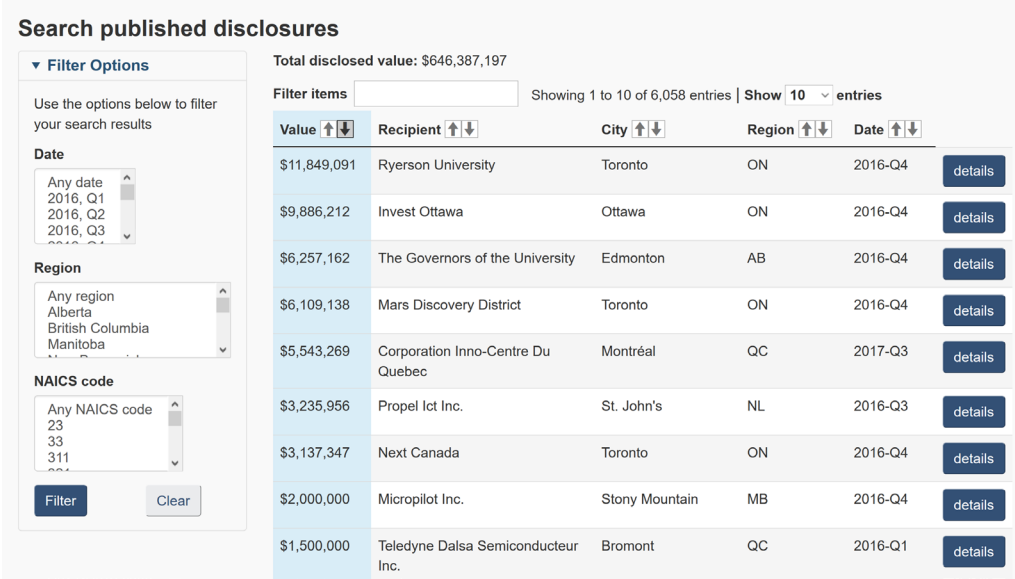
- Agriculture - https://www.cio.com.au/article/644491/cba-helps-ship-17-tonnes-almonds-blockchain/
- Foresterie - blockchain to track the planting of trees worldwide and create rewards for planting trees - https://medium.com/@afhenderson/blockchain-for-social-good-4e6d0d4468d3
- Exploitation minière - https://techcrunch.com/2018/04/26/ibm-introduces-trustchain-a-blockchain-to-verify-the-jewelry-supply-chain/
- Énergie – PowerLedger - https://www.powerledger.io/



https://carbongrid.io/

2.4 Gouvernement, éducation, santé

- Monnaies - https://www.technologyreview.com/s/608910/governments-are-testing-their-own-cryptocurrencies/
- Registres - https://cointelegraph.com/news/netherlands-land-registry-to-test-blockchain-solution-for-real-estate
- Expédition - Le Danemark sera « le premier pays du monde à utiliser une chaîne de blocs pour l'enregistrement des navires dans ses registres d'immatriculation. - https://cointelegraph.com/news/denmark-joins-eu-blockchain-partnership-plans-to-implement-tech-in-shipping
- Données – PARI CNRC – Prototype de publication à l'aide d'une chaîne de blocs - https://nrc-cnrc.explorecatena.com/en/
- Dossiers médicaux - https://cointelegraph.com/news/alibaba-founded-insurtech-firm-promotes-blockchain-use-in-healthcare-industry

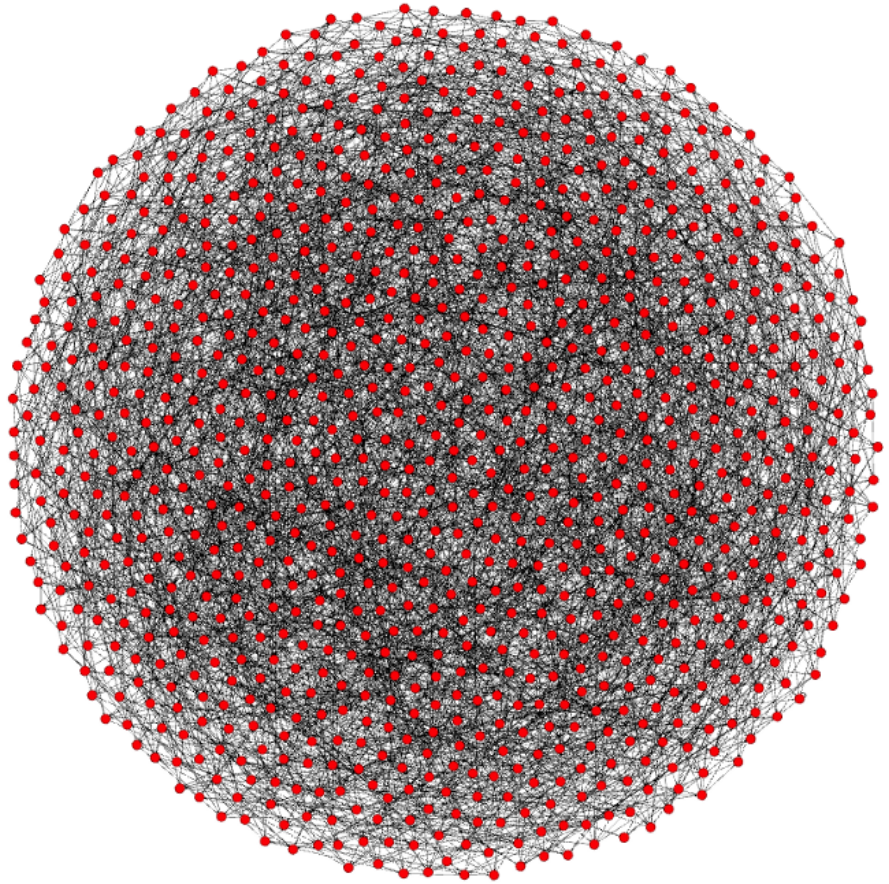


https://nrc-cnrc.explorecatena.com/en/

3. Pièces de monnaie

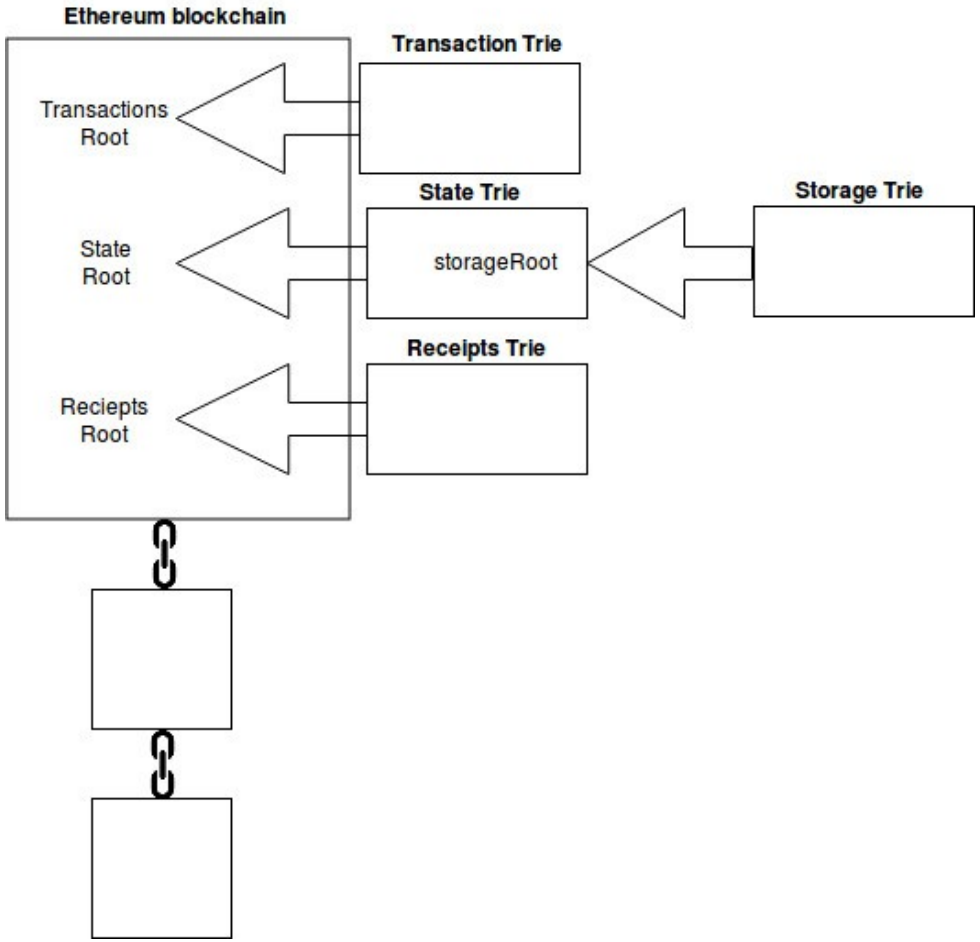
3.1 Bitcoin

- Bitcoin: A Peer-to-Peer Electronic Cash System - Livre blanc par Satoshi Nakamoto - https://bitcoin.org/bitcoin.pdf
- Actuellement : 115 000 nœuds
- Chaque nœud est connecté à 8 autres nœuds
- L'« état » d'un compte Bitcoin est représenté par l'ensemble des sorties de transaction non dépensées (*Unspent Transaction Output,* ou UTXO).
- Lightning - https://lightning.network/
- Le réseau Lightning est un protocole de paiement en « deuxième couche » qui fonctionne par-dessus une chaîne de blocs (la plupart du temps Bitcoin) https://en.wikipedia.org/wiki/Lightning_Network



3.2 Ethereum (et dApps)

- “Bitcoin is the Digital Gold but Ethereum is the Silicon” (Bitcoin, c’est de l’or numérique, mais Ethereum, c’est du silicium) https://medium.com/@Michael_Spencer/bitcoins-glory-days-over-the-future-of-blockchain-5fe303f18537
- Fondateur: Vitalik Buterin - https://github.com/ethereum/wiki/wiki/White-Paper
- Solidity - « Solidity est un langage de programmation conçu pour aider à la rédaction de contrats intelligents.[1] Il est utilisé pour la mise en œuvre de contrats intelligents sur diverses plateformes de chaîne de blocs. » [*Traduction*] https://en.wikipedia.org/wiki/Solidity
- Applications décentralisées (dApps)
  Conçues pour divers secteurs allant des marchés prévisionnels aux jeux, elles vont devenir de plus en plus prépondérantes avec l’amélioration constante du réseau. 1 573 applications à ce jour (4 juin 2018) https://www.stateofthedapps.com/



3.3 Ripple et Stellar

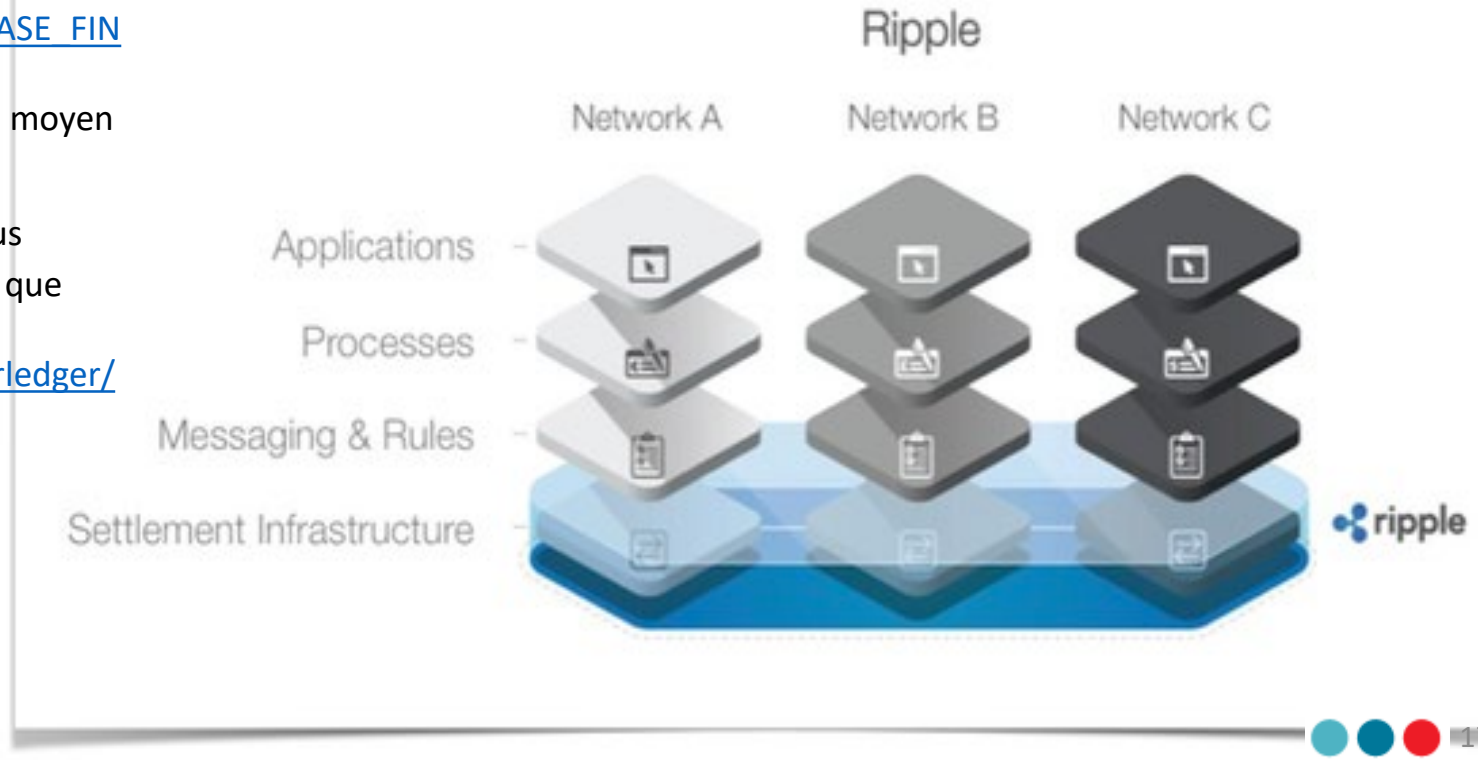
- **Ripple** a un réseau planétaire de banques reliées à sa plateforme. Les banques participantes peuvent effectuer les paiements internationaux dans un délai de trois à cinq secondes au lieu de quelques jours, explique la société . https://www.therecord.com/news-story/8653190-uw-gets-research-funding-for-deep-dive-into-blockchain-technology/

- il remplacera SWIFT en tant que fournisseur mondial de services de messagerie financière sécurisée http://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf
- Un prochain produit (xRapid) utilisera le XRP comme moyen de «trouver de la liquidité»

- **Interledger** est le protocole qui se trouve sous RippleNet. Il est en cours de développement en tant que norme Web potentielle sous le W3C - https://w3c.github.io/webpayments/proposals/interledger/

- **Stellar**

- Ripple décentralisé, collaboration avec IBM



3.4 Portefeuilles, échanges, réseaux

- Échanges
  - Centralisés – Coinbase https://blog.coinbase.com/ , Binan - https://www.binance.com/
  - Décentralisés – Altcoin - https://altcoin.io/ , IDEX - https://idex.market/eth/aura
- Réseaux
  - *Towards a Design Philosophy for Interoperable Blockchain Systems*, Thomas Hardjono, Alexander Lipton, Alex Pentland https://arxiv.org/abs/1805.05934
- Portefeuilles
  - « Ce que vous conservez dans votre portefeuille, c'est la clé privée qui est utilisée pour accéder à vos pièces de monnaie (dépense/transfert). » [Traduction] https://cryptocurrencyhub.io/i-bought-my-first-bitcoin-now-what-fdf7dc9ad150

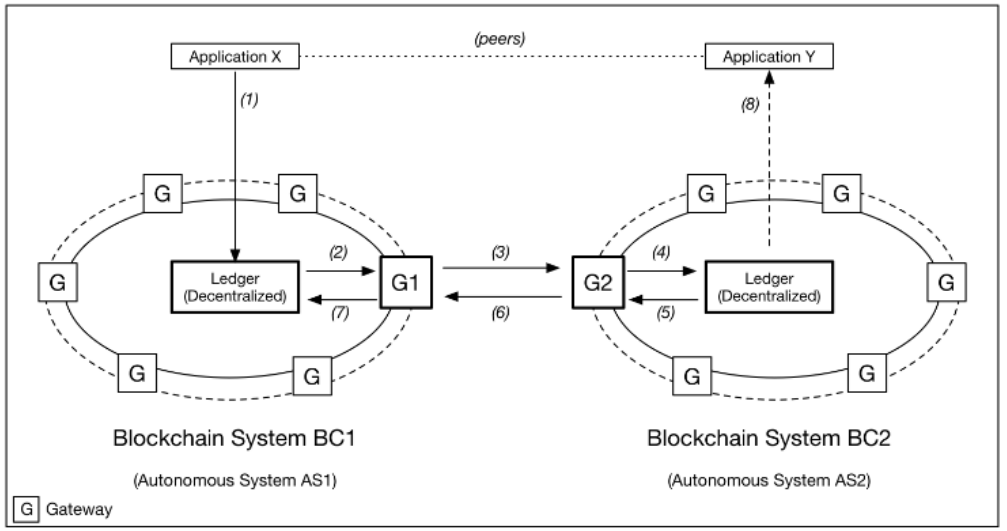
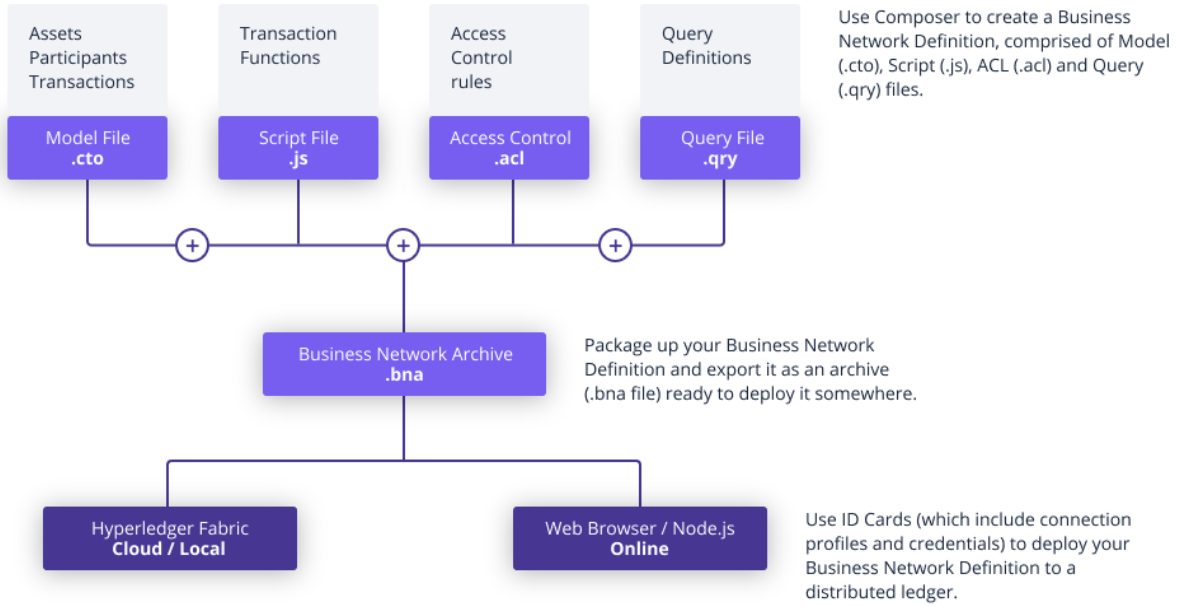


Figure 5: Set of Gateways for Reachability and Transaction Mediation

4. Plateformes et services

4.1 Hyperledger Fabric

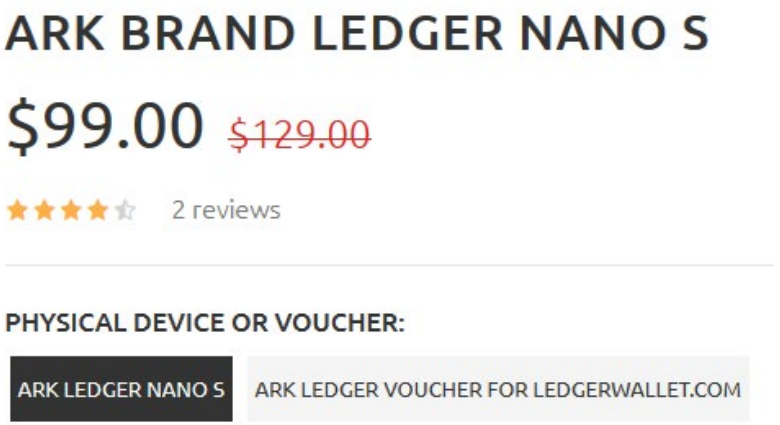
- Réseaux d'entreprises privées, hébergement sur l'infrastructure Bluemix d'IBM, ou sur conteneurs Docker
- Favorise une gouvernance, des normes et un code source ouverts
- Définition du réseau d'entreprise
  - un ensemble de fichiers modèles
  - un ensemble de fichiers JavaScript
  - un fichier de contrôle d'accès



https://www.hyperledger.org/projects/fabric

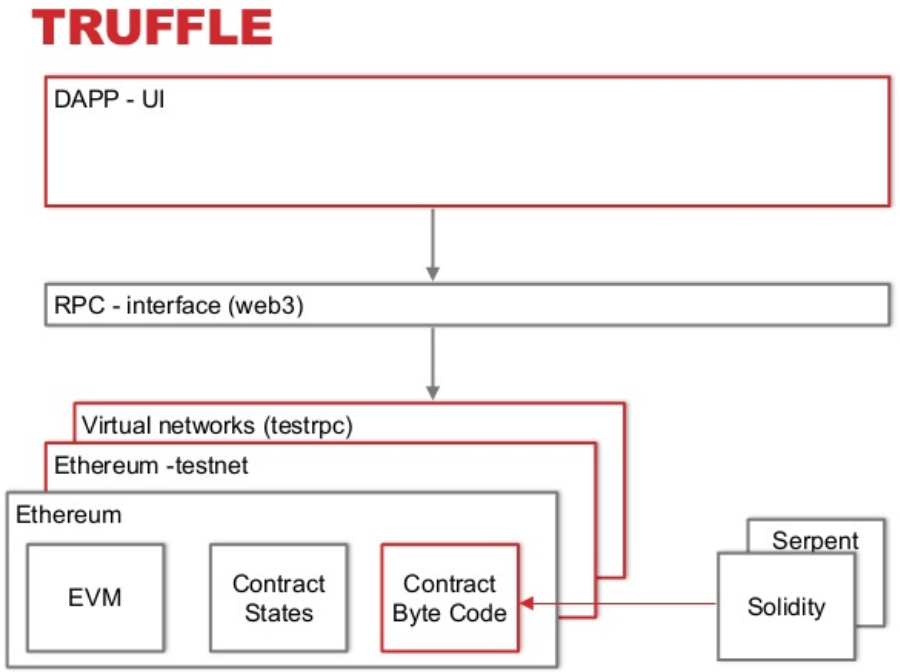
4.2 Ark

- ARK, une plateforme sécurisée conçue pour une adoption de masse, «offrira les services que les consommateurs désirent et dont les développeurs ont besoin. » https://ark.io/ - explorer: https://explorer.ark.io/
- Ark! Le Wordpress de la crypto! https://decentralize.today/some-great-projects-are-out-there-they-just-dont-talk-about-them-21d677e29ecf
- Le portefeuille de bureau ARK est compatible avec le logiciel de portefeuille sécurisé Ledger Nano S.



4.3 Truffle (exemple du CNRC)

- un cadre de développement pour Ethereum - http://truffleframework.com/
  - Truffle prend en charge la gestion des fichiers (*artifacts*) relatifs à vos contrats pour vous épargner cette tâche.
  - Ganache - https://truffleframework.com/ganache - une chaîne de blocs accessible en un seul clic
  - Drizzle- Un ensemble de bibliothèques frontales qui facilite le codage des interfaces utilisateurs et rend celles-ci plus prévisibles.



https://www.slideshare.net/MartinKppelmann/build-dapps-13-dev-tools

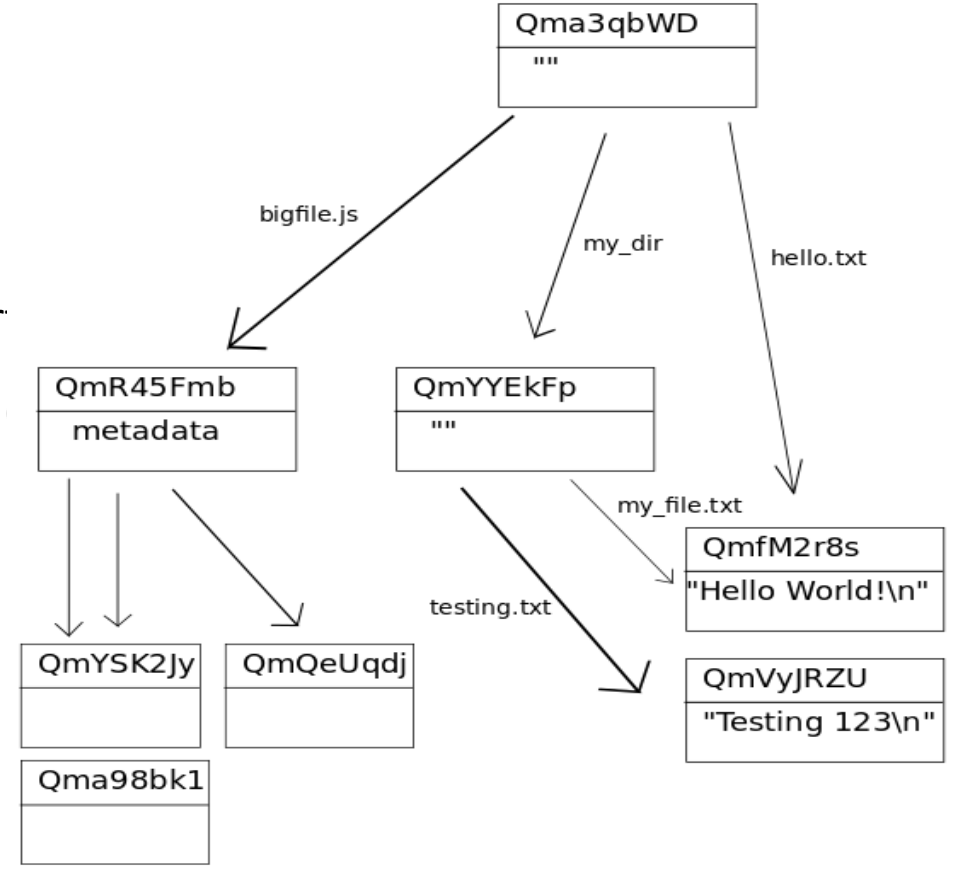
4.4 IPFS / IPLD

IPFS papier blanc: [IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3)](#).

- IPFS est constitué d'un réseau de nœuds pair-à-pair (des ordinateurs capables de communiquer directement entre eux)
- Ces nœuds peuvent stocker du contenu (des fichiers de n'importe quel type)
- Le contenu est référencé à l'aide d'un hachage et est immuable (si le contenu est modifié, son hachage le sera aussi). Dans le cas d'IPFS, la clé donnant accès à la table de hachage distribuée est un hachage dérivé du contenu.

Hosting a website on IPFS - https://ipfs.io/ipfs/QmdPtC3T7Kcu9iJg6hYzLBWR5XCDcYMY7HV685E3kH3EcS/2015/09/15/hosting-a-website-on-ipfs/

- IPLD - Inter Planetary Linked Data
- Site Web d'IPLD : - https://ipld.io/
- Les spécifications d'IPLD et les mises en œuvre d'IPLD.

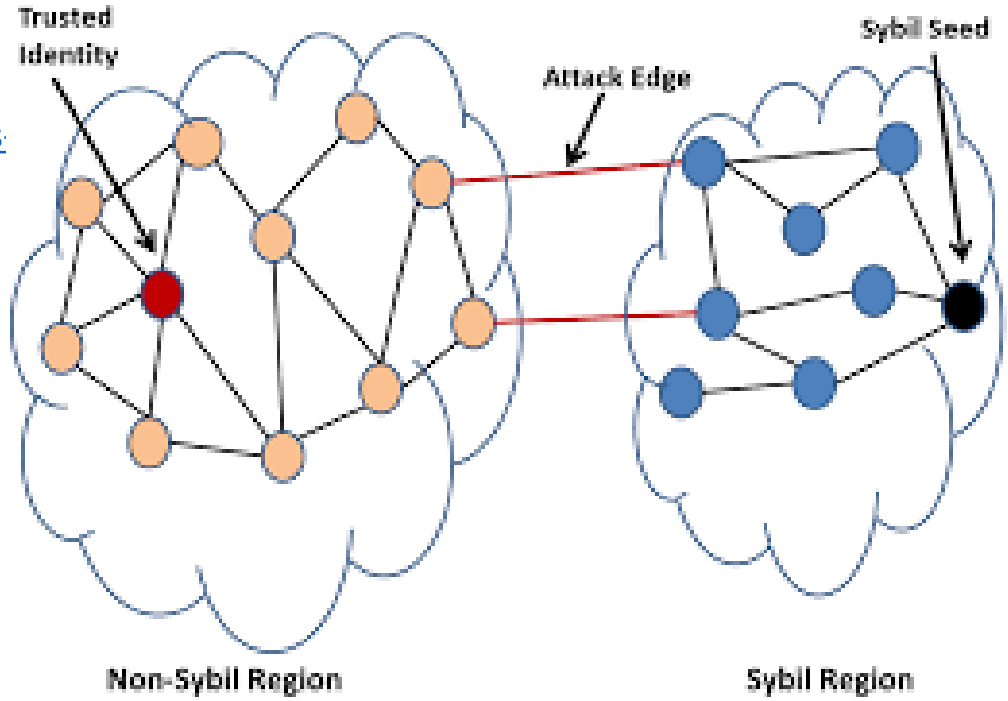


https://whatdoesthequantsay.com/2015/09/13/ipfs-introduction-by-example

5. Quelques problèmes

5.1 Conceptual Issues

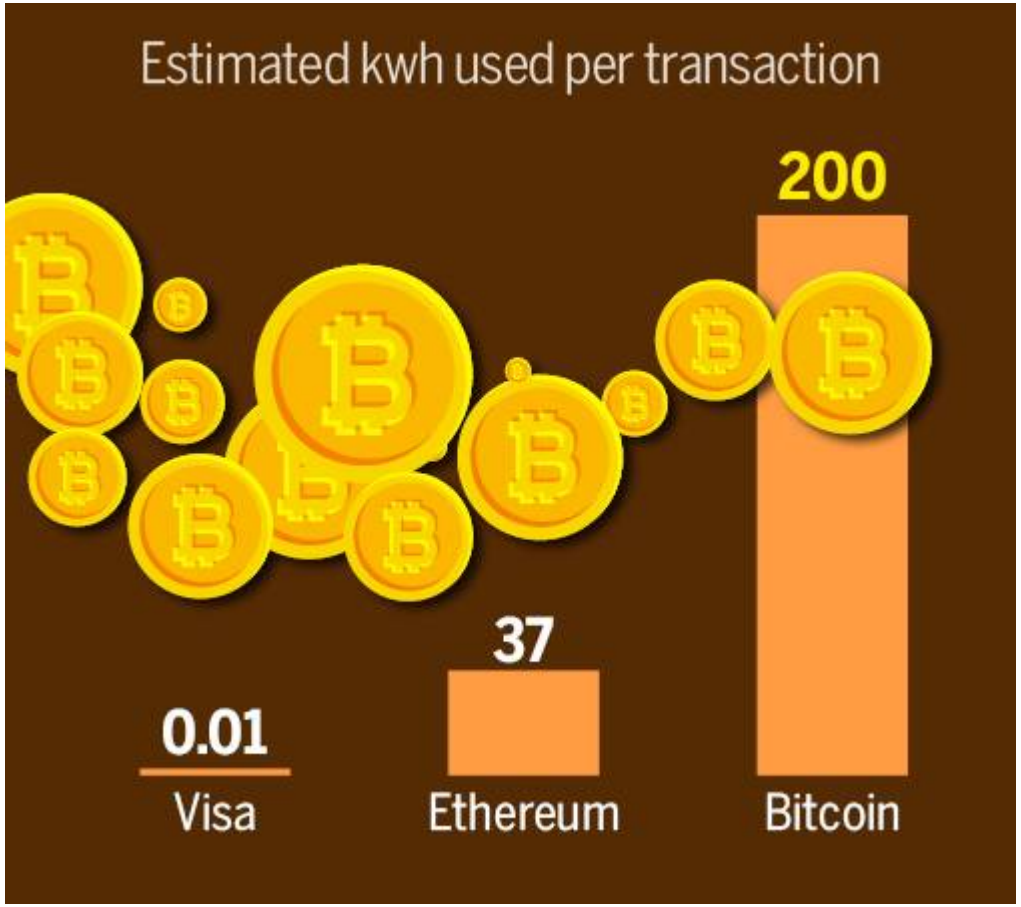
- Où se trouve la valeur : protocoles, applications décentralisées ou portefeuilles?
  - https://medium.com/lightspeed-venture-partners/fat-protocols-vs-fat-dapps-vs-fat-wallets-4d33ead29130
- Incitatifs économiques et le problème du « rien à perdre » (*Nothing at Stake*)
  - https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb
- Immuabilité (et le cadre général de protection des données)



https://pdfs.semanticscholar.org/30e4/1ec151d1499b580155be4dee168530d80145.pdf

5.2 Coût et consommation d'énergie

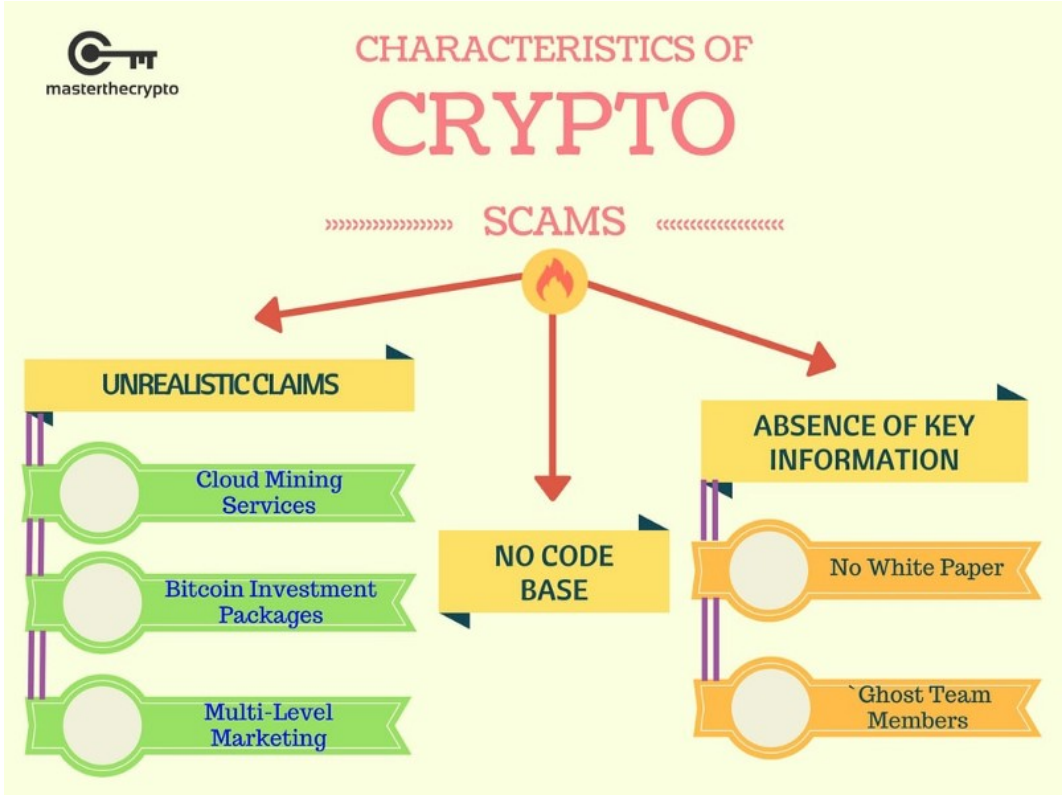
- Fiabilité des logiciels
- Consommation d'énergie
  - Le système Bitcoin consomme plus d'énergie que 6 millions de foyers.
  - Il consomme actuellement l'équivalent de 10 % de la consommation totale d'énergie au Canada.
  - 1 transaction en bitcoins coûte plus que 100 000 transactions via le système Visa.
- Problème d'échelle - Bitcoin 7 tx/s, Ethereum 50 tx/s Visa's 24,000 tx/s.
  https://medium.com/thunderofficial/2018-blockchain-scaling-all-else-7937b660c08



https://www.businesstoday.in/top-story/bitcoins-now-an-energy-guzzler/story/266310.html

5.3 Enjeux sociaux et éthiques

- Distribution des jetons et inégalité
- Réglementation et fiscalité
  - https://medium.com/forbes/tax-trouble-for-certain-bitcoin-traders-41414e4d47a8
- Défaillances du marché, culture libertaire
- Escroqueries et fraudes
  - Fausses ICO (offres initiales de pièces)
  - Manipulation du marché
  - Combines à la Ponzi
- Cybersécurité



https://medium.com/@bdaqio/top-10-stay-away-ico-directions-in-2018-117973fe8a66