NRC·CNRC

NRC.CANADA.CA

Distributed Ledger Technologies like Blockchain…looking under the hood

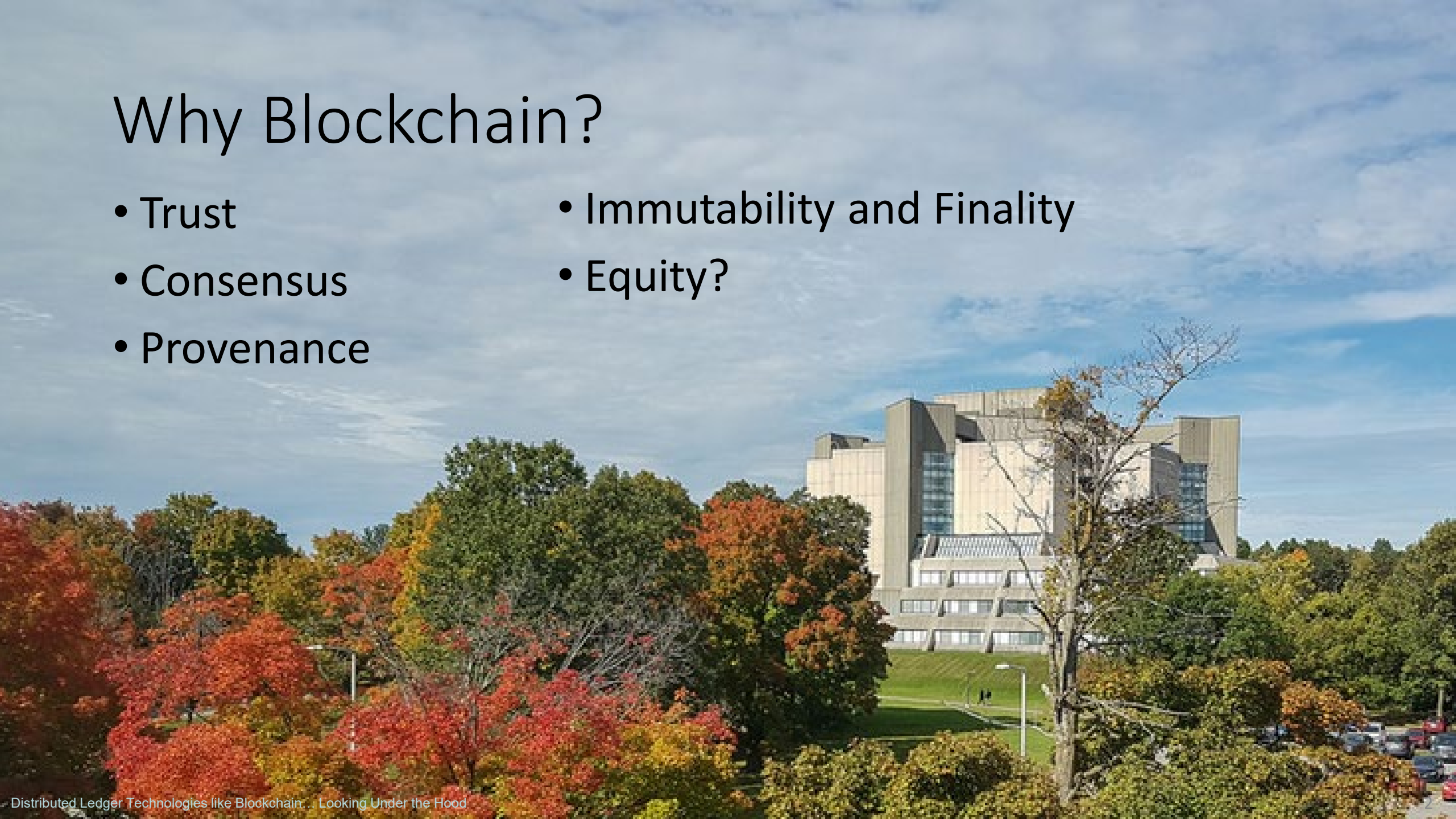
Stephen Downes

Digital Technologies Research Centre

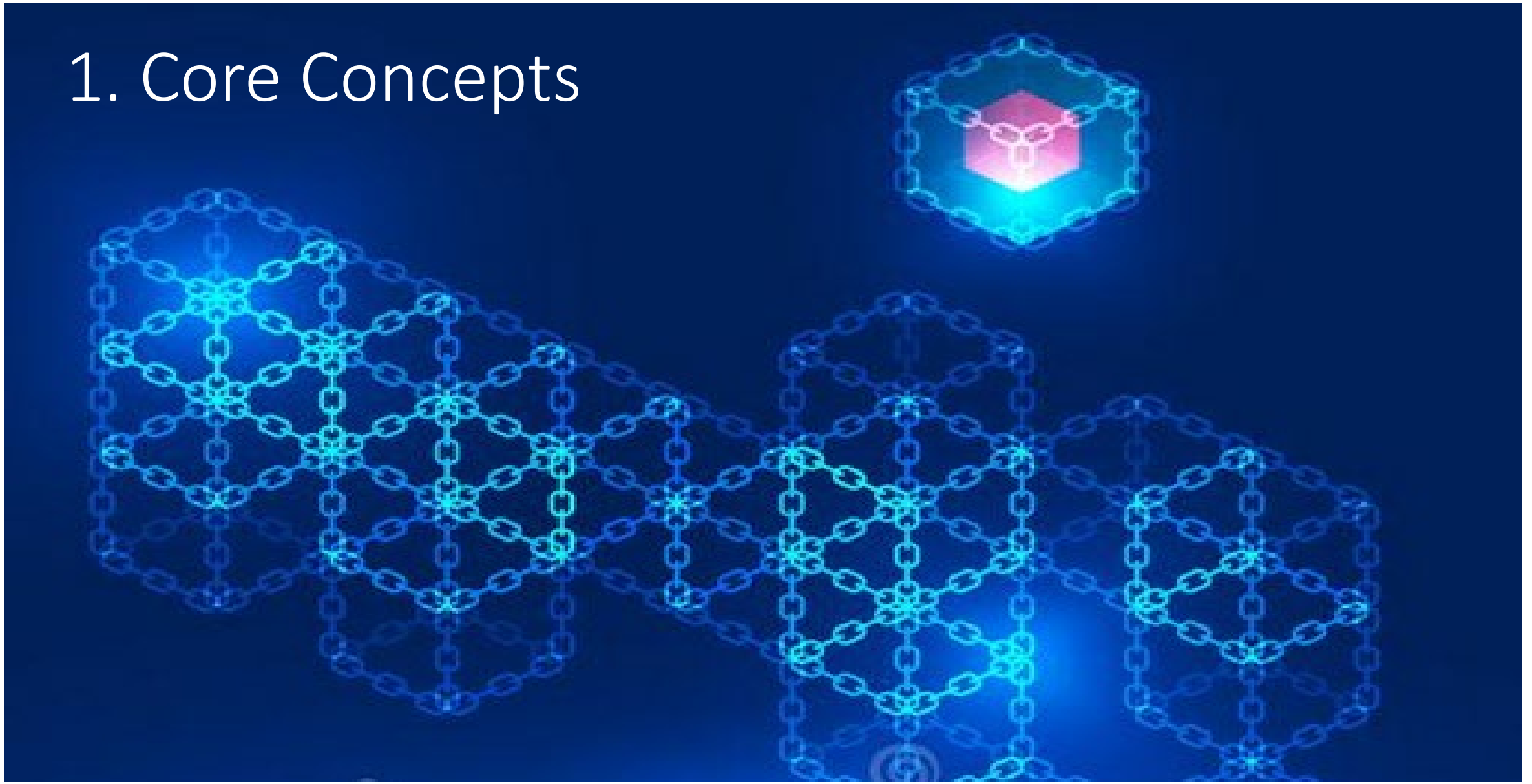
November 23, 2018

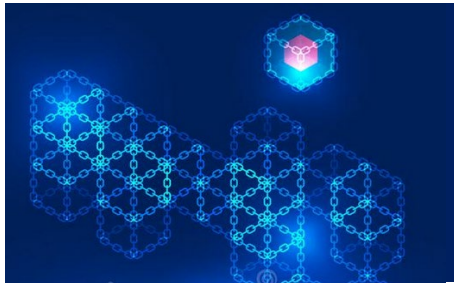
Why Blockchain?

- Trust
- Consensus
- Provenance
- Immutability and Finality
- Equity?



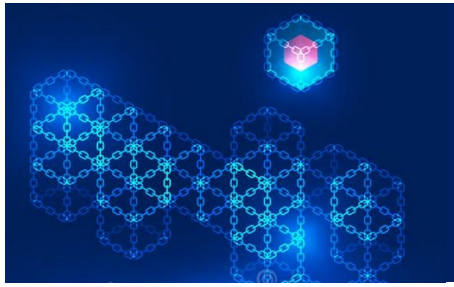
1. Core Concepts





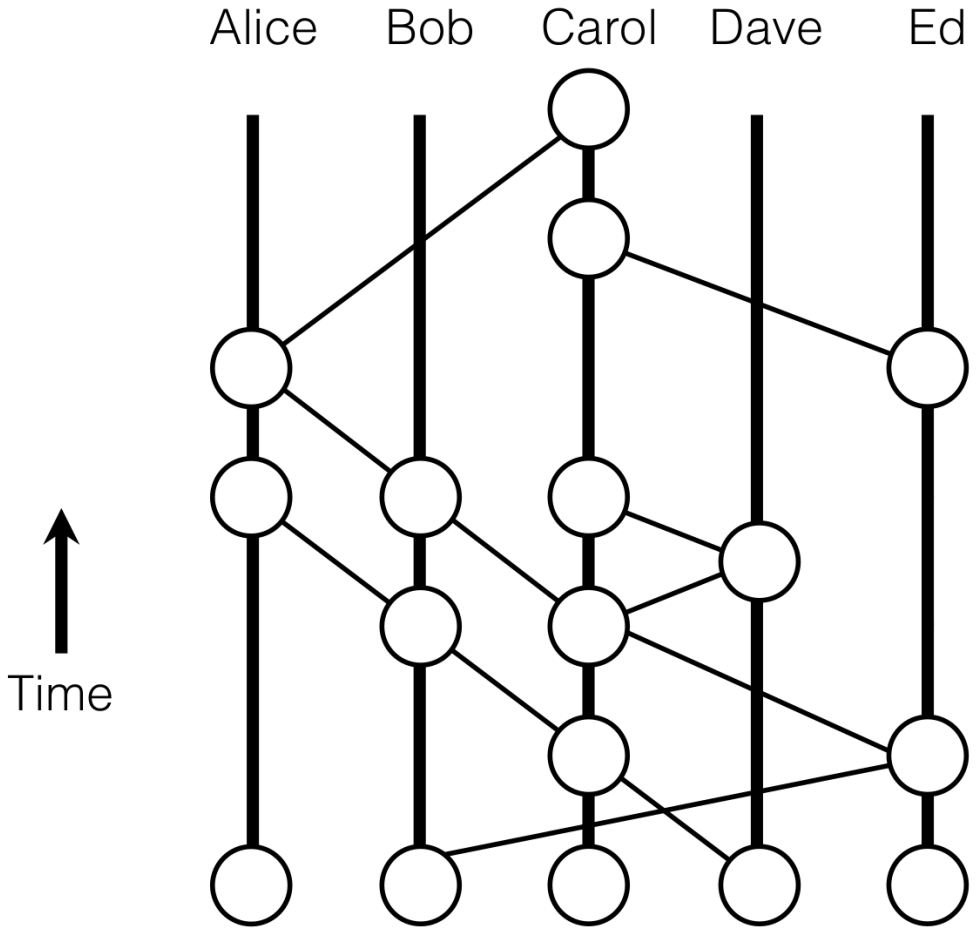
1.1 Assets, Ledgers

- Ledger contents include:
  - Transactions: P gives x to Q
  - States: P has n instances of x
  - Conditions:
    - Contract: if <transaction> then <transaction>
    - Inferences: if <state> then <state>

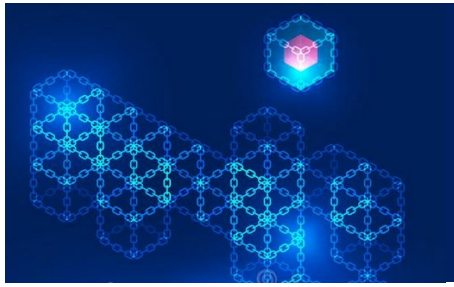


1.2 Distributed Ledgers

"A distributed ledger technology (DLT) is a system where we share information and we don't trust each other individually, but we trust the group as a whole. DLTs allow us to come up with a consensus on the order of transactions and timestamps."



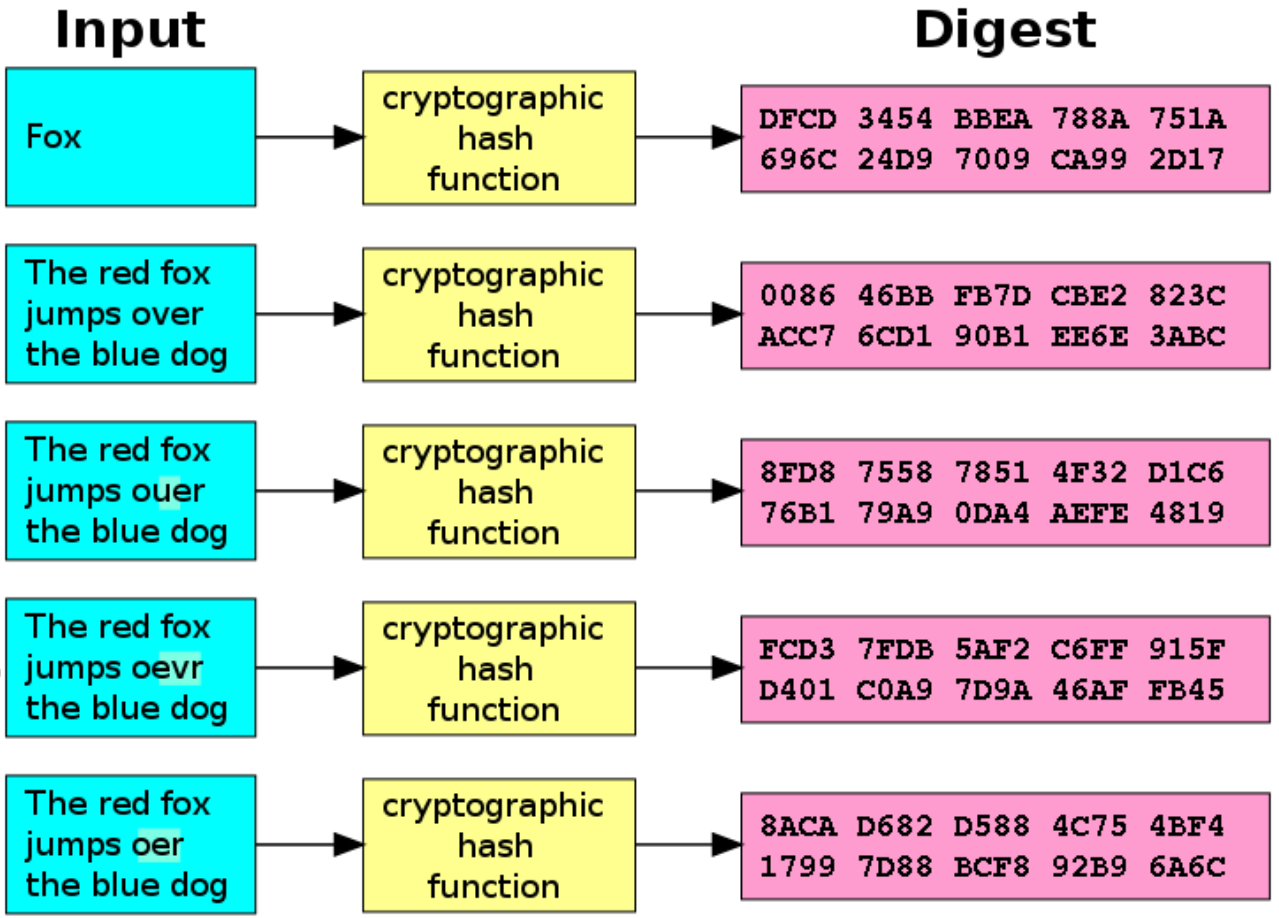
https://hackernoon.com/an-overview-of-hashgraph-b0900a1fd7bf



1.3 Cryptographic Hash Functions

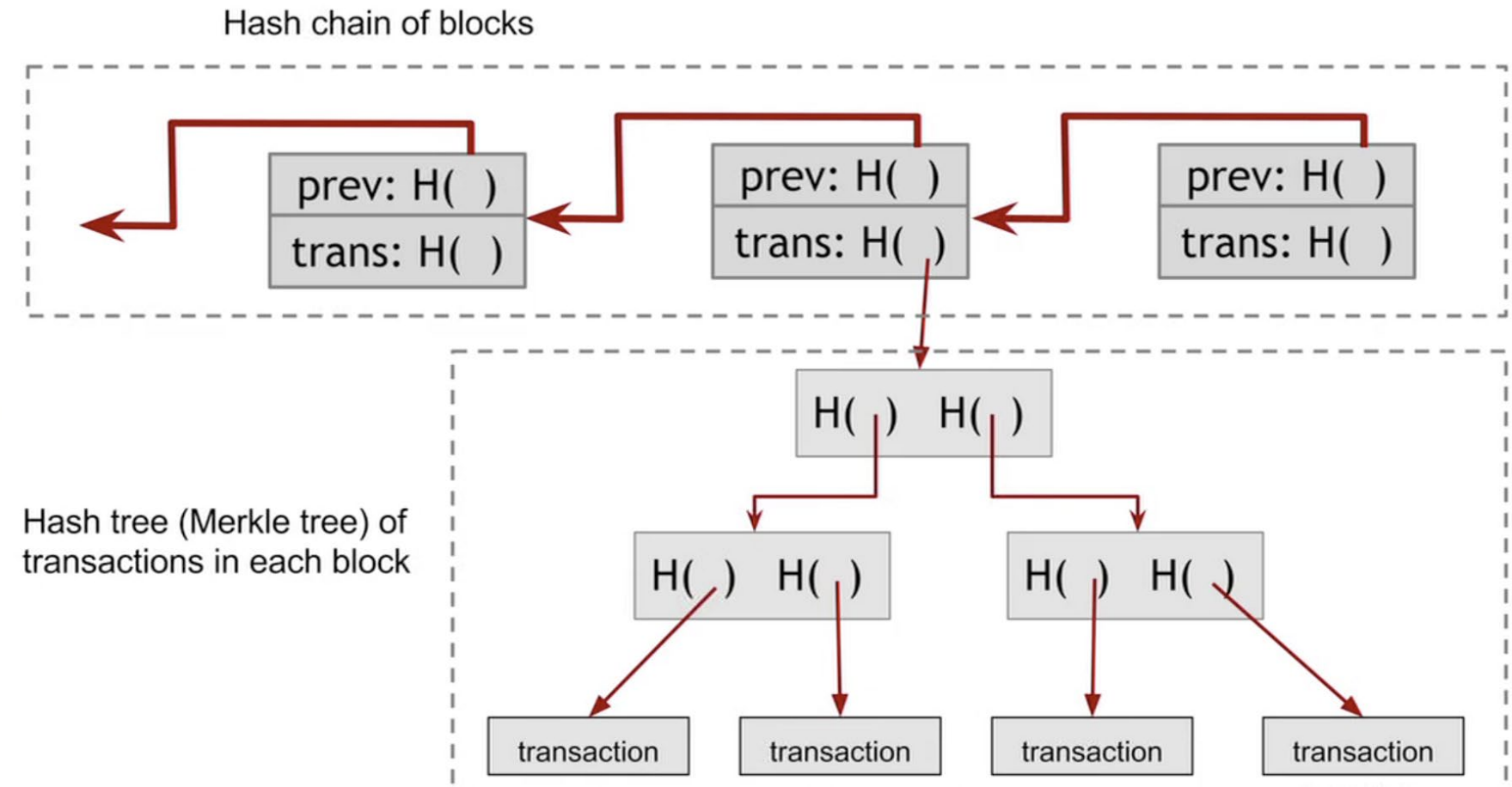
"a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash) and is designed to be a one-way function.."

- Algorithms:
  - MD5, SHA1 (unsuitable)
  - SHA2 (SHA-256 and SHA-512)
  - SHA3, BLAKE2
- Signatures



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

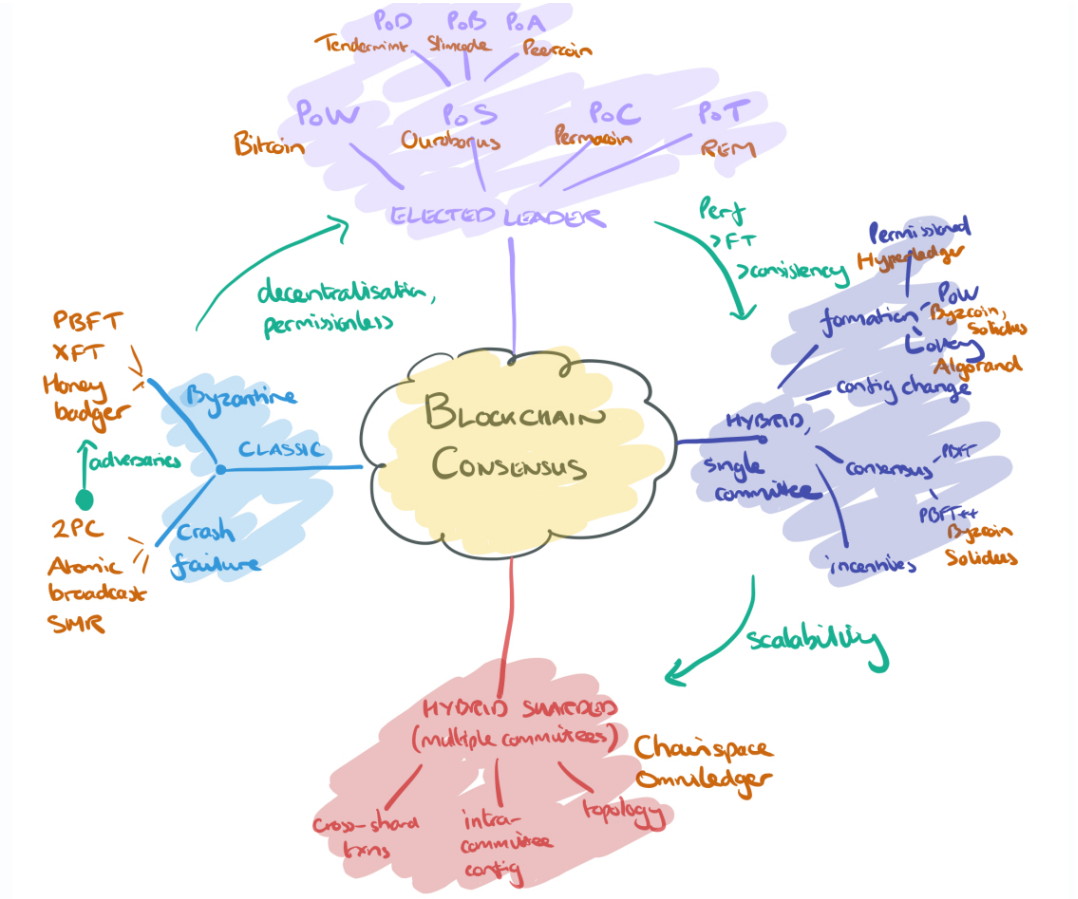
1.4 Construction of a Blockchain



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

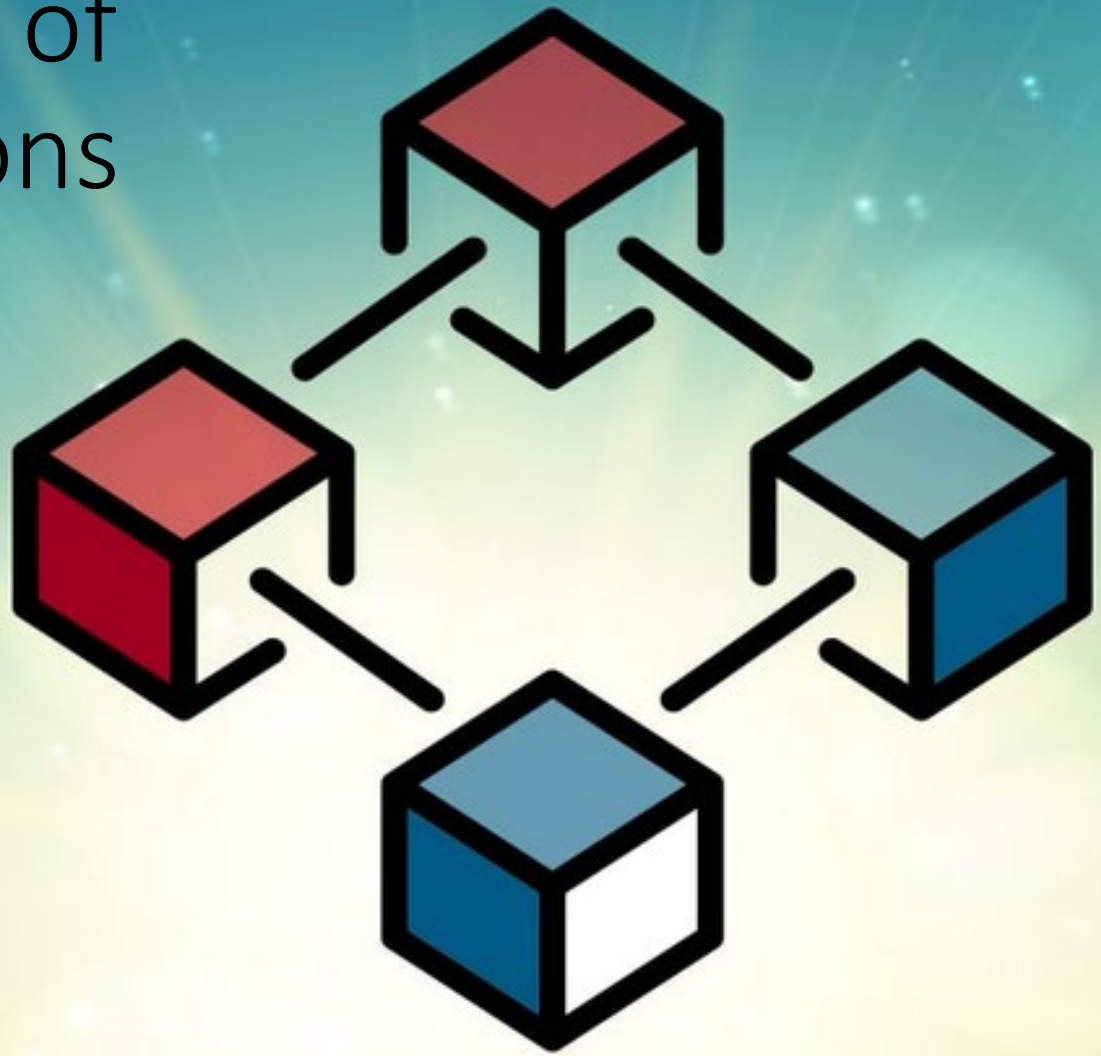
1.5 Consensus

"The best known and most widely deployed mechanism is of course proof-of-work (aka. Nakamoto consensus). Forks can occur, and are resolved by PoW consensus, which amounts to picking the chain with the most accumulated work."



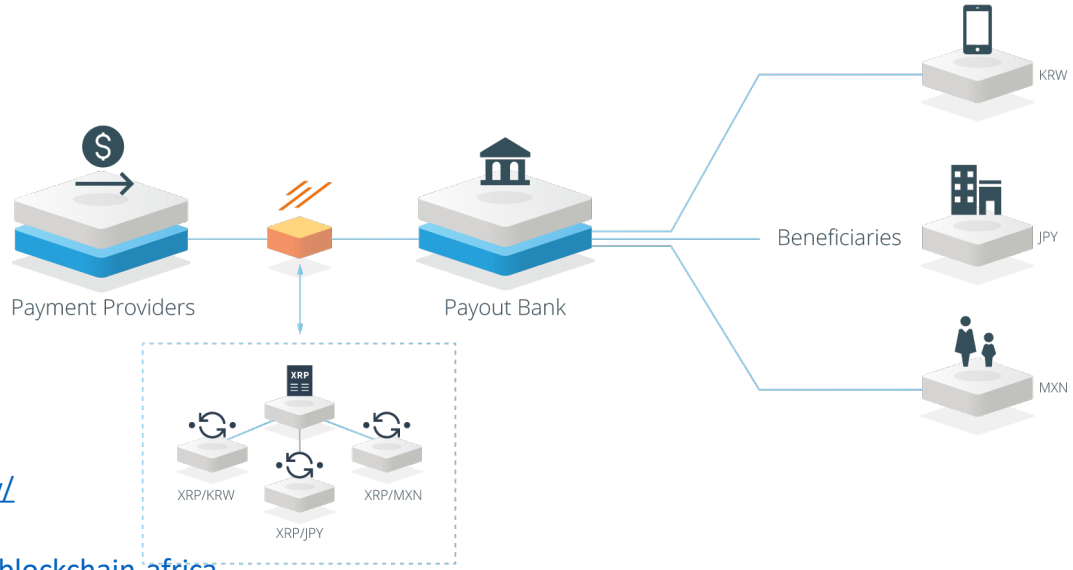
https://blog.acolyer.org/2018/02/12/sok-consensus-in-the-age-of-blockchains/

2. Examples of Applications



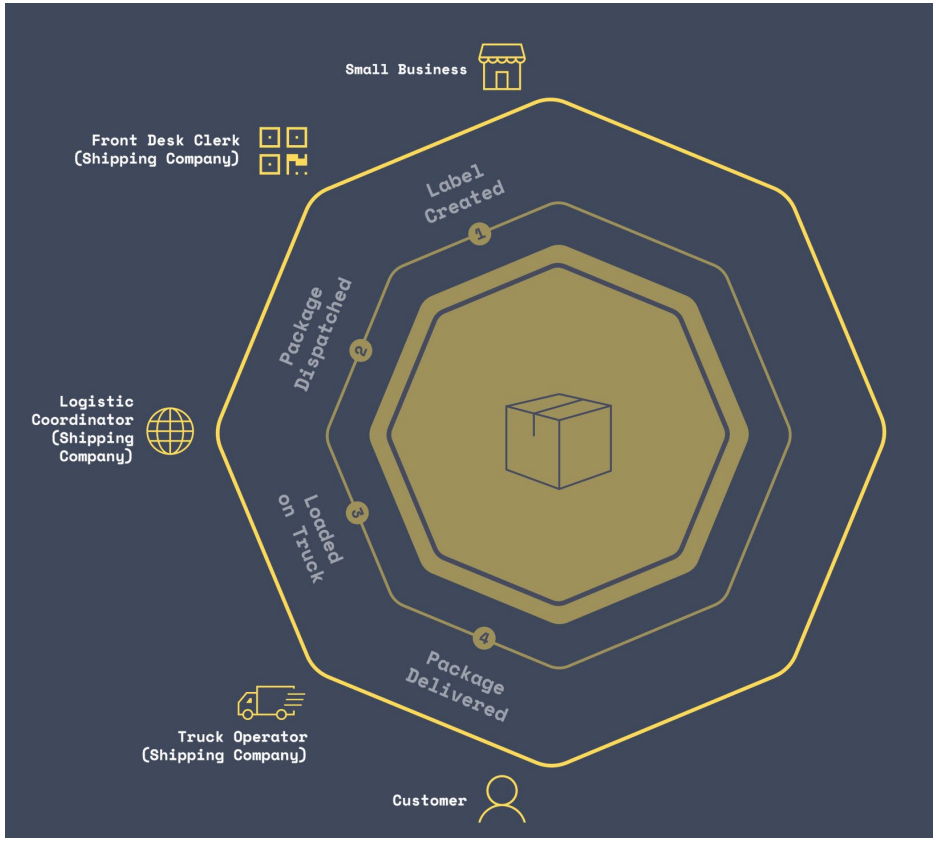
2.1 Currency and Financial

- Payments
  - Square - https://www.coindesk.com/square-gets-a-bitlicense-new-york-crypto/
- Gift Cards
  - eGifter, Gyft - https://www.gyft.com/bitcoin/ , https://www.egifter.com/
- Financial services
  - Banks - https://www.ethnews.com/gmo-internet-group-creates-a-bank
  - Hedge Funds - https://www.bitwiseinvestments.com/fund
  - Bonds and Liquidity - https://ripple.com/solutions/source-liquidity/
  - Crowdfunding - https://www.idgconnect.com/blog-abstract/30700/blockchain-africa



2.2 Business, Audit, Compliance

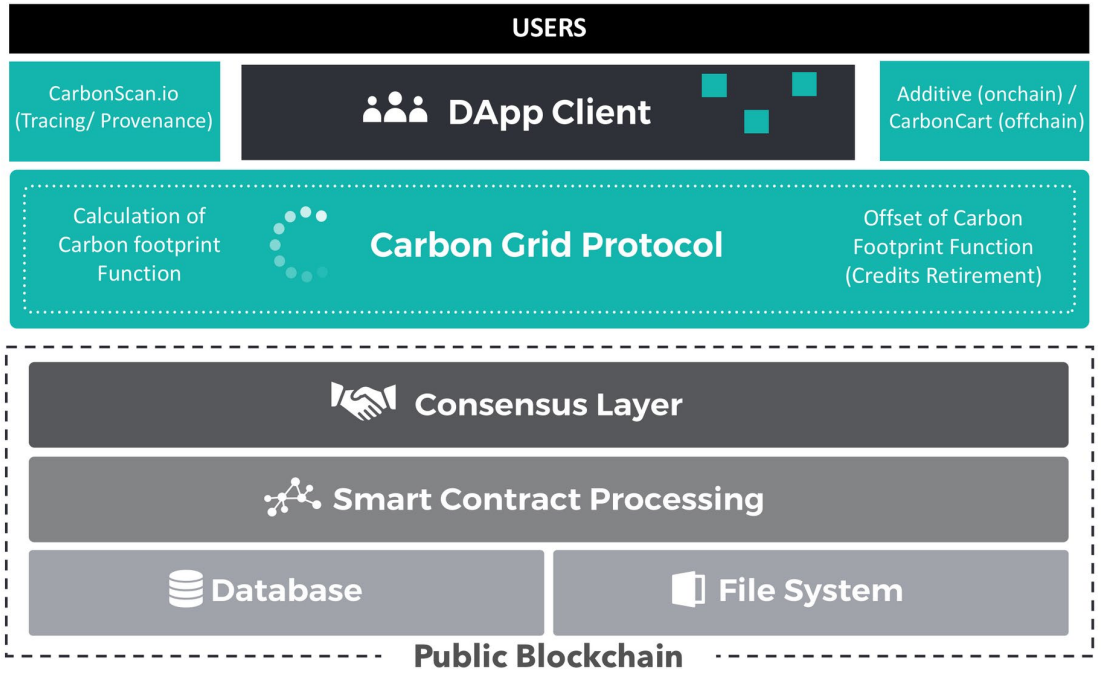
- Law and contracts - https://agreements.network/
- Markets - https://techcrunch.com/2017/04/11/bext360-is-using-robots-and-the-blockchain-to-pay-coffee-farmers-fairly/
- Asset Management - https://www.coindesk.com/td-bank-considers-public-blockchain-for-asset-tracking/
- Supply Chain - https://peerledger.com/mimosi/ gives companies a trusted, immutable record of all track-and-trace transactions across supply chains, https://viant.io/ Supply chain mgmt. built on Ethereum
- Shipping - 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 Resources and Industry

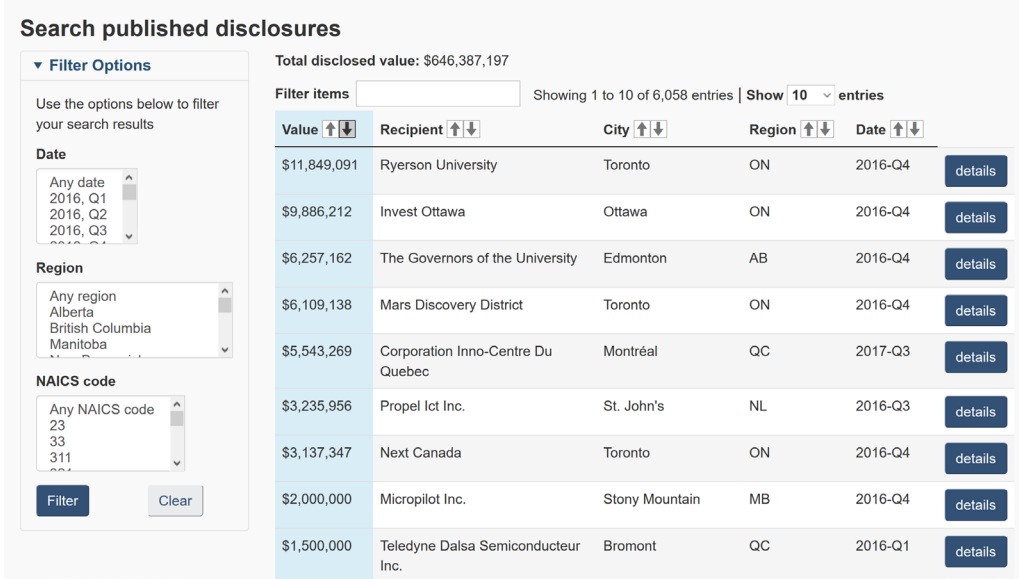
- Agriculture - https://www.cio.com.au/article/644491/cba-helps-ship-17-tonnes-almonds-blockchain/
- Forestry - blockchain to track the planting of trees worldwide and create rewards for planting trees - https://medium.com/@afhenderson/blockchain-for-social-good-4e6d0d4468d3
- Mining - https://techcrunch.com/2018/04/26/ibm-introduces-trustchain-a-blockchain-to-v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



https://carbongrid.io/

2.4 Government, Education, Health

- Currency - https://www.technologyreview.com/s/608910/governments-are-testing-their-own-cryptocurrencies/
- Registries - https://cointelegraph.com/news/netherlands-land-registry-to-test-blockchain-solution-for-real-estate
- Shipping - Denmark will be “the first country in the world [to] use blockchain technology to register ships in the Danish ship registers.” - https://cointelegraph.com/news/denmark-joins-eu-blockchain-partnership-plans-to-implement-tech-in-shipping
- Data – NRC-IRAP Blockchain Prototype - https://nrc-cnrc.explorecatena.com/en/
- Medical Records - https://cointelegraph.com/news/alibaba-founded-insurtech-firm-promotes-blockchain-use-in-healthcare-industry

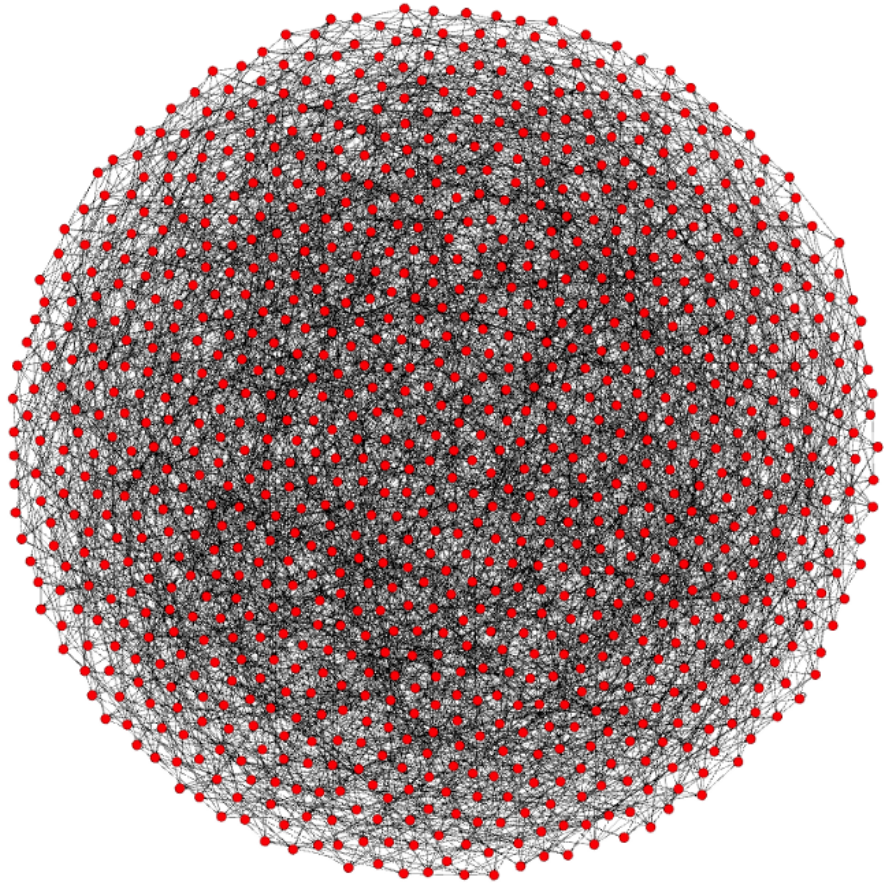


https://nrc-cnrc.explorecatena.com/en/

3. Coins

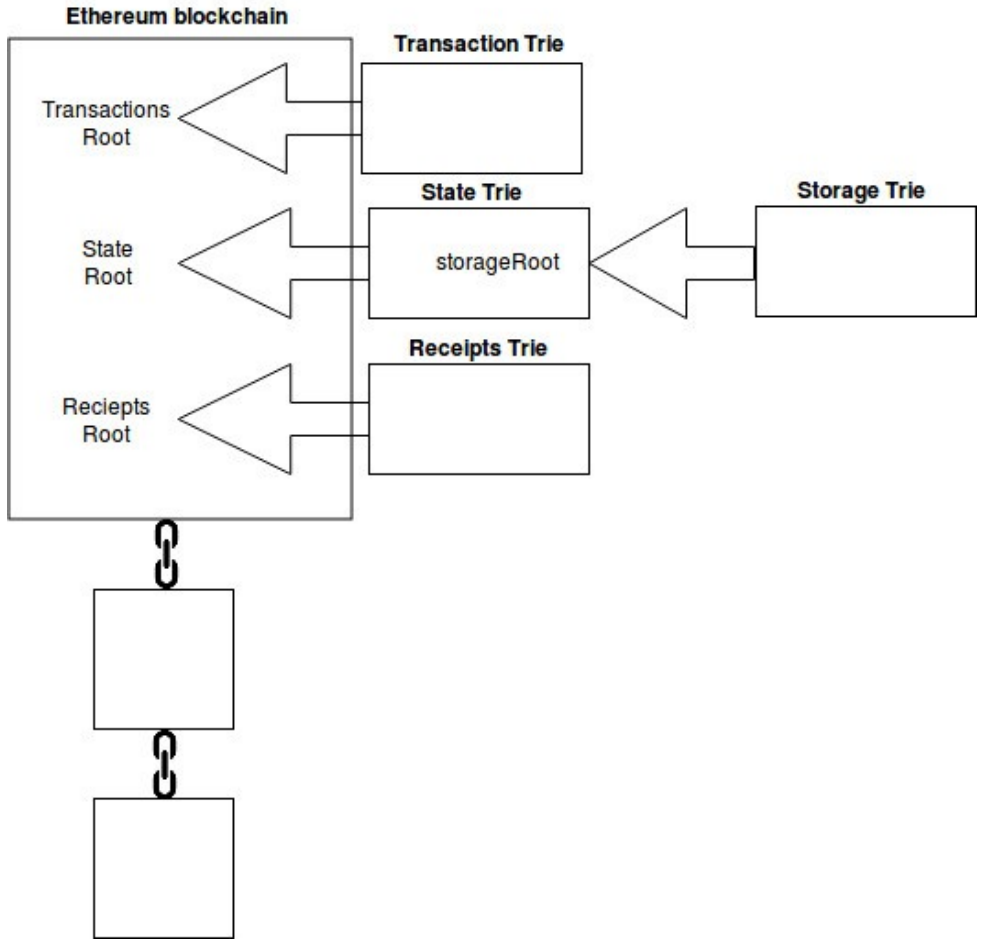
3.1 Bitcoin

- Bitcoin: A Peer-to-Peer Electronic Cash System white paper by Satoshi Nakamoto - https://bitcoin.org/bitcoin.pdf
- Currently 115,000 nodes
- Each node connects to 8 other nodes
- Bitcoin's "state" is represented by its global collection of Unspent Transaction Outputs (UTXOs).
- Lightning - https://lightning.network/
- The Lightning Network is a "second layer" payment protocol that operates on top of a blockchain (most commonly Bitcoin) - https://en.wikipedia.org/wiki/Lightning_Network



3.2 Ethereum (and dApps)

- "Bitcoin is the Digital Gold but Ethereum is the Silicon" https://medium.com/@Michael_Spencer/bitcoins-glory-days-over-the-future-of-blockchain-5fe303f18537
- Founder: Vitalik Buterin - https://github.com/ethereum/wiki/wiki/White-Paper
- Solidity - "Solidity is a **contract**-oriented programming language for writing smart contracts.[1] It is used for implementing smart contracts[2] on various blockchain platforms." https://en.wikipedia.org/wiki/Solidity
- Decentralized Applications (dApps) - consist of everything ranging from prediction markets to gaming, and will continue to grow stronger as the network is improved upon. 1573 today (June 4, 2018) https://www.stateofthedapps.com/

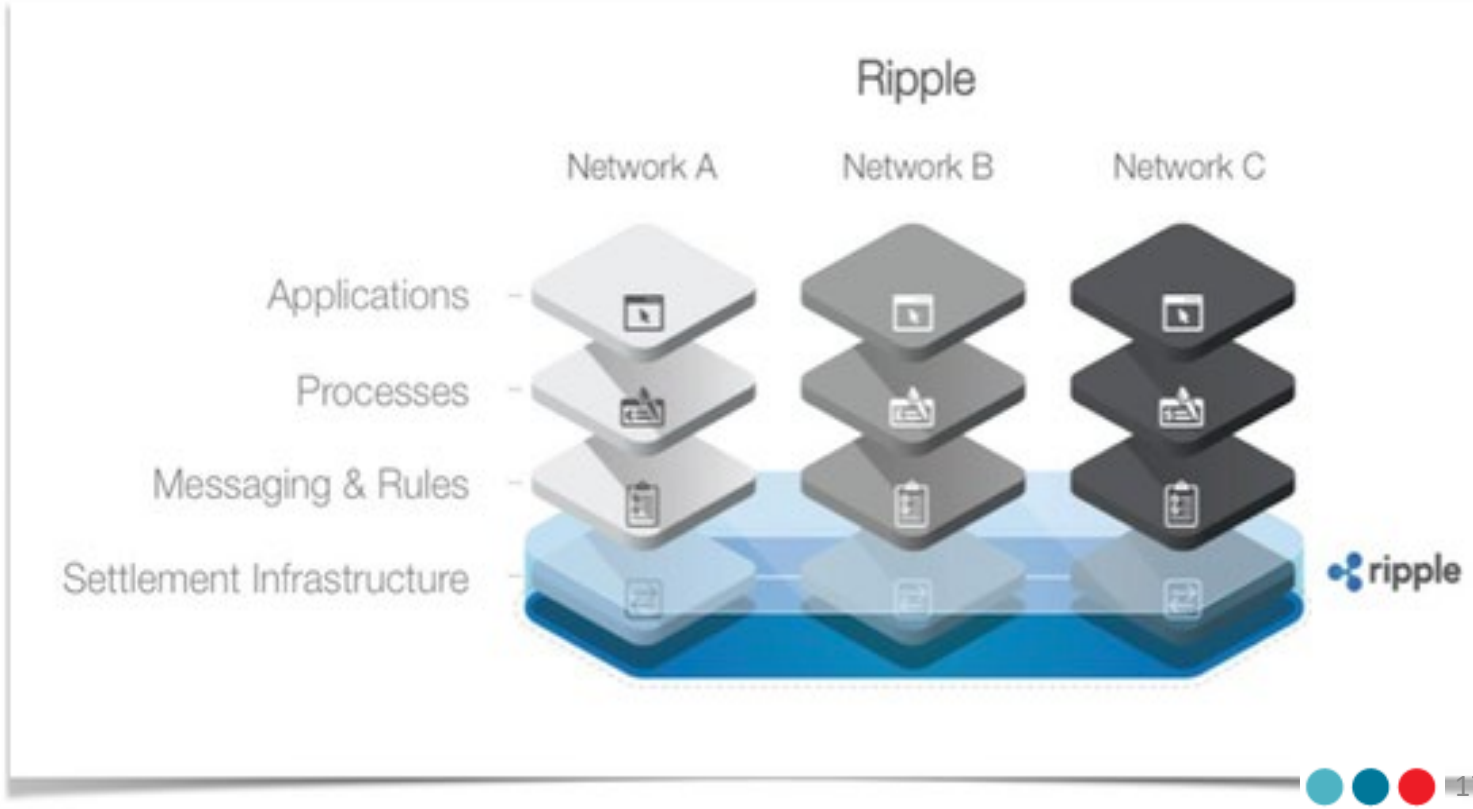


3.3 Ripple and Stellar

- **Ripple** has a network of banks around the world on its platform. International payments can be processed by participating banks within three to five seconds, rather than two to five days, it says.
  https://www.therecord.com/news-story/8653190-uw-gets-research-funding-for-deep-dive-into-blockchain-technology/

- it will replace SWIFT as a global provider of secure financial messaging services
  http://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf
- An upcoming product (**xRapid**) will use XRP as a way to 'source liquidity'
- **Interledger** is the protocol that sits under RippleNet.
- It is being developed as a potential web standard under the the W3C - https://w3c.github.io/webpayments/proposals/interledger/

- **Stellar**
- Decentralized Ripple, collaboration with IBM



3.4 Wallets, Exchanges, Networks

- Exchanges
  - Centralized – Coinbase https://blog.coinbase.com/ , Binance - https://www.binance.com/
  - Decentralized – Altcoin - https://altcoin.io/ , IDEX - https://idex.market/eth/aura
- Networks
  - Towards a Design Philosophy for Interoperable Blockchain Systems, Thomas Hardjono, Alexander Lipton, Alex Pentland https://arxiv.org/abs/1805.05934
- Wallets
  - "What you're actually keeping in your wallet is the private key that is used to access (spend/transfer) your coins." https://cryptocurrencyhub.io/i-bought-my-first-bitcoin-now-what-fdf7dc9ad150

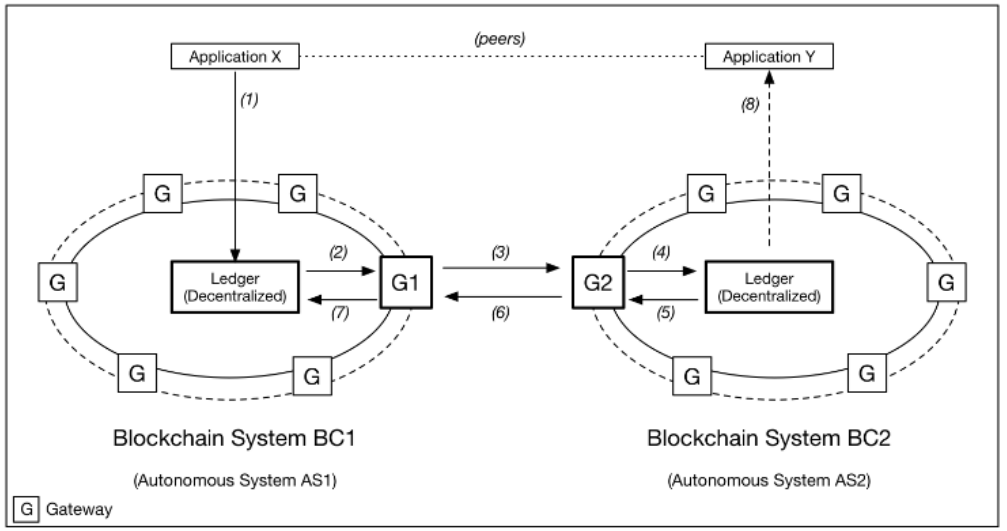


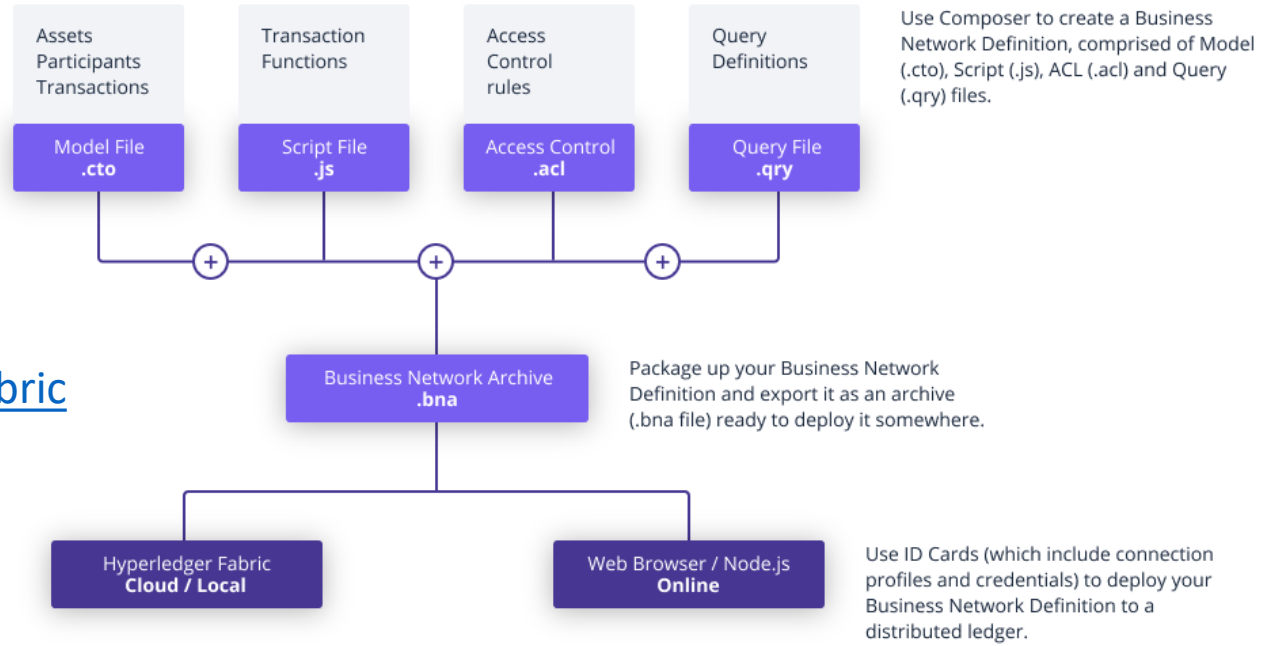
Figure 5: Set of Gateways for Reachability and Transaction Mediation

4. Platforms and Services

4.1 Hyperledger Fabric

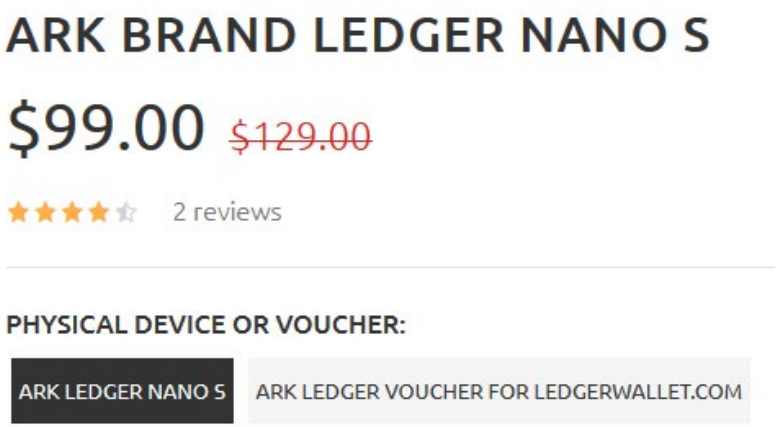
- Private business networks, IBM Bluemix hosting, or Docker containers
- Emphasizes open governance, open standards & open source
- Business Network Definitions
  - a set of model files
  - a set of JavaScript files
  - an Access Control file

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



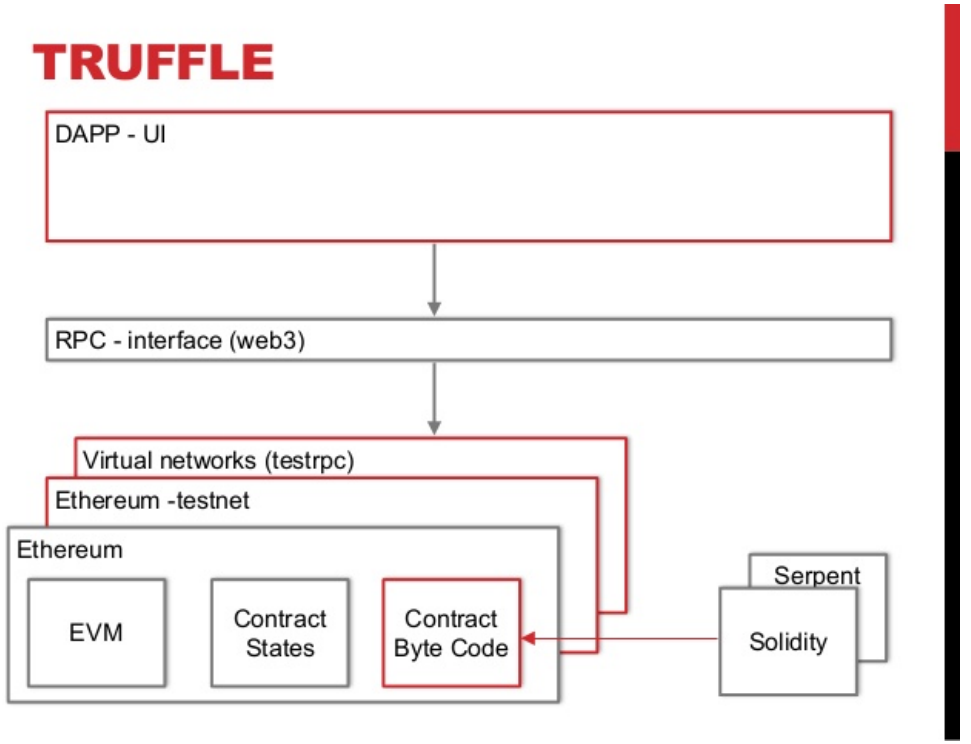
4.2 Ark

- ARK is a secure platform designed for mass adoption and will deliver the services that consumers want and developers need.” https://ark.io/ - explorer: https://explorer.ark.io/
- Ark! The wordpress of crypto! https://decentralize.today/some-great-projects-are-out-there-they-just-dont-talk-about-them-21d677e29ecf
- ARK Desktop Wallet supports the Ledger Nano S secure hardware wallet.



4.3 Truffle (NRC Example)

- a development framework for Ethereum - http://truffleframework.com/
  - Truffle takes care of managing your contract artifacts so you don't have to.
  - Ganache - https://truffleframework.com/ganache - one-click blockchain
  - Drizzle- A collection of front-end libraries that make writing dapp user interfaces easier and more predictable.



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

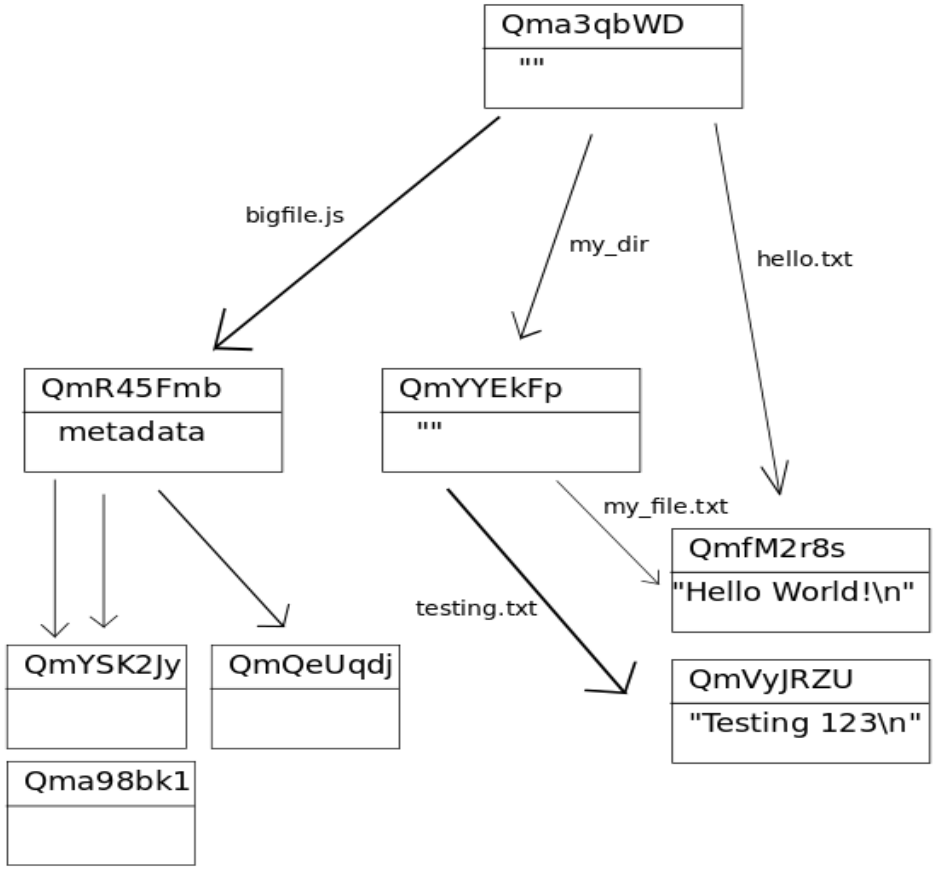
4.4 IPFS / IPLD

IPFS white paper: IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3).

- IPFS consists of a network of peer-to-peer nodes (aka computers that talk to each other directly)
- These nodes can store content (any type of file)
- Content is represented by a hash and is immutable (if the content changes, so does the hash) - In the case of IPFS, the key of the distributed hash table is a hash over the content.

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

- IPLD - Inter Planetary Linked Data
- IPLD website - https://ipld.io/
- the IPLD specs and the IPLD implementations.

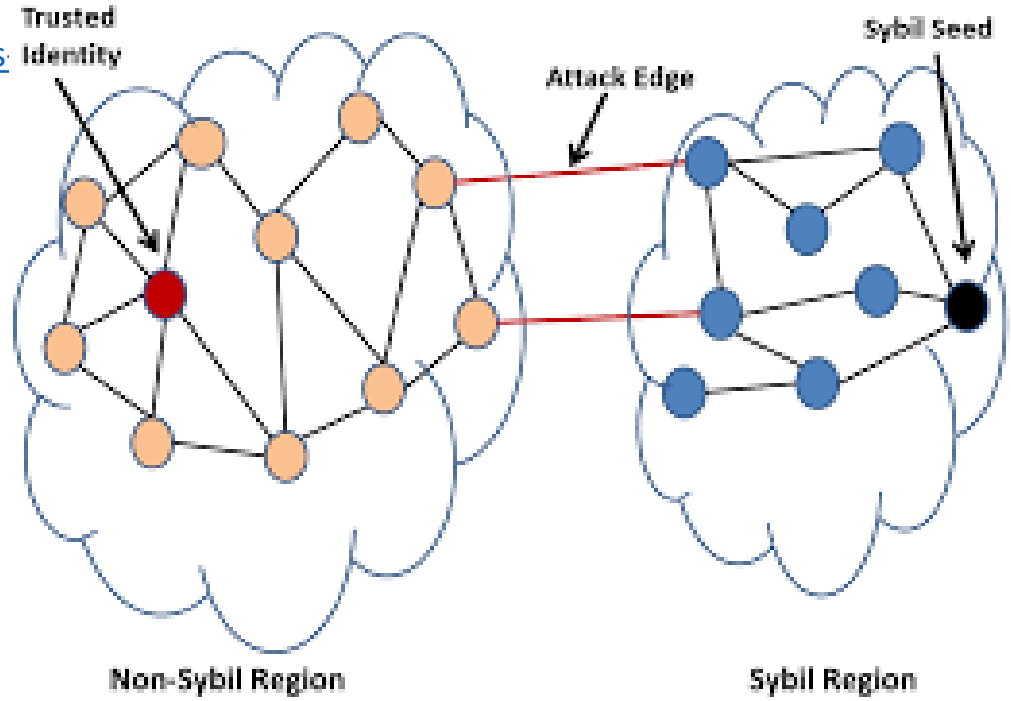


https://whatdoesthequantsay.com/2015/09/13/ipfs-introduction-by-example

5. Some Issues

5.1 Conceptual Issues

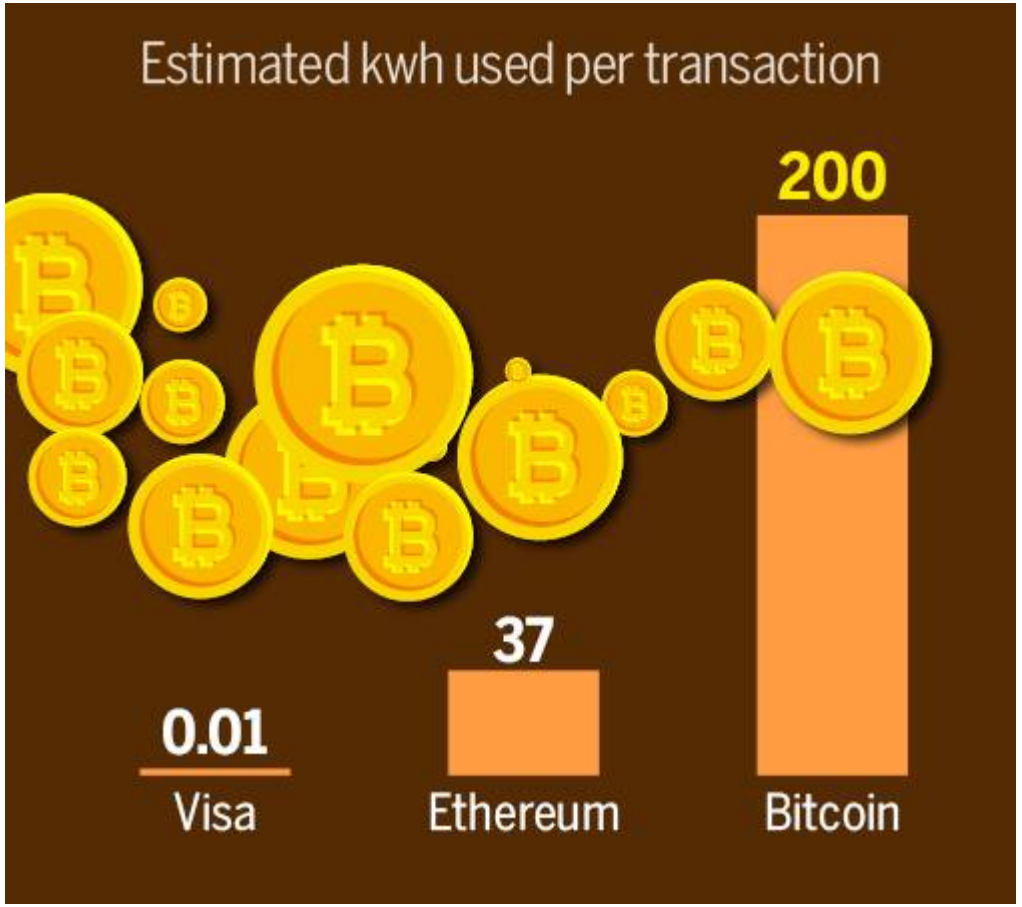
- Locus of Value - Fat Protocols vs Fat Dapps vs Fat Wallets
  - https://medium.com/lightspeed-venture-partners/fat-protocols-vs-fat-dapps-vs-fat-wallets-4d33ead29130
- Economic Incentives and the Nothing at Stake Problem
  - https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb
- Immutability (and GDPR)



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

5.2 Cost and Energy Consumption

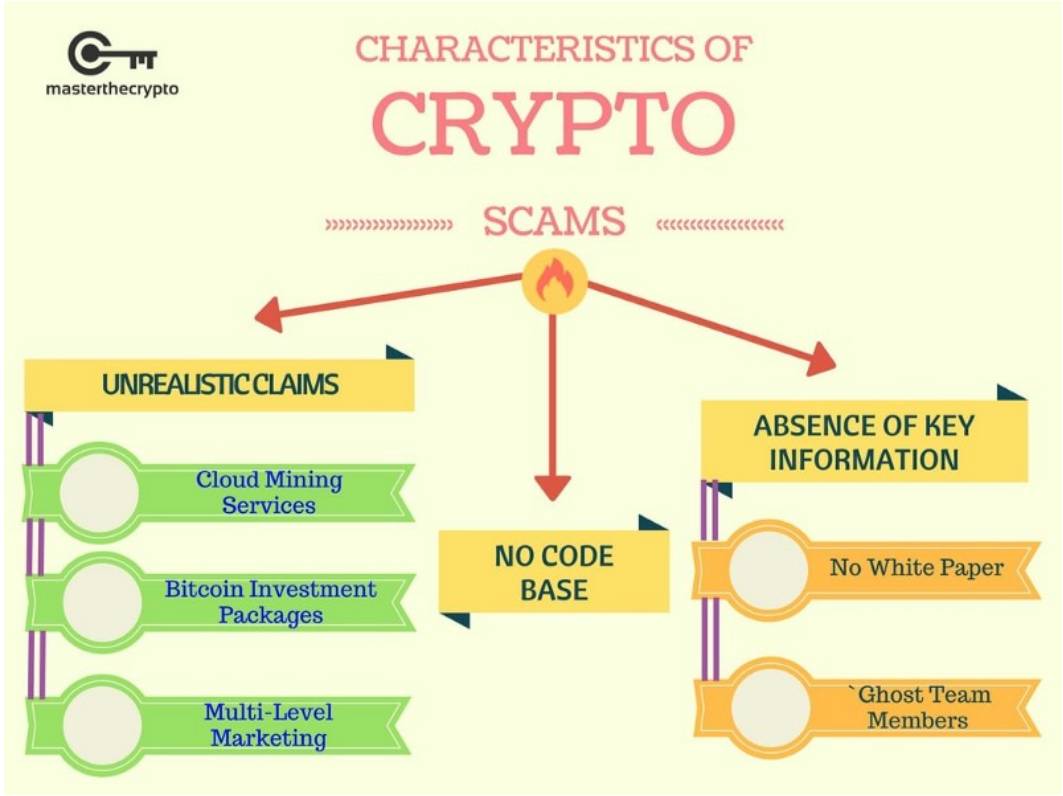
- Software reliability
- Energy Consumption
  - Bitcoin uses an amount of energy that could power over 6,000,000 homes.
  - It currently consumes the equivalent of 10% of Canada's total energy consumption.
  - 1 BC transaction costs more than 100,000 Visa transactions.
- Scaling - Bitcoin 7 tx/s, Ethereum 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 Social and Ethical Issues

- Token distribution and inequality
- Regulation and taxation
  - https://medium.com/forbes/tax-trouble-for-certain-bitcoin-traders-41414e4d47a8
- Market failures, libertarian culture
- Scams and fraud
  - Fake ICOs
  - Market manipulation
  - Ponzi schemes
- Cybersecurity



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