Distributed Ledger Technology and how it is applied in Blockchain

Presented BY: Dr Abdurashid Turgunov

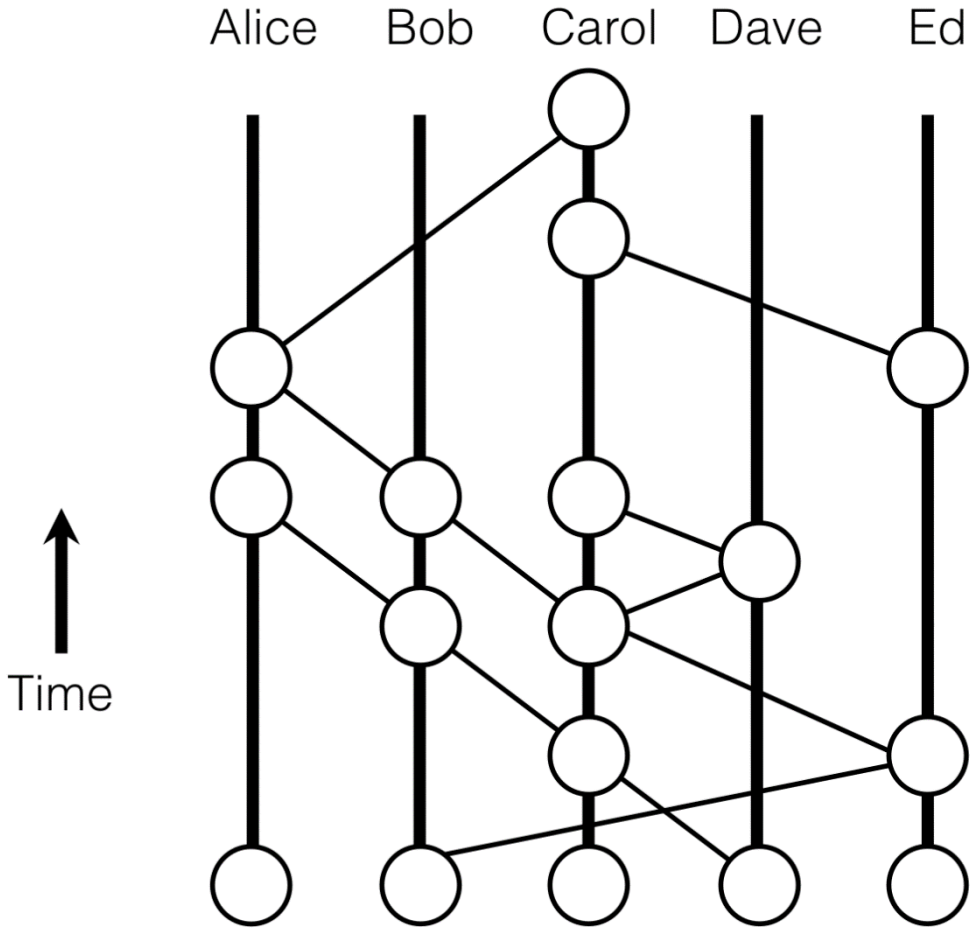
Course name: Blockchain Technology

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."

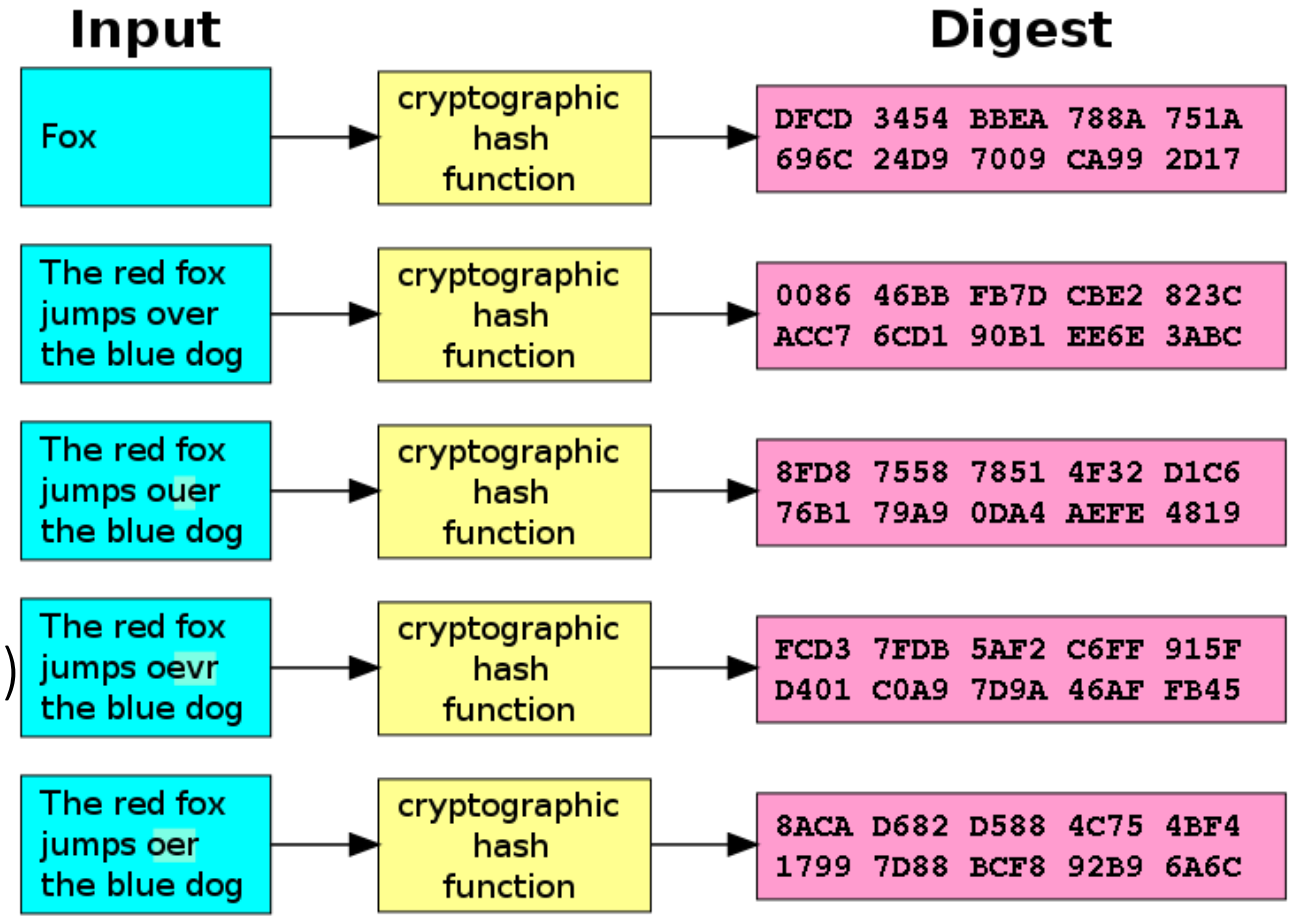


https://hackernoon.com/an-overview-of-hashgraph-b0900a1fd7bf

1.3 Cryptographic hash functions

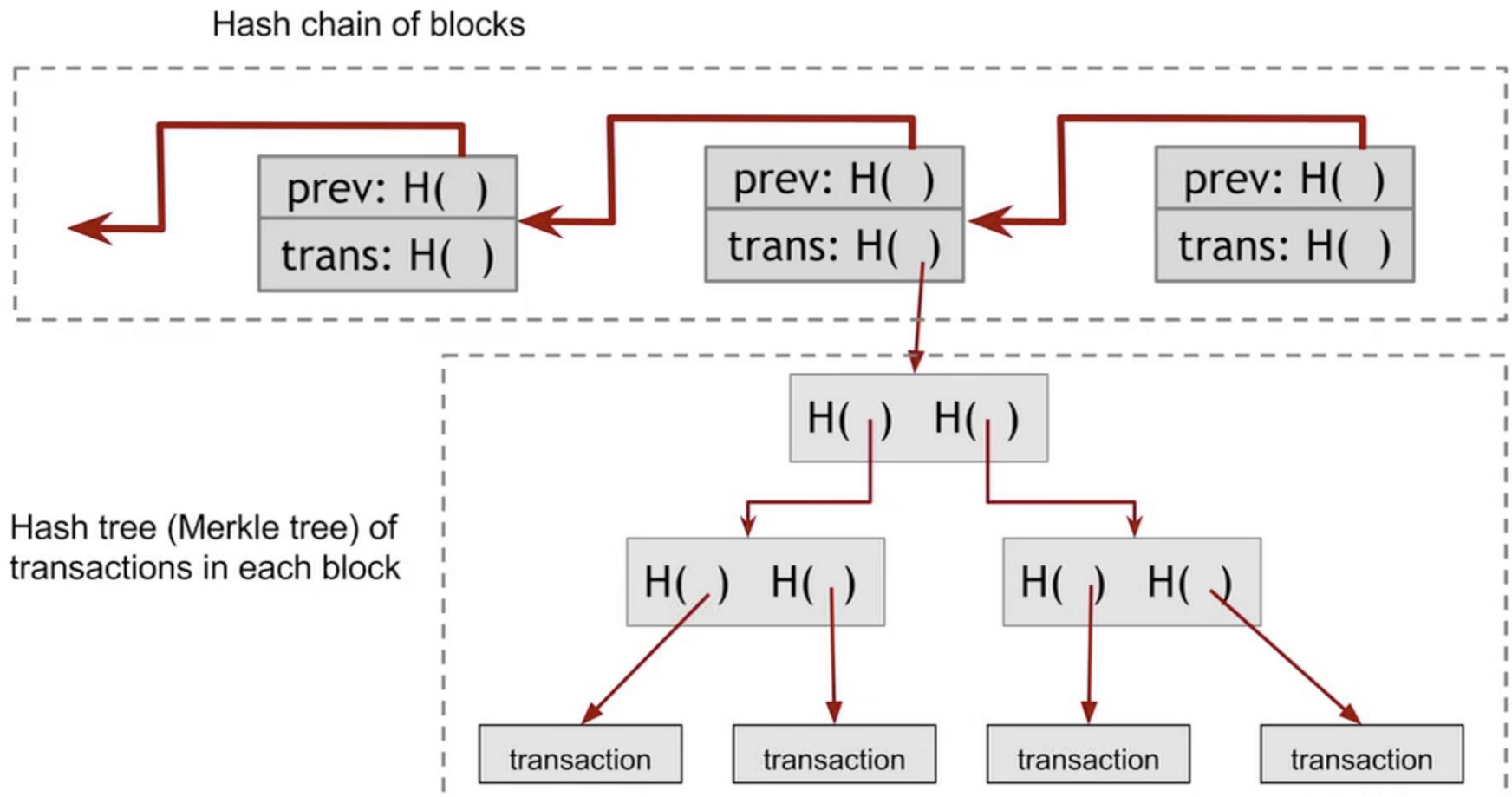
"a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash) and is designed to be a one-way function.."

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



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

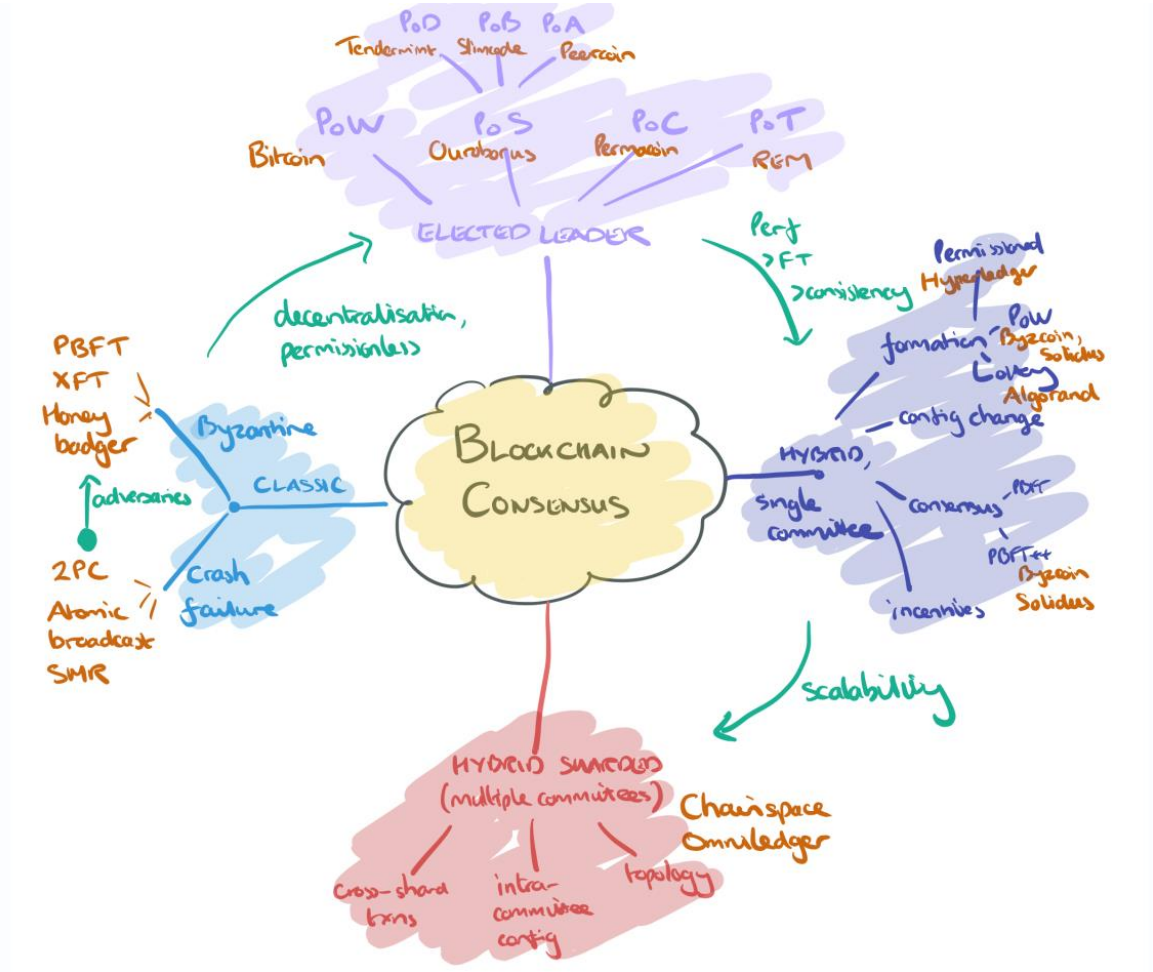
14 Construction of a blockchain



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

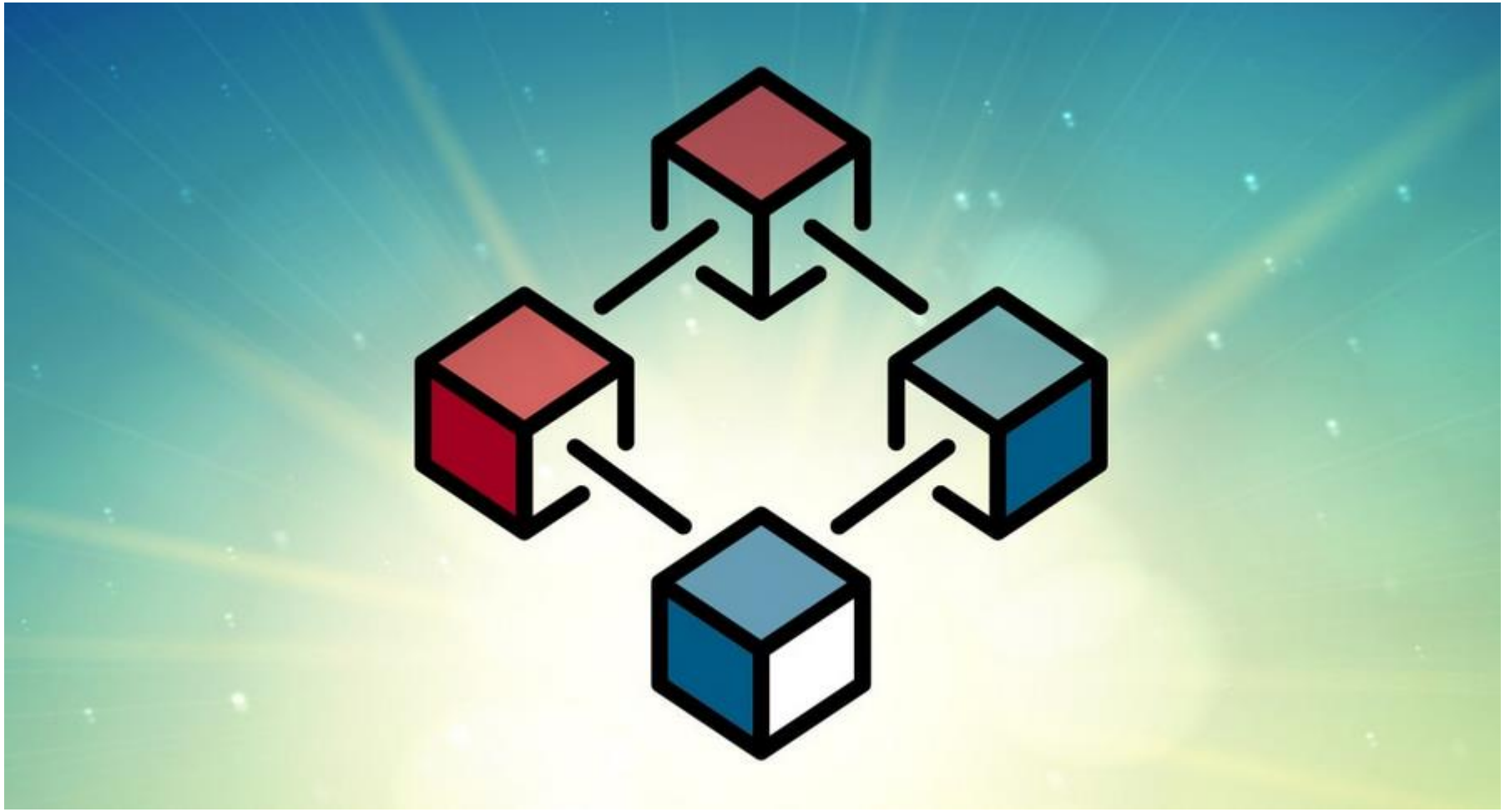
1.5 Consensus – an intro, proof of work, alternatives

"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

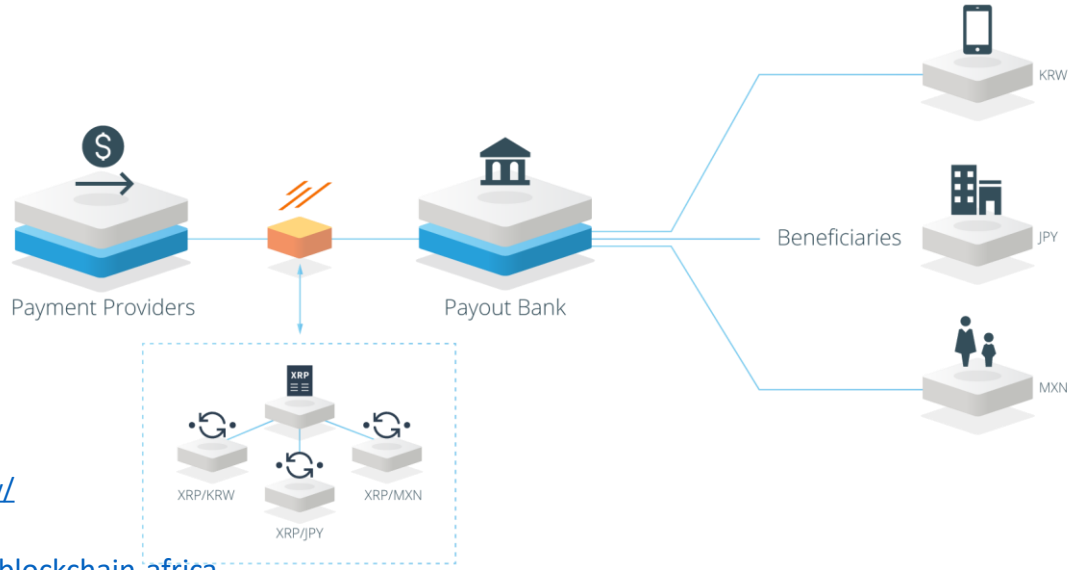


2.1 Benefits of Blockchain

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

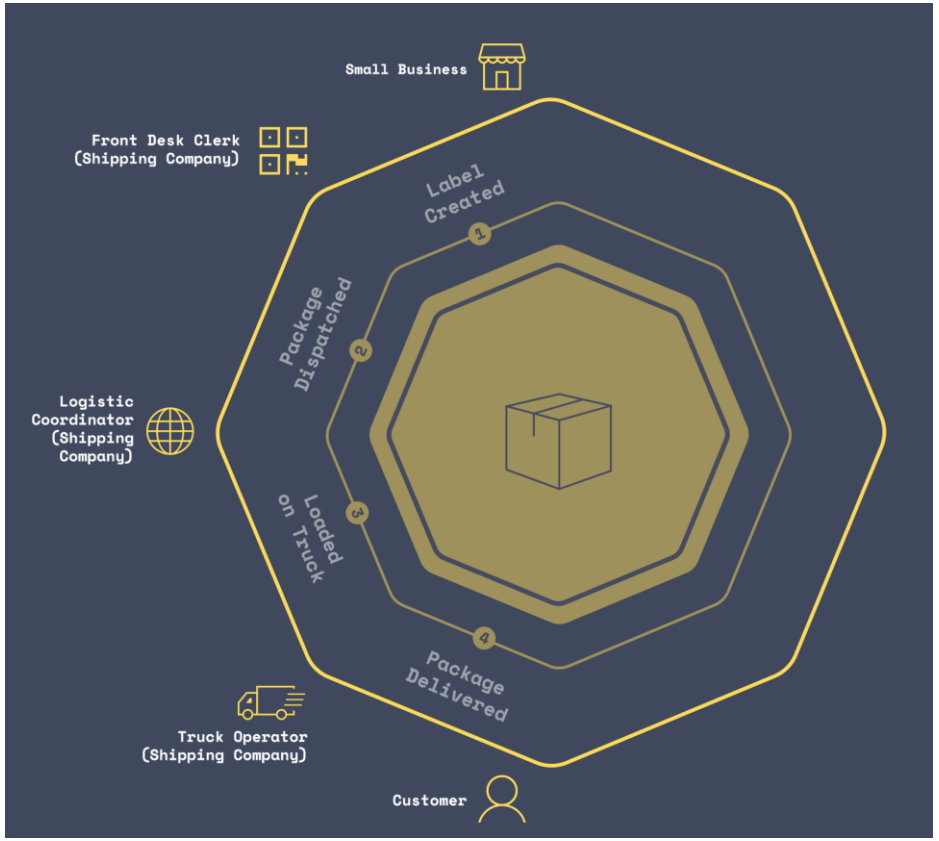
2.1 Currency and Financial

- 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 networking, audit, compliance

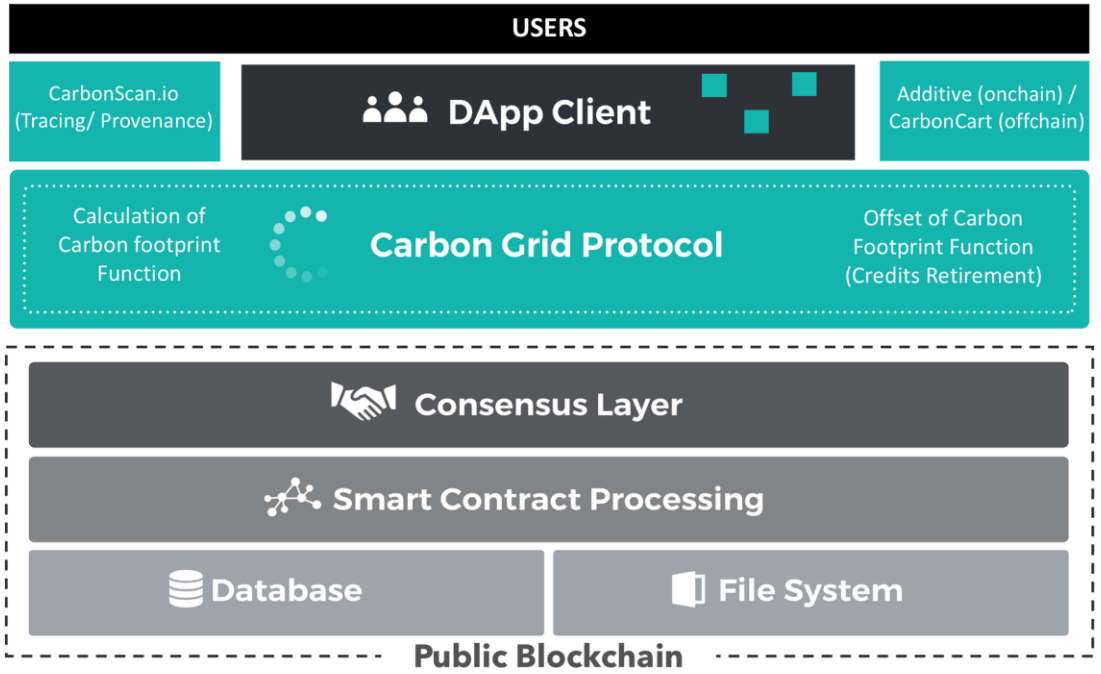
- Law and contracts - https://agreements.network/
- Markets - https://techcrunch.com/2017/04/11/bext360-is-using-robots-and-the-blockchain-to-pay-coffee-farmers-fairly/
- Asset Management - https://www.coindesk.com/td-bank-considers-public-blockchain-for-asset-tracking/
- Supply Chain - https://peerledger.com/mimosi/ 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

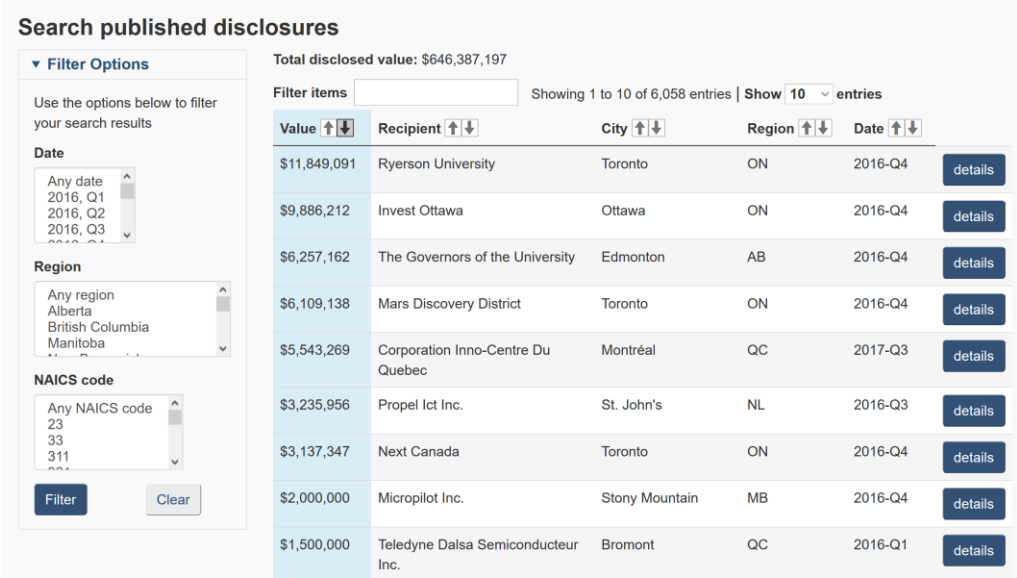
- Agriculture - https://www.cio.com.au/article/644491/cba-helps-ship-17-tonnes-almonds-blockchain/
- Forestry - blockchain to track the planting of trees worldwide and create rewards for planting trees - https://medium.com/@afhenderson/blockchain-for-social-good-4e6d0d4468d3
- Mining - https://techcrunch.com/2018/04/26/ibm-introduces-trustchain-a-blockchain-to-v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



https://carbongrid.io/

2.4 Government, education and 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

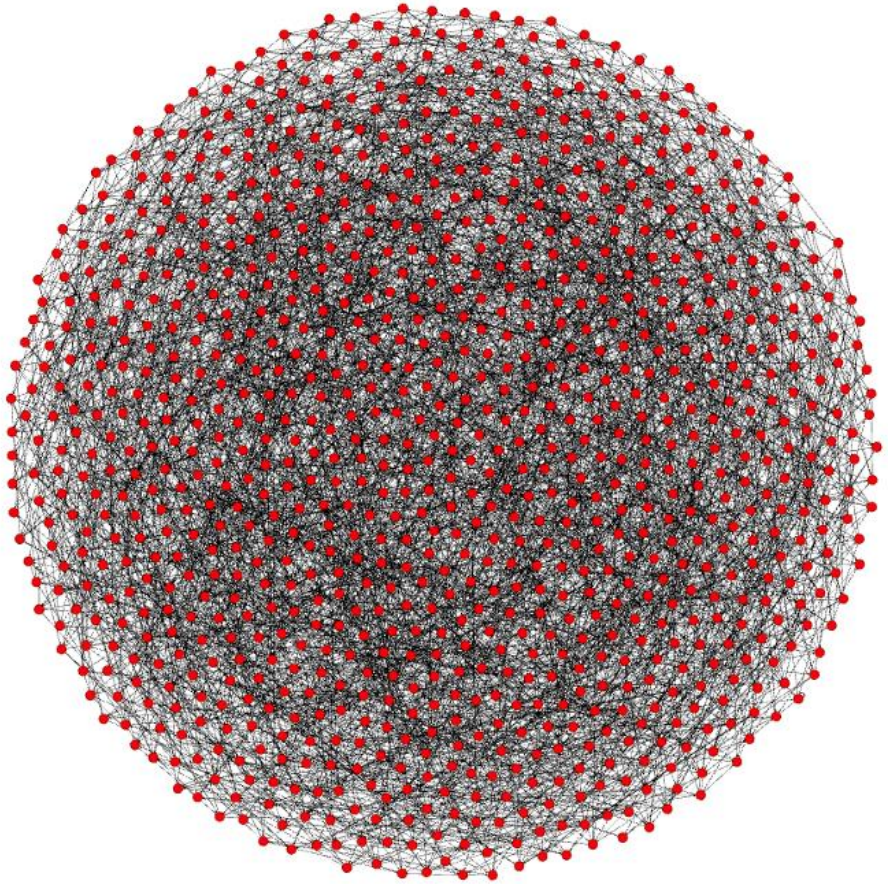


https://nrc-cnrc.explorecatena.com/en/

3. Coins

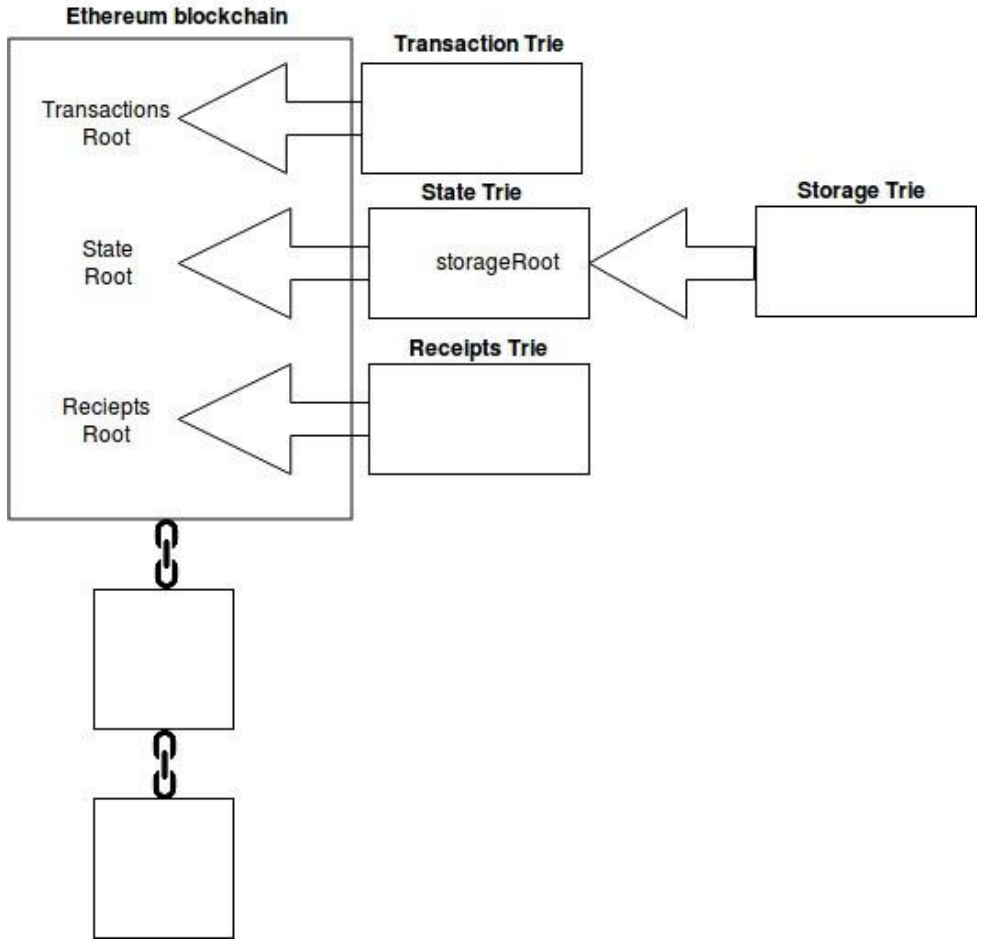
3.1 Bitcoin

- 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/

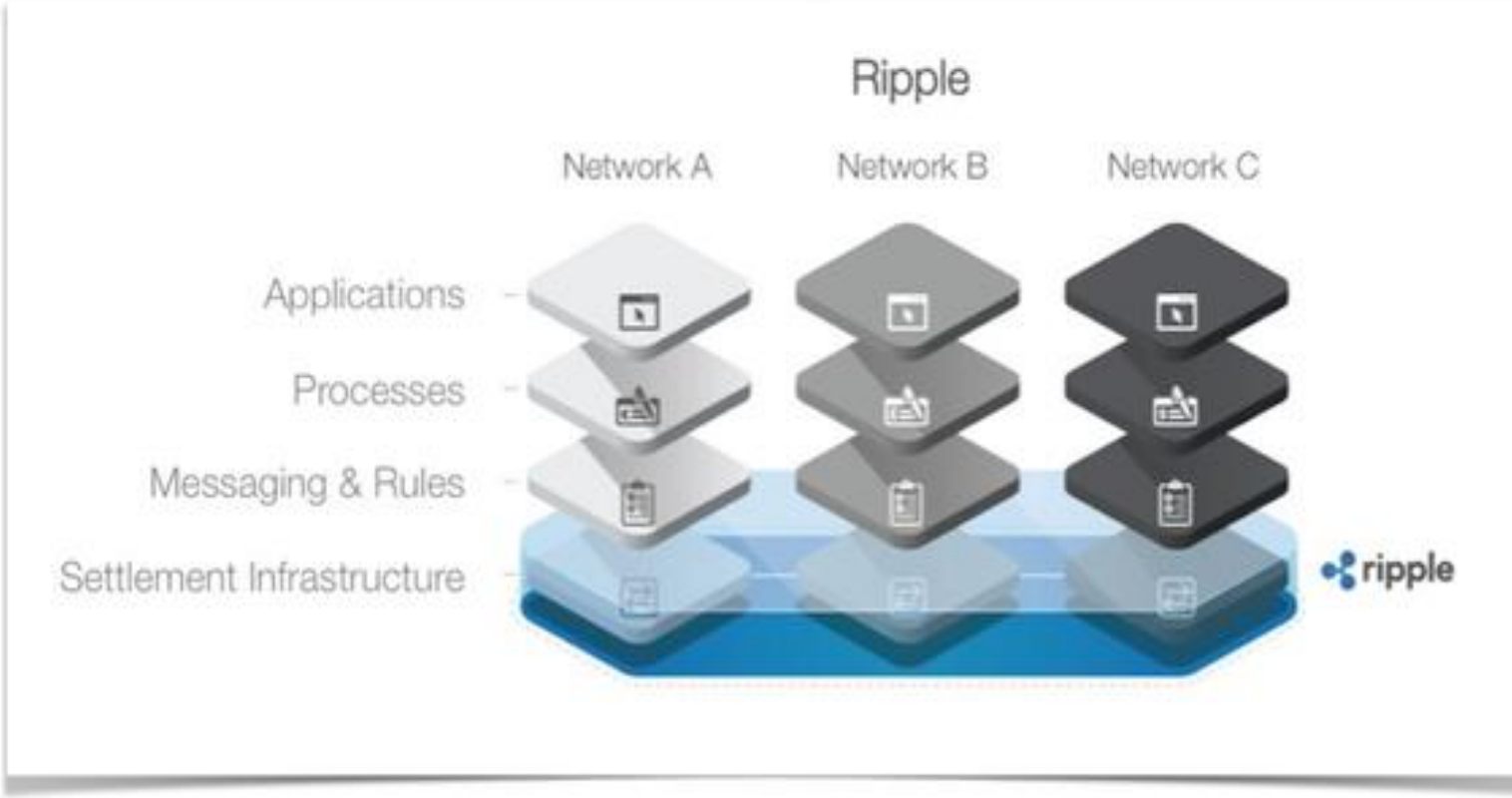


3.3 Ripple and Stellar

- **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 and 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

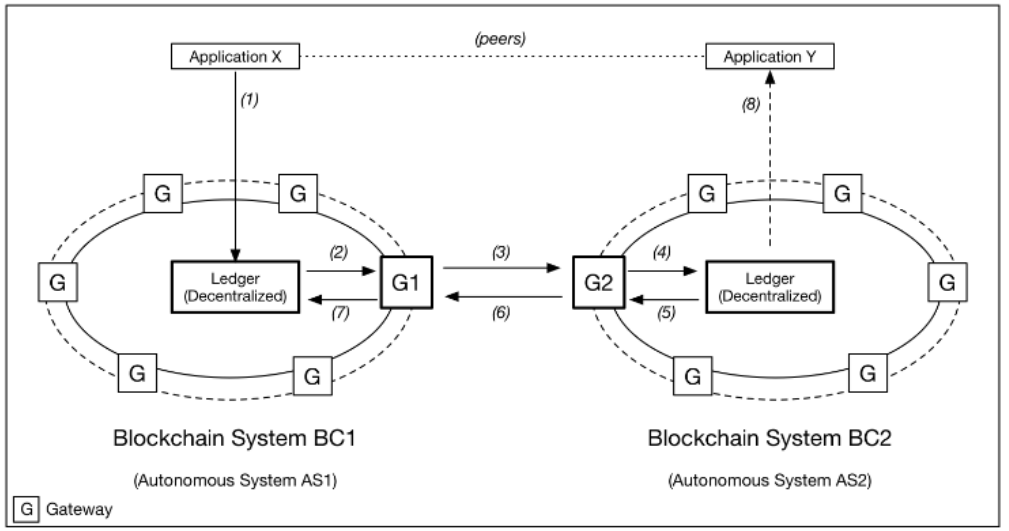
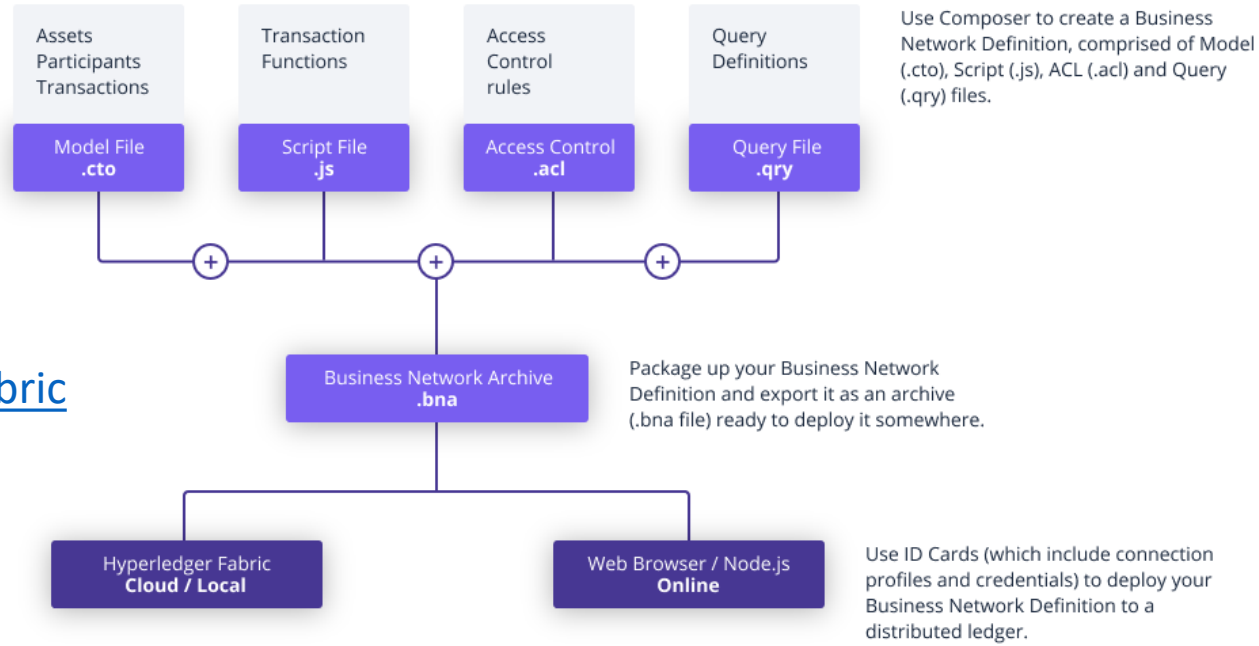


Figure 5: Set of Gateways for Reachability and Transaction Mediation

4. Platforms and Services

4.1 Hyperledger Fabric

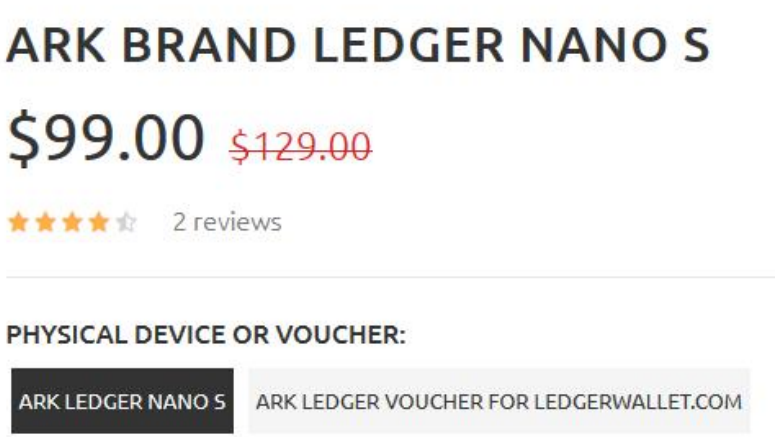
- Private business networks, IBM Bluemix hosting, or Docker containers
- Emphasizes open governance, open standards & open source
- Private business networks, IBM Bluemix hosting, or Docker containers
- Emphasizes open governance, open standards & open source
- Business Network Definitions
  - a set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



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

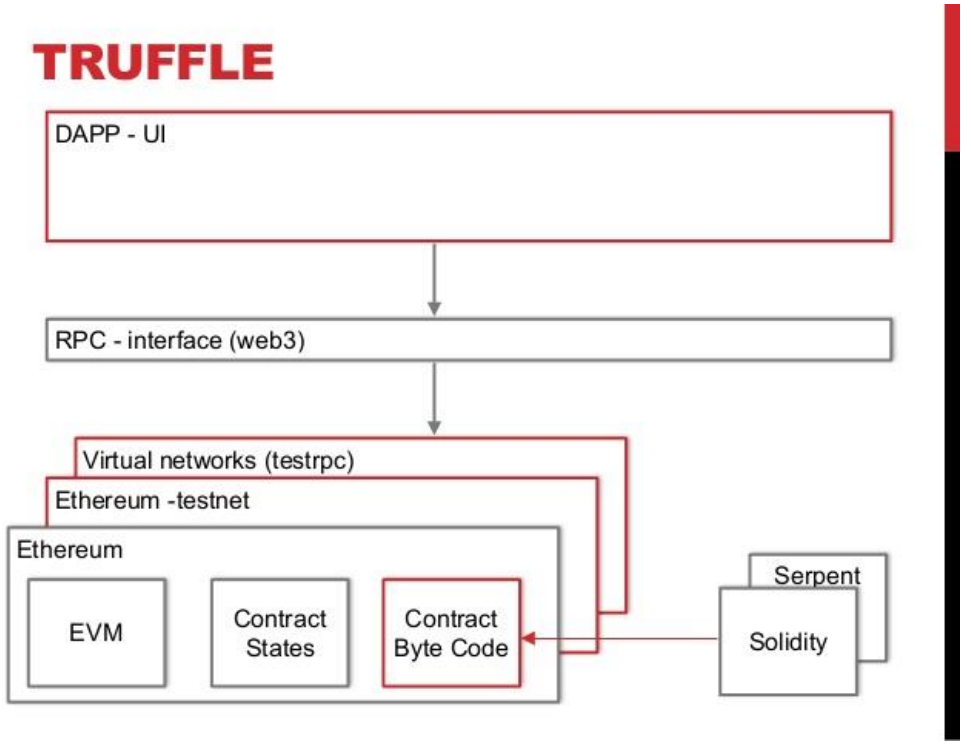
4.2 Ark

- 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

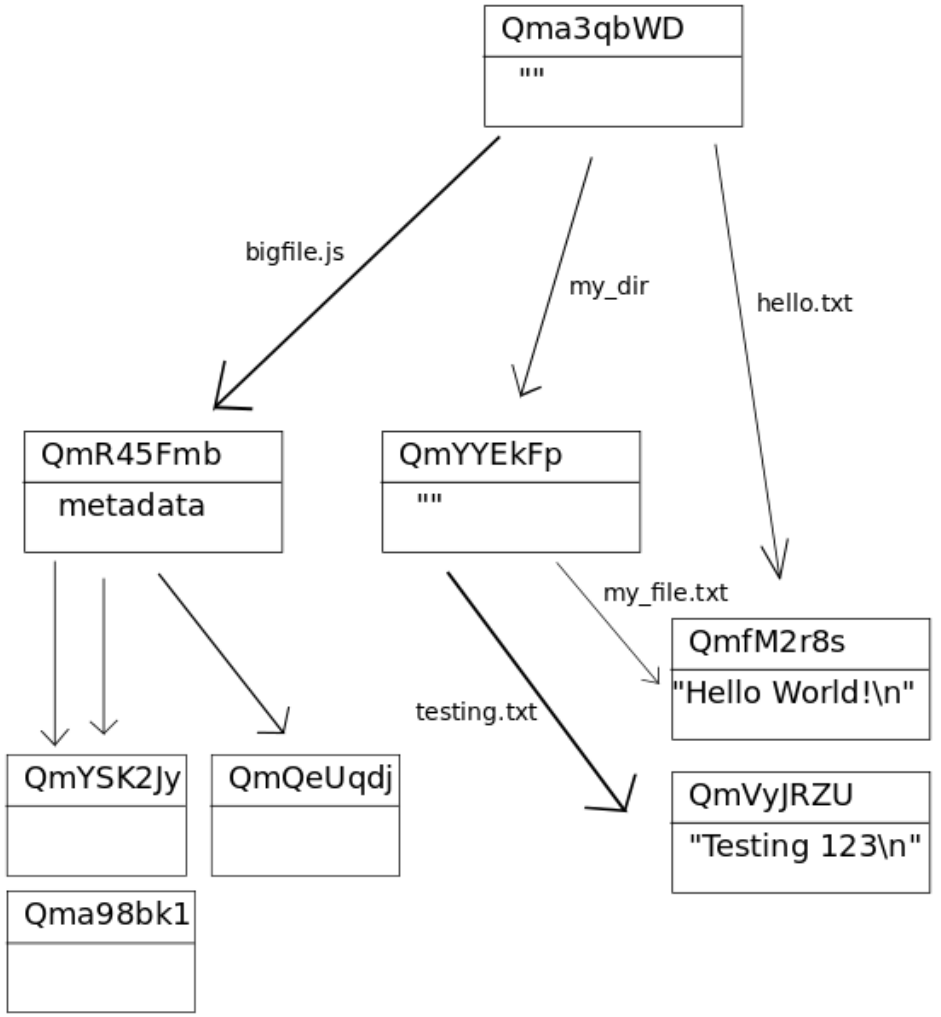
4.4 IPFS - IPLD

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

- PFS 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/

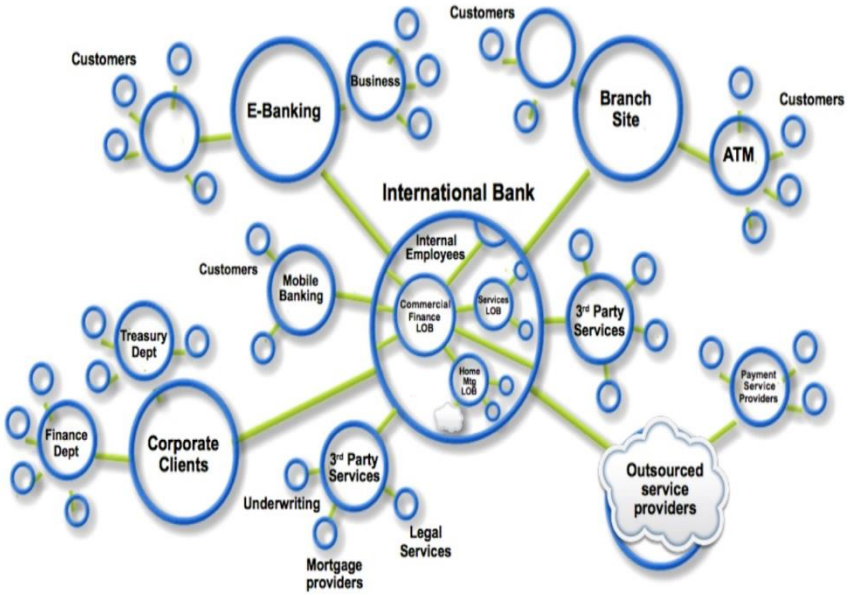
- IPLD - Inter Planetary Linked Data
- IPLD website (Inter Planetary Linked Data) - https://ipld.io/
- the IPLD specs and the IPLD implementations.



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

Business Networks, Markets & Wealth

- Businesses don't exist in isolation
  - Connected to customers, suppliers, banks, partners etc. through Business Network
  - Networks cross geography & regulatory boundary
- Wealth is sum total of value of goods & services across business network
  - Growth constrained if silo'd or inefficient
- Flow goods & services across business network is a Market
  - OPEN (fruit market, outcry commodities, or
  - CLOSED (supply chain financing, bonds)

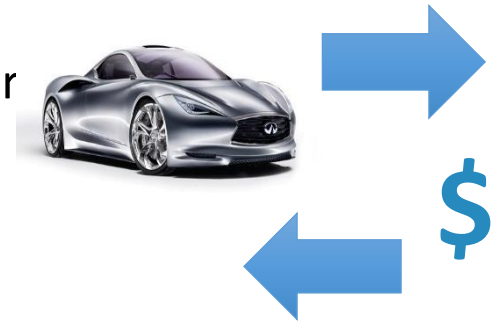


Transferring Assets, building Value

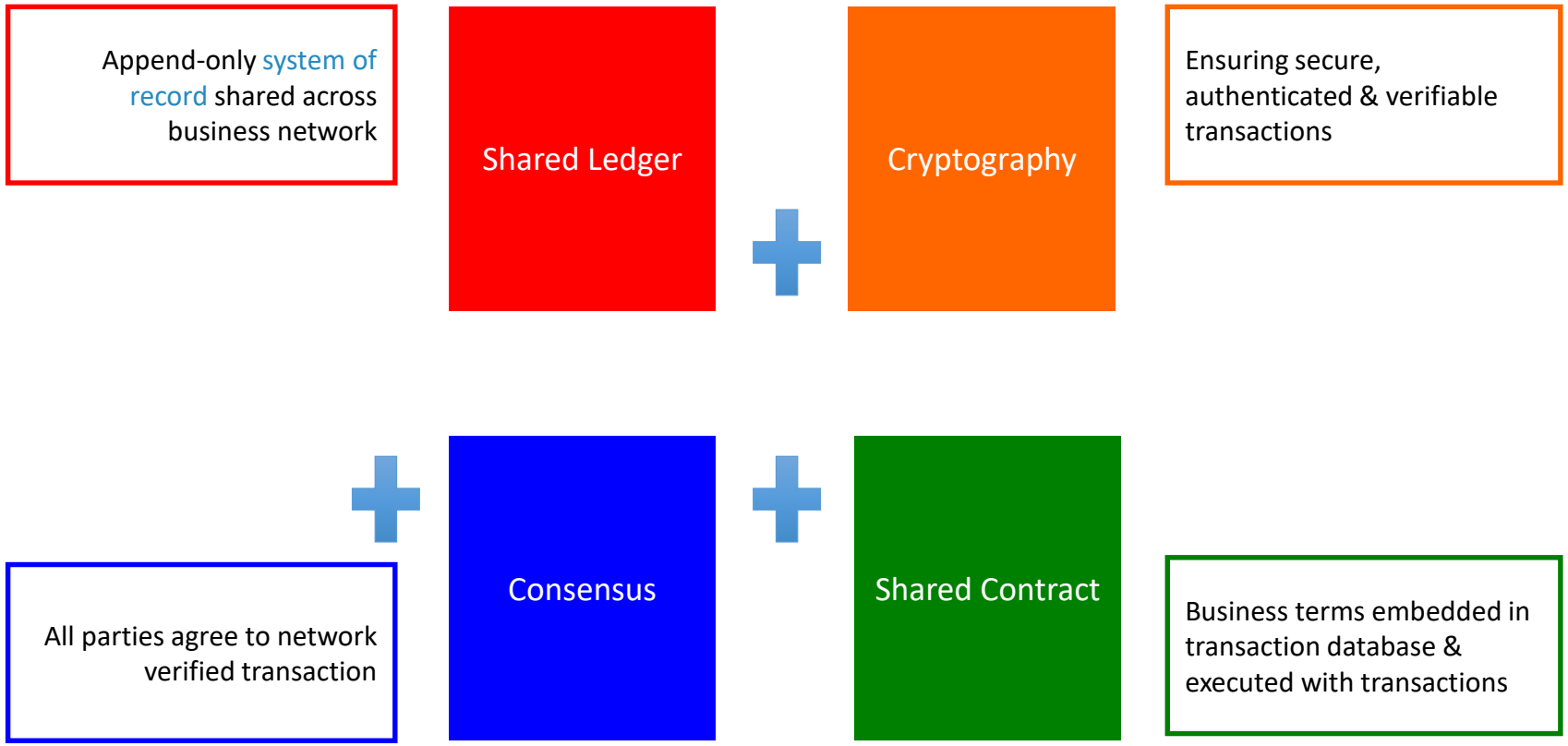
- Anything that is capable of being owned or controlled to produce value, is considered an asset
  - can be tangible or intangible
  - value can be converted into cash.
- Cash also an asset.
- Asset examples:
  - Cars, value clothes (physical)
  - Bonds, securities, repurchase agreements (intangible)
  - Licenses & patents (intangible assets)
  - Music, video, games (intangible, digital)

Participants, Transactions & Contracts

- A participant is a member of a business network
  - Customer, Supplier, Government, Regulator
  - Usually reside in an organization
  - Have specific identities and roles
- A transaction is an asset transfer between two or more participants, for example
  - John gives a car to Anthony (simple)
  - John gives a car to Anthony, Anthony gives money to John (more complex)
- A contract is set of conditions under which transactions occur, for example
  - If Anthony pays John money, then car passes from John to Anthony (simple)
  - If car won't start, funds do not pass to John (as decided by independent third party arbitrator)

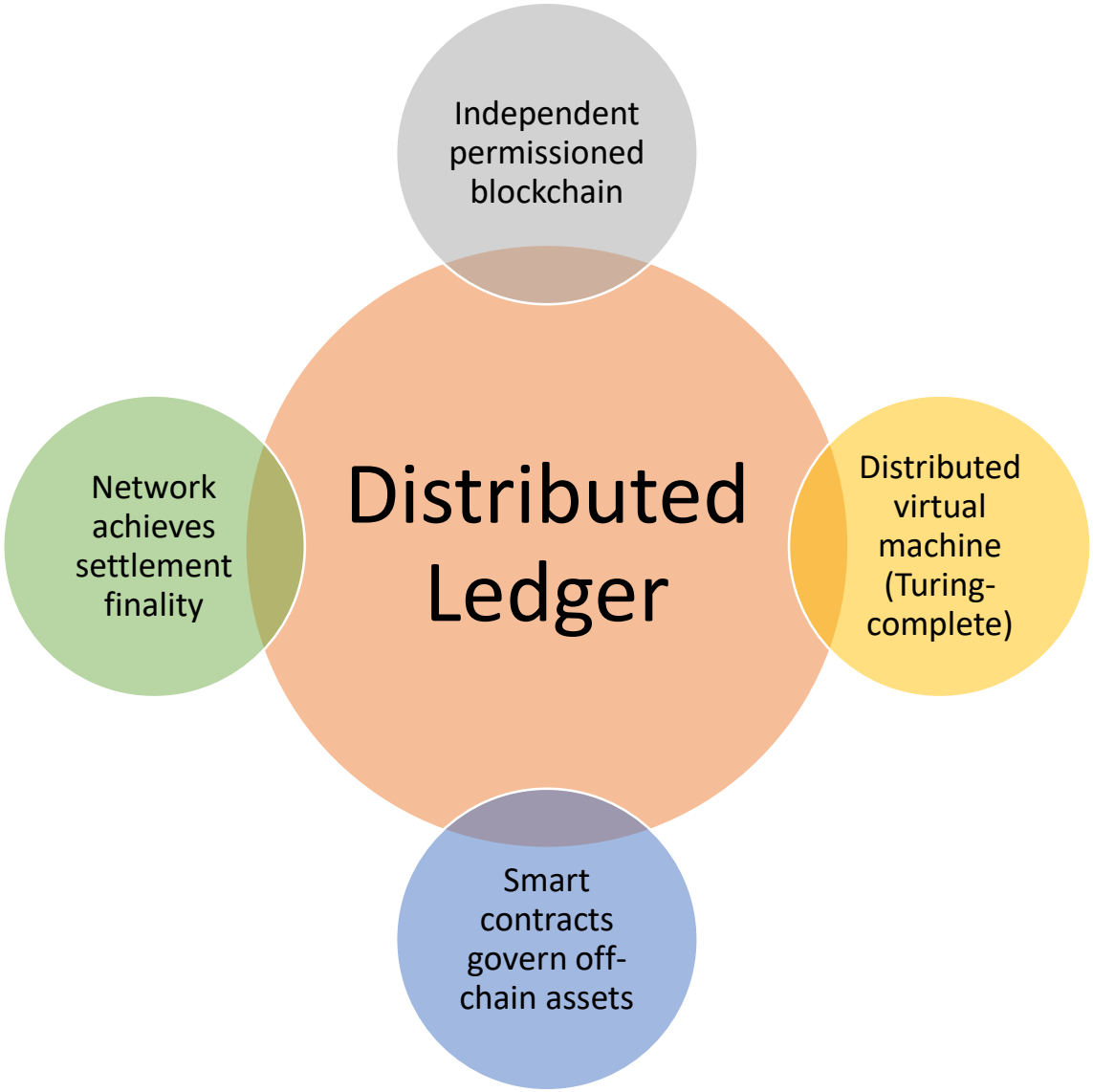


Blockchain in a nutshell



Broader participation, lower cost, increased efficiency

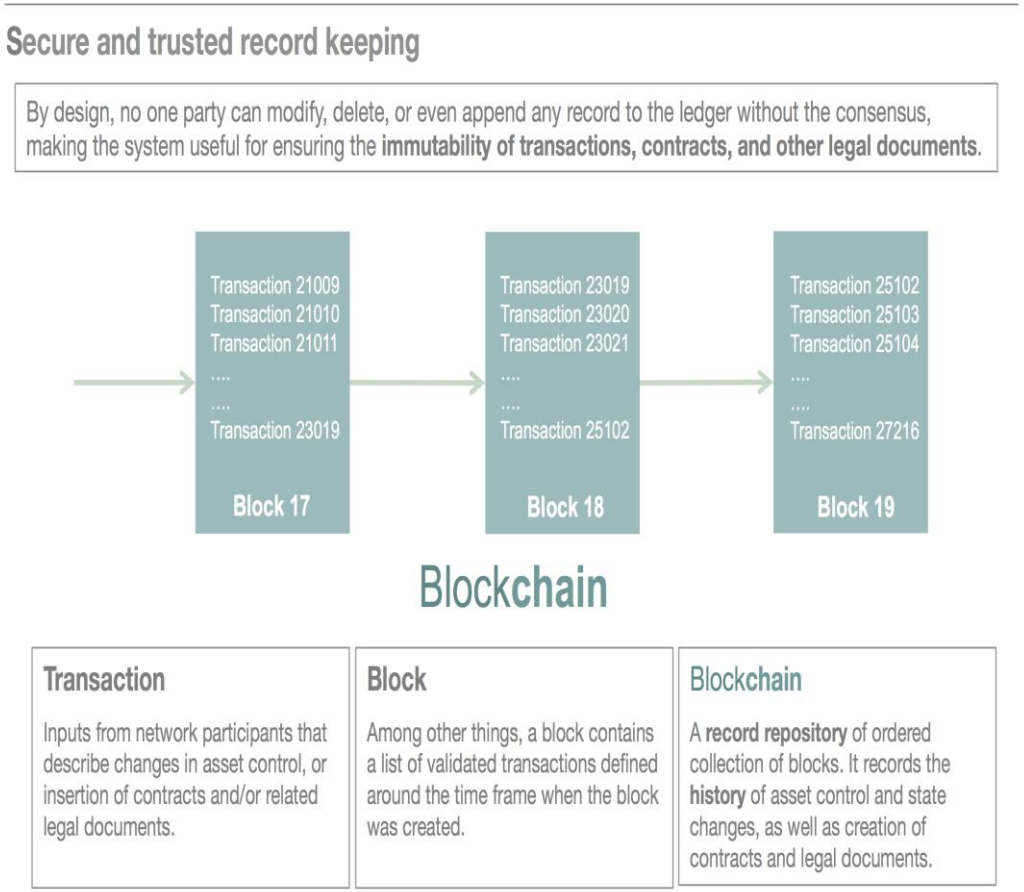
Distributed Ledger - Components



http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

Why blockchain?

Blockchains are an emerging technology pattern that can radically improve banking, supply-chain and other transaction networks, giving them new opportunities for innovation and growth while reducing cost and risk.



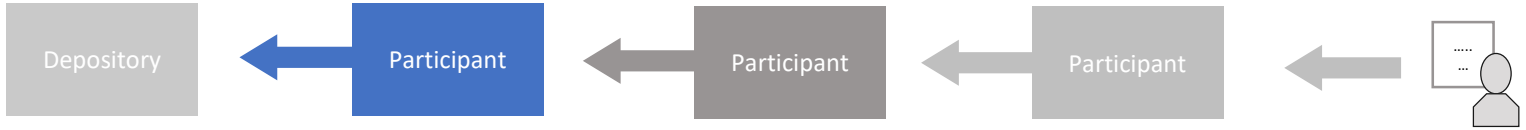
Economic transactions on a distributed ledger can be programmed to record virtually anything of value: your identity, a will, a deed, a title, a license, intellectual property, and also almost any type of financial instrument.

"How seriously should we take this? I would take it as seriously as we should have taken the concept of the Internet in the 1990s."

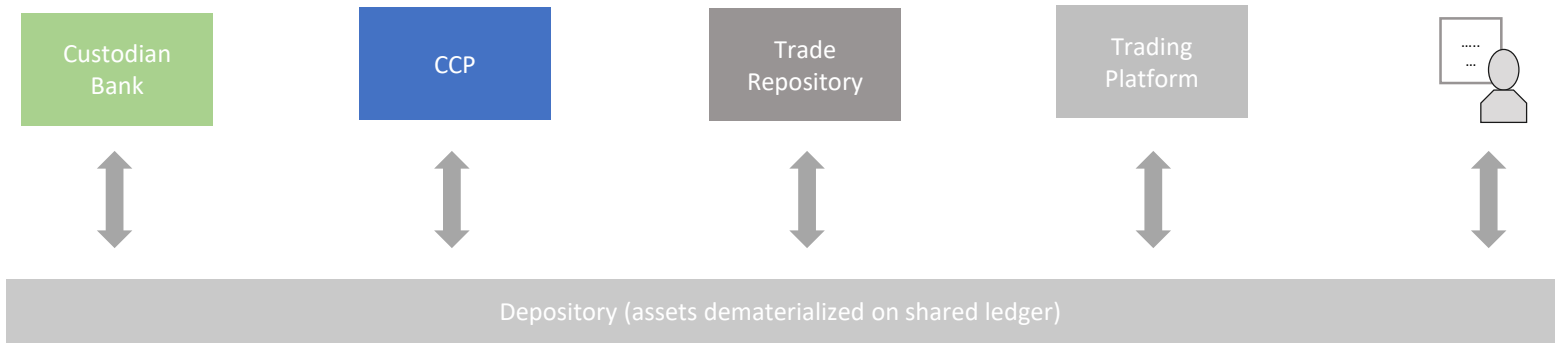
—Blythe Masters, DAH http://bit.ly/1JENgb4

Reduce costs and complexity

Blockchain technology offers a way for market participants to access dematerialized assets **directly** without always going through other participants needlessly



Centralized Repository (today's system): most participants are disconnected from their asset depository, settling transaction would require participants to collaborate in a flow that is **slow**, **inefficient,** and **expensive**



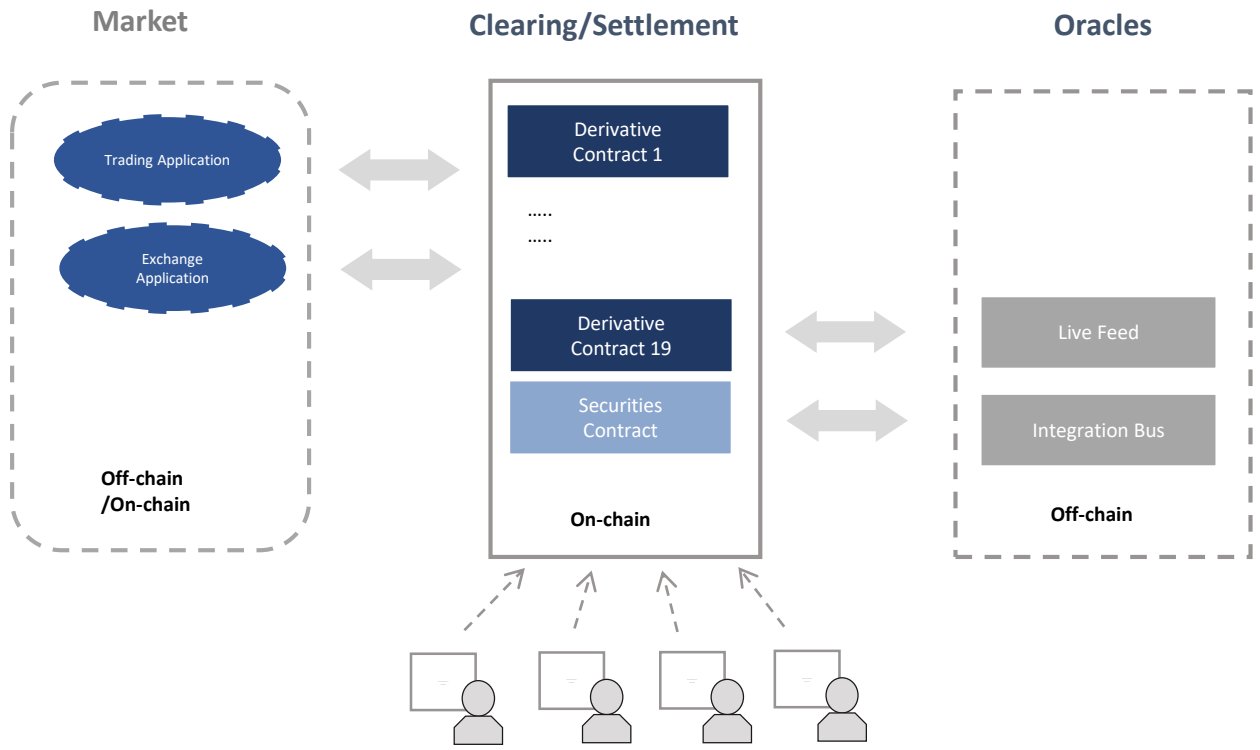
Shared Repository: all participants can interact with depository directly without going involving third parties, potentially making post trade operations **cheaper** and **faster**

Financial Industry Applications best suited for Blockchain

- Financial Instruments
  - Payments – Cross Border, P2P, Corporate and Interbank
  - Private Equity
  - Bonds
  - Derivative commodities
  - Trading records
  - Spending records
  - Mortgage/Loan records
  - Microfinance
  - Servicing records
- Stack of Processes
  - Clearing Networks
  - International Transfers
  - Clearing and Settlement
  - auditing, reconciliation, reporting, settlement
  - Asset Ownership

Blockchain for Financial Market

Trading, clearing, and settlement functions can all be automated on a blockchain network using smart contracts and oracles.



Market	*Clearing/Settlement*	*Oracle*
Trading/exchange applications can live either on-chain or off-chain (i.e. off-chain applications are often more centralized, but likely offer better latency).	Final clearing/settlement of financial assets can be automated through smart contracts, which have direct access to assets defined on chain.	Oracles are off chain services that integrate on-chain contracts with existing systems; network participants do not interact with oracles directly.

IBM – Financial Services use cases for Blockchain

Blockchain for Banking
Letters of Credit As a bank handling letters of credit (LOC) for my clients, I need a common ledger that allows me and all counter-parties to have the same validated record of transaction and fulfilment of conditions, so that we can increase trust and speed of execution from 4 days to <1 day. If we can drive out 99% of the time and cost, we can offer innovative LOC solutions for a wider range of clients, including start-ups that are “born global.
Corporate Debt As a bank handler of corporate debt, I need a Blockchain based system so that I can pay vendor invoices for my corporate client immediately and win the highest NET discount while immediately letting my client validate that the invoice was executed and the money paid, and also so that I don't need to build another system for innovative factoring use cases and government oversight measures — one API for all. I want to do this at a market-level, so that I don’t have to build one for each of my client relationships, and so that I can spread the cost of building and maintaining the system.
Repurchase Agreements As a repurchase agreement trader, I need a transparent marketplace of bids and asks, so that I can discover, trade, and execute agreements with relative assurance that there will be no repudiation or other issues. I don’t want to have to be subject to the string of counterparties exerting control over the market; rather, I want to be an equal partner in the network, trade directly, and spread the costs/risks.
Supply Chain and Self-Executing B2B Contracts As a corporate buyer, I want to be able to submit my purchase contract to a network I share with the supplier, which will convert the agreement into a validated, trusted, self-executing process, so that when the PO is appended to the ledger, supply has been received, and other events occur, the terms of the contract are automatically executed, and both the suppler, me (the buyer), our banks, logistics partners and other stakeholders all can have visibility and be assured of proper completion of the transaction.

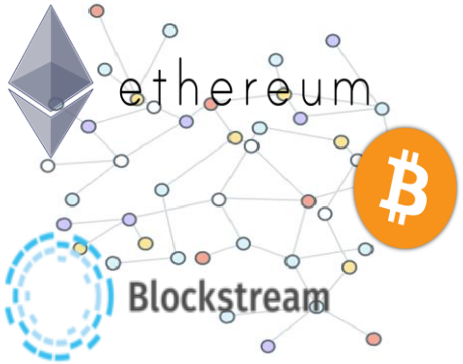
IBM – Financial Services use cases for Blockchain

Blockchain for Banking Consortia	
Security Services	**Security Settlement:** Once financial assets are dematerialized on a shared ledger, all stakeholders will have direct access to the asset depository and the power to settle trades, without always going through intermediaries needlessly. **Post Trade Operation**: Post trade processes such as trade capture, enrichment, confirmation/affirmation, clearing, and settlement can be automated on shared ledger, potentially reducing post trade operation time from days to seconds. **Trade Repository:** By design, Blockchain is a secure record repository of ordered collection of financial transactions. It records the history of asset control and state changes, reducing the need of maintaining a separate trade repository for record keeping.
Capital Market	**Derivative Trading:** Connect potential buyers and sellers on a decentralized network. Offers placed on Blockchain network can be automatically seen by all participants, the network will be cheaper and potentially bigger than ECNs today because the risk and cost of maintaining the network is spread across all participants (there will not be a single owner charging premium for maintaining the service. **Derivative Post-Trade Management**: Derivatives contracts can be managed and automated through smart contracts on shared ledger, significantly cutting down the management cost and time while reducing the intra-day risk. **Syndicated Loan:** Help borrowers and arrangers to broadcast their offers to all potential investors on a Blockchain network, and to automate the syndication process.
Trade Finance	**Cross-Currency Payment:** Automatically connecting market makers and bypassing intermediaries to significantly reduces time taken for cross currency payment from days to seconds.
Card Operation	**KYC:** Creditor card issuers can record customer credit histories on a shared ledger so that customer information can be easily shared (or sold) between companies.

Why isn't blockchain ready for business?

There are two options for building private network for businesses 1) Reconfigure a public network fabric for private use, or 2) Build on top of a untested private network fabric that's available

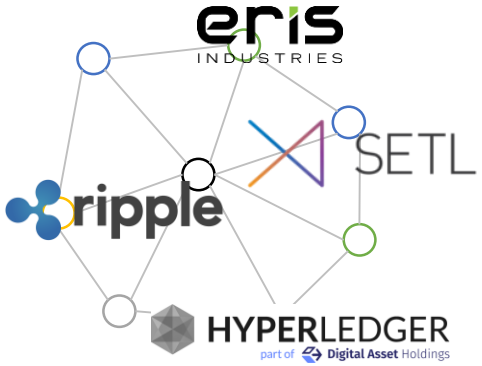
Public Network Fabric



Business Adoption Challenges

1. Designed for public network
2. Slow and inefficient
3. Built-in virtual currency
4. Difficult to push upgrades
5. Heavily forked
6. Lack enterprise support

Private Network Fabric



Business Adoption Challenges

1. Incomplete & usually untested
2. Usually too simple & inflexible
3. Still lack critical enterprise features such as identity management system
4. Generally lack community support
5. Not standardized

IBM – What we bring and what needs to be done

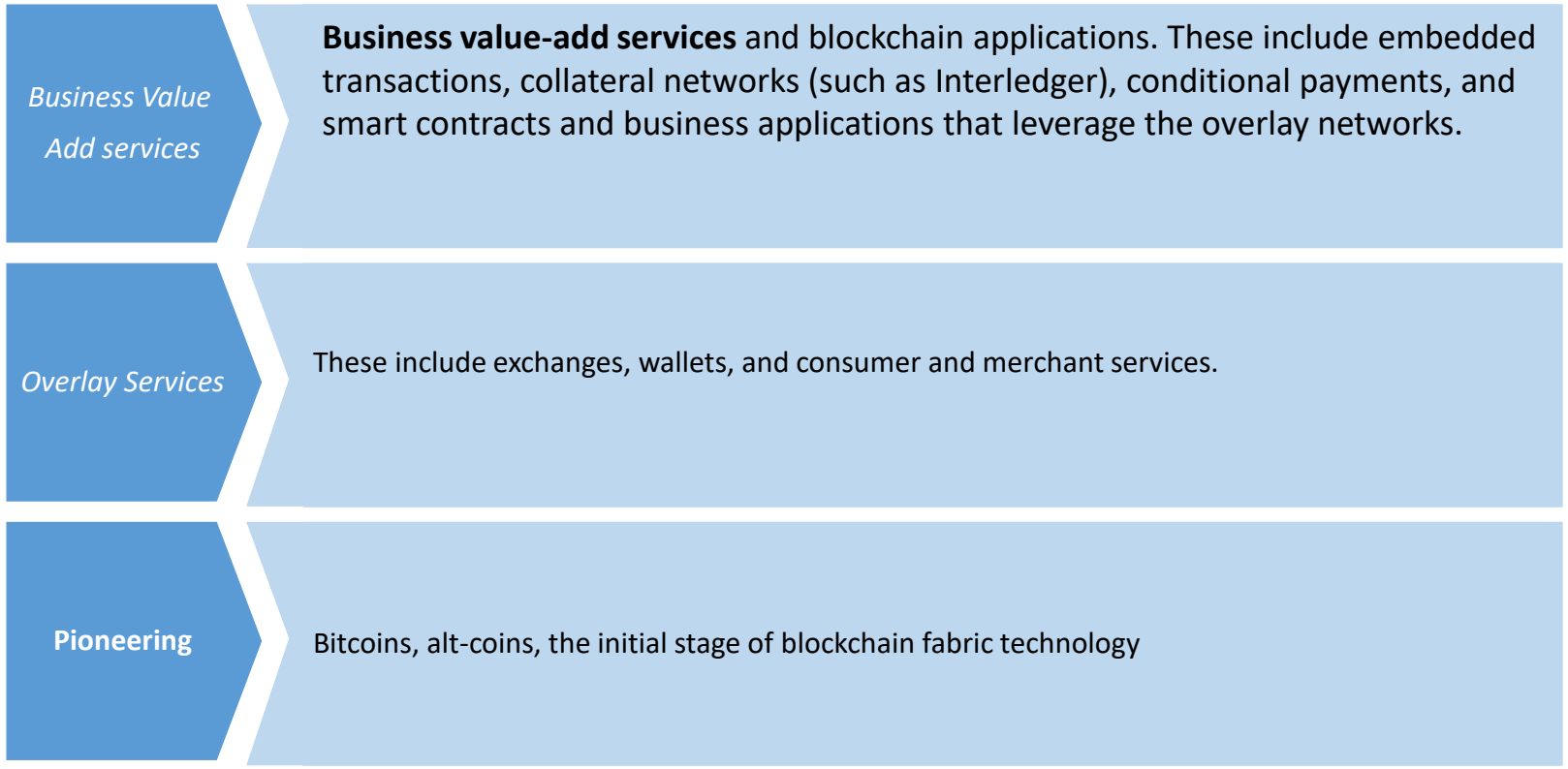
IBM brings the advisory capabilities as well as necessary tools …

- World Wide Cloud with Government Certification : one-click international multi-node geographic deployment of validating Blockchain peers that can be assigned to parties in the network, all on Softlayer.
- World experts in identity and cryptography research, significant IP in works.
- World leader in business rules processing.
- Domain experts in financial services, government systems, and supply chain.

…to execute in this field:

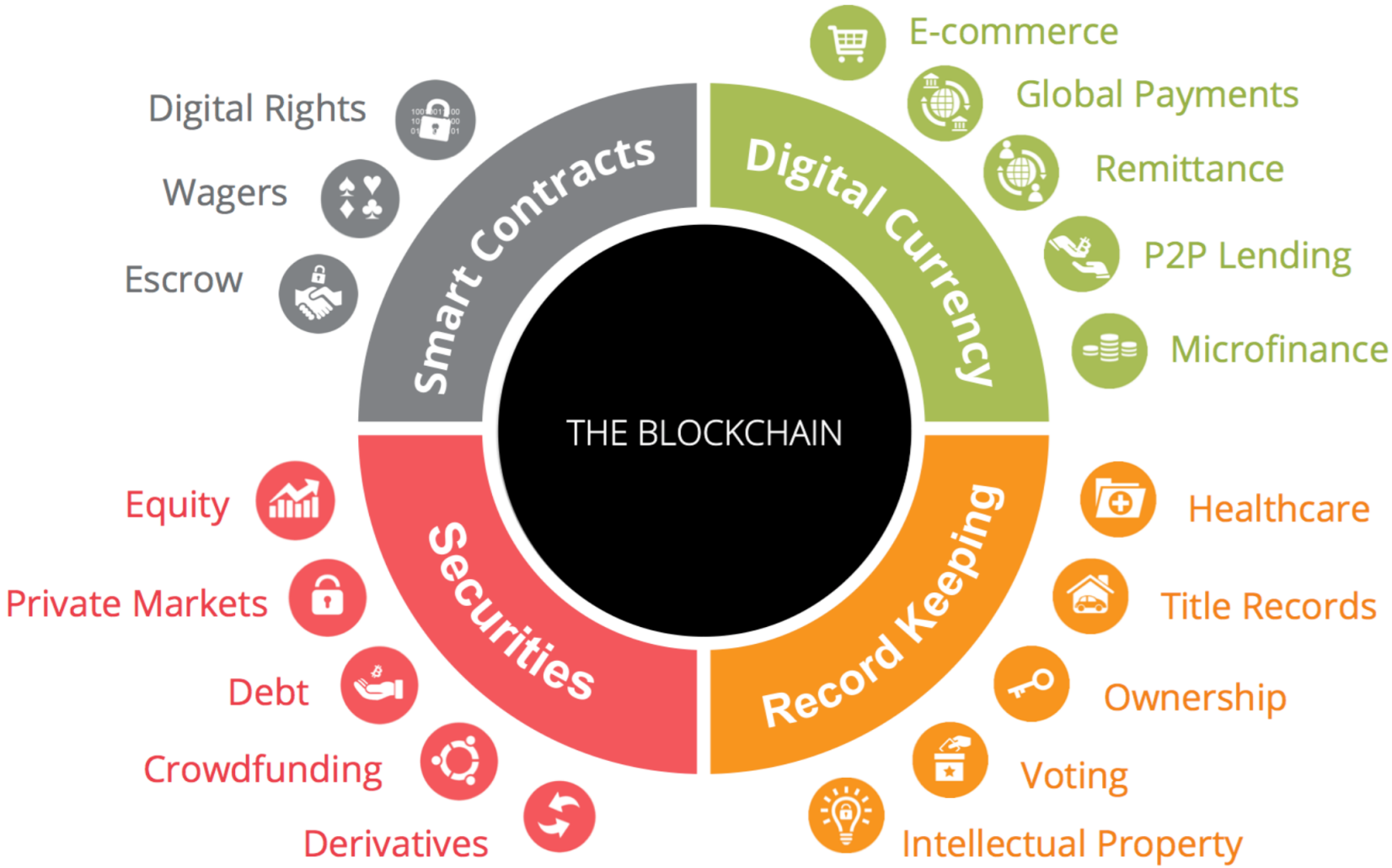
- **Identity, Certificates:** In order to transact on the Blockchain without exposing strategic information to others, a party's identity must be both transparent to the party it's transacting with while opaque to others. This requires sophisticated identity management, which IBM is researching and developing.
- **Inter-network services:** In addition to identity management, current Blockchain platforms are challenged in enabling cross-ledger services. Say, for example, a bank performed KYC on a merchant in one network, and now the same bank is working with the same merchant in another network. Why do KYC twice? IBM can provide the support for this and other cross-network managed operations.

Phases of Blockchain Innovation



Blockchain Potential Applications & Disruption

The blockchain is radically changing the future of transaction based industries



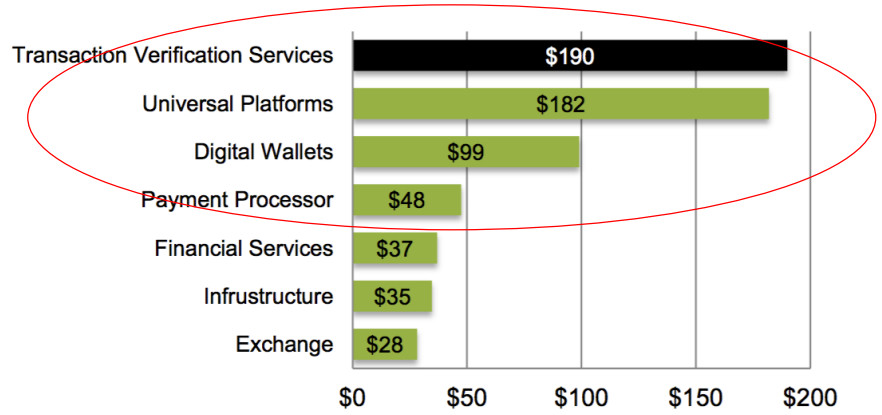
Venture Capital Landscape

- Over $190 million of venture capital funds invested to secure the blockchain, bitcoin's key innovation
- BTCS is the only public company focused on securing the blockchain with a fully integrated solution

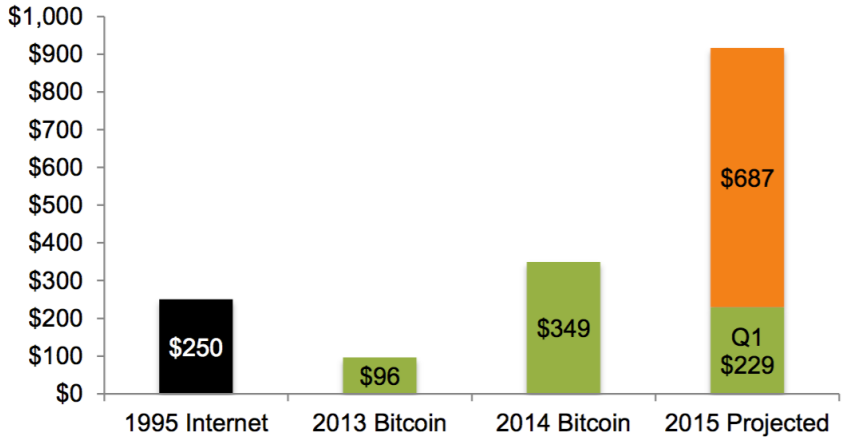
Active Investors

ACCEL PARTNERS
ANDREESSEN HOROWITZ
khosla ventures
venture assistance, strategic advice, venture capital
Goldman Sachs
NYSE New York Stock Exchange
DFJ GROWTH
IDG资本 IDG Capital Partners
WINKLEVOSS CAPITAL
Ribbit Capital
Index Ventures
RRE Ventures
LIGHTSPEED VENTURE PARTNERS

Sector Distribution of Top 15 Funded Companies (millions)



Early Internet VC Investment vs. Blockchain (millions)



Source: CoinDesk.com, as of 4/10/2015

Reference and source

- 1. Bitcoin & Cryptocurrency Technologies: Bitcoin Mining, Blockchain Basics And Cryptocurrency Trading & Investing For Beginners | 7 Books In 1 by Boris Weiser (Author)
- 2. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Crypto Trading, Derivatives, Digital Assets) – Illustrated, September 15, 2018 by Antony Lewis (Author)
- 3. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World – June 12, 2018 by Don Tapscott (Author), Alex Tapscott (Author)
- 4. Blockchain Technology for IoT Applications (Blockchain Technologies) 1st ed. 2021 Edition
- by Seok-Won Lee (Editor), Irish Singh (Editor), Masoud Mohammadian (Editor)
- 5. Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher (Author) Format
- 6. Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond – October 19, 2017 by Chris Burniske (Author), Jack Tatar (Author)