Blockchain and Cryptocurrencies

The potential to rewire financial services and other systems?

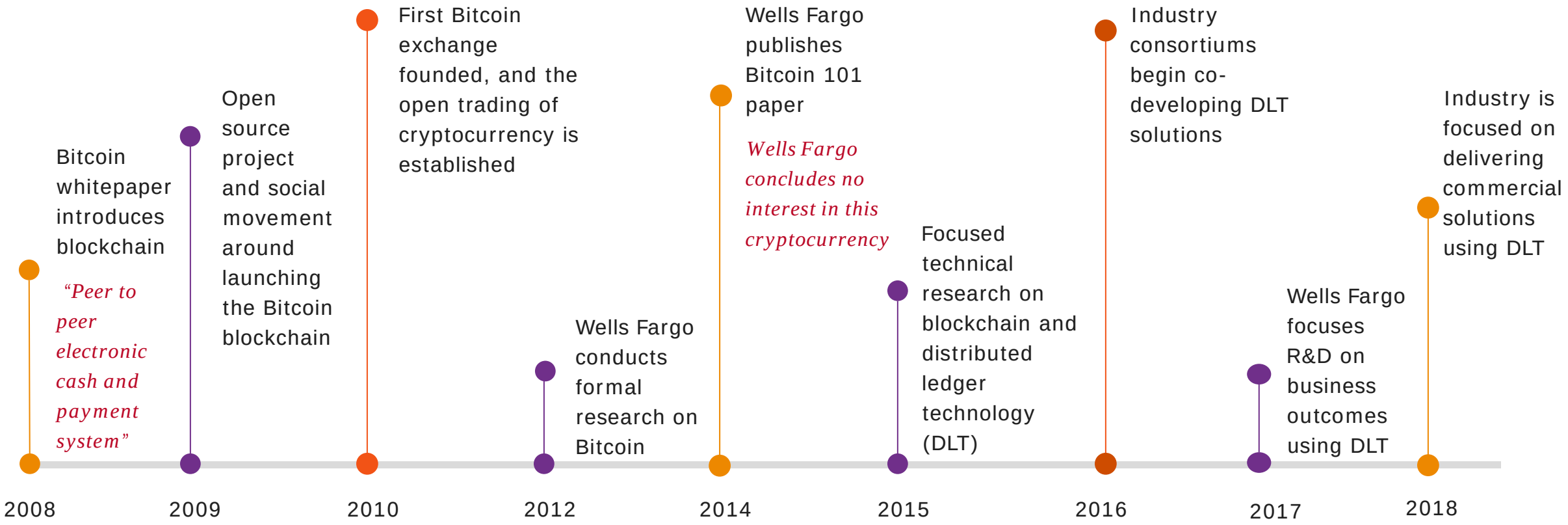
Steven Shafer

Treasury Management Sales Consultant

May 22, 2018


SEGA
GENESIS
16-BIT
POWER
ON
OFF
RESET
VOLUME

A brief history of blockchain and distributed ledger technology



What is blockchain?

- A blockchain is a distributed ledger of transactions that have been validated through a consensus mechanism between members in a network.

- Transactions are chronologically grouped into blocks of data, each cryptographically linked to predecessor transactions down to the genesis block, thereby creating a chain of blocks.

- Since each block draws upon the “hashed” data reference of the previous block in the chain, it is virtually impossible to add, remove or change data without being detected by other members in the network.

How does a blockchain work?

Current Blockchain

Transaction 999
Transaction 998
Transaction 997

Reference to Prior Block

Transaction 996
Transaction 995
Transaction 994

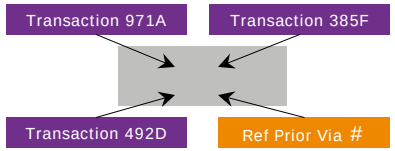
Reference to Prior Block

Transaction 993
Transaction 992
Transaction 991

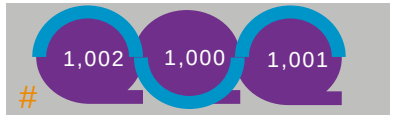
Reference to Prior Block

Adding a New Block

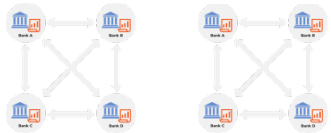
Record recent transactions in the network, each with a timestamp, and bundle them into a block, also with a timestamp and with a reference to the prior block.



Secure the block in the network using cryptography and computing power to create a “hash” that represents the data, and verify it to prove that the prior hashes all match up and therefore the new block hash is legitimate.



Add the new block to the chain and distribute it to the network as appropriate.



Updated Blockchain

Transaction 1,002
Transaction 1,001
Transaction 1,000

Reference to Prior Block

Transaction 999
Transaction 998
Transaction 997

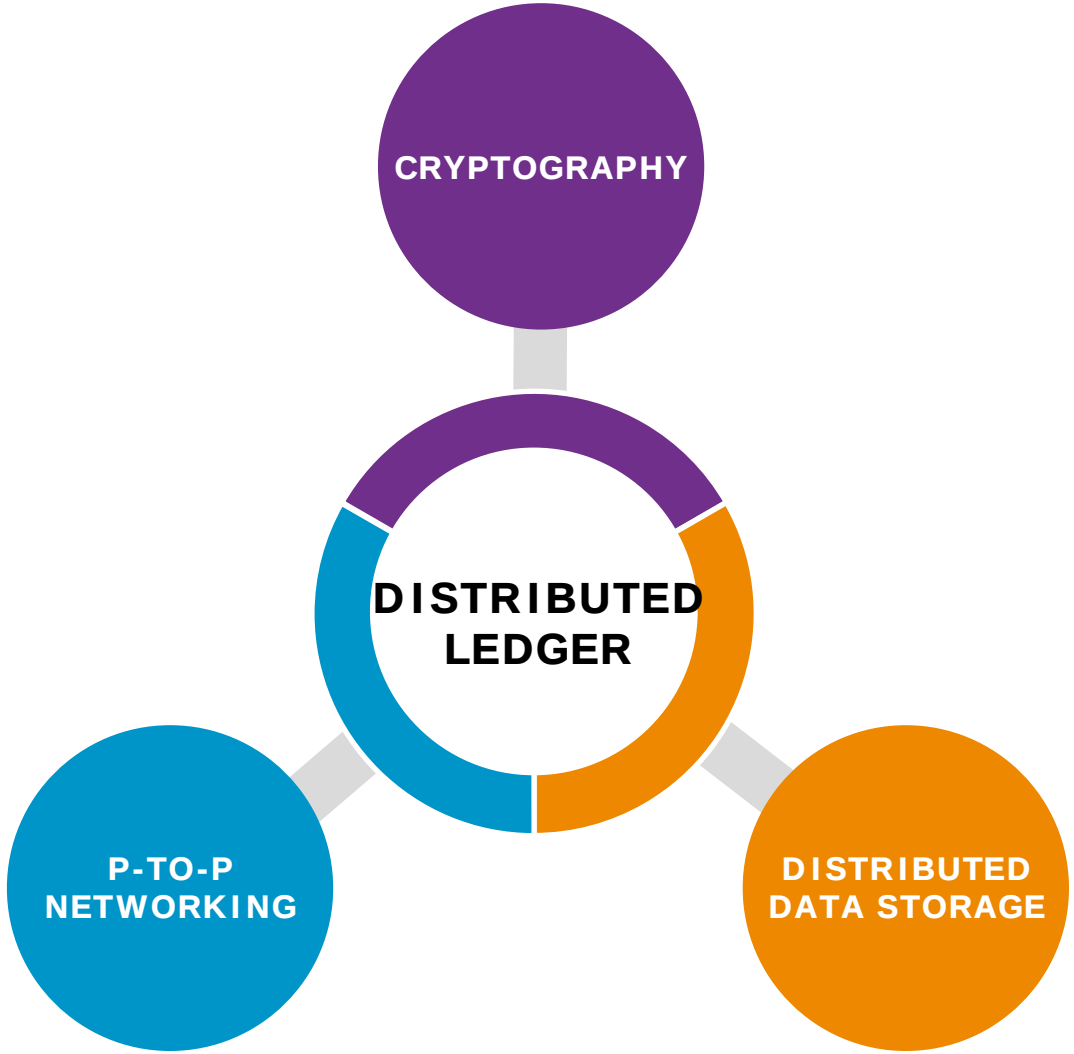
Reference to Prior Block

Transaction 996
Transaction 995
Transaction 994

Reference to Prior Block

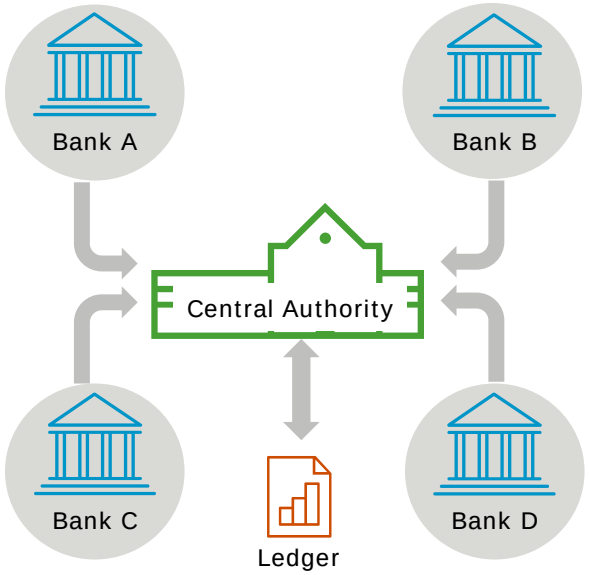
Blockchain versus Distributed Ledger Technology (DLT)

- A blockchain is just one type of distributed ledger, and not all distributed ledgers necessarily employ blocks or chain transactions.
- A distributed ledger is comprised of three core technologies combined in different arrangements depending upon the use case.
  - **Cryptography** – securely validates identity, permissions and transactions on the network
  - **Distributed data storage** – ensures shared view of the same data and eliminates the need for reconciliation
  - **Peer-to-peer networking**– connects participants to shared data in real time



Why DLT?

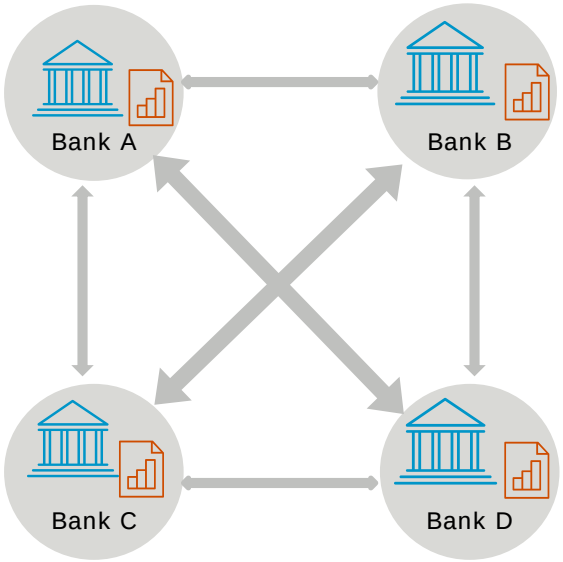
Centralized Ledger



- Transactions are recorded by a central, trusted authority maintaining a centralized ledger that must be reconciled with each participants copy of the ledger
  - Limited visibility into business records due to multiple non-standard data sources and external parties also with multiple sources of data
  - Inter-transaction dependencies which need to be verified due to central administrator and SOR
  - Lack of data standards and security of data in reconciliation processes

Why DLT?

Distributed Ledger



- Transactions are recorded on a common, shared ledger and confirmed by participants in real time, thus creating trust in the network and eliminating the need for reconciliation
  - Removes intermediary parties to settlement, saving time and reducing operational expense
  - Records are committed only once consensus is achieved thus eliminating reconciliation, and creating a reusable trusted source of data
  - Greater security with “immutable records” such that the system itself can be used for irrefutable evidence and regulatory scrutiny

DLT examples: financial services

Global Payment Services

Improve operations around cross currency exchange of value to reduce risk.

Lending & Trade Finance

Open new markets in trade finance with better financial terms than currently exist.

Investment Banking and Capital Markets

Reduce or remove the need for many post-settlement operations, and add efficiencies of scale; explore tokenization to increase asset utility.

Identity Services

Improve client engagement and experience with mutualized internal customer data management.

DLT examples: other companies

Cross Border Payments

Improve operations around cross currency exchange of value to reduce risk.

Smart Contracts

Executes contracts publically stored while maintaining privacy of the individuals involved

Shared Data

Sharing Healthcare and Food distribution information across borders, both inter and intra-company; i.e. tracing a head of lettuce from the grocery store back to the specific source farm

Personal Identification Records

Validate specific driver's license and passport information

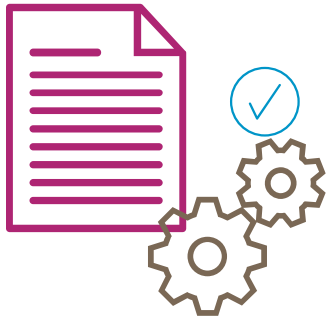
Smart Contracts

Blockgeeks

1

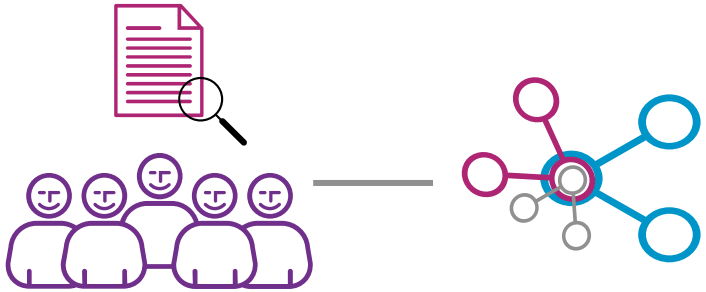
An option contact between parties is written as code into the blockchain. The individuals involved are anonymous, but the contact is the public ledger.

2



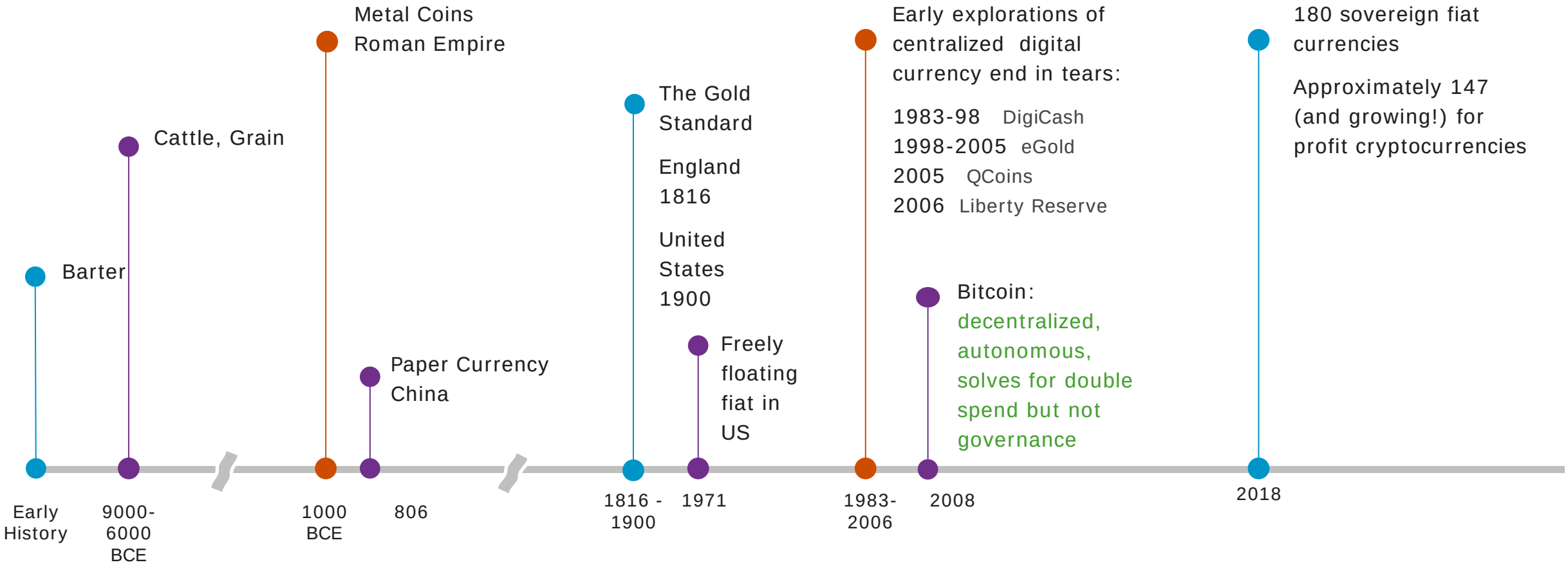
A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

3



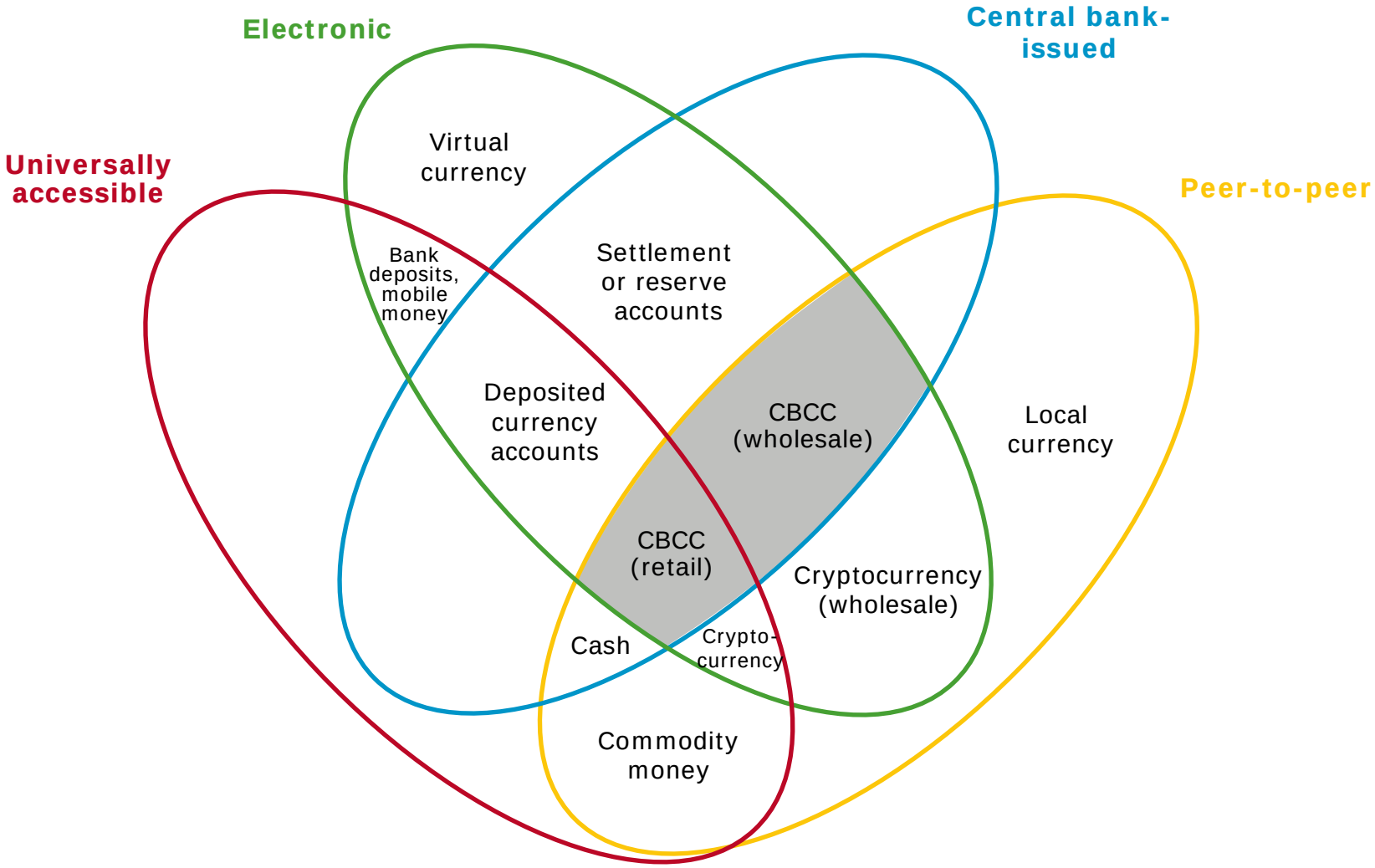
Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions

A brief history of currency - value stores and transfer mechanisms



What is next for currency?

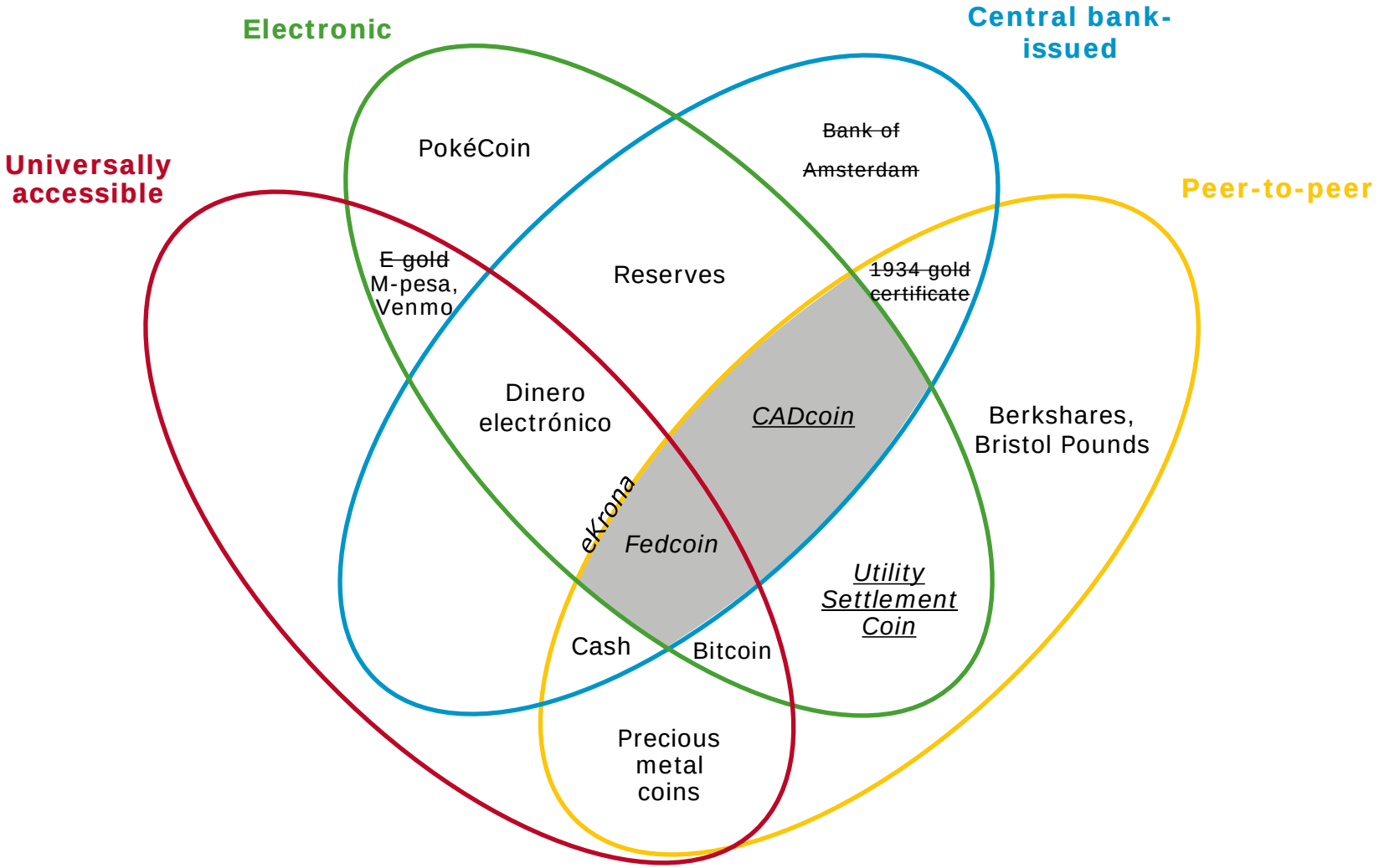
The Money Flower: A Taxonomy of Money



Source: https://www.bis.org/publ/qtrpdf/r_qt1709z.htm

What is next for currency?

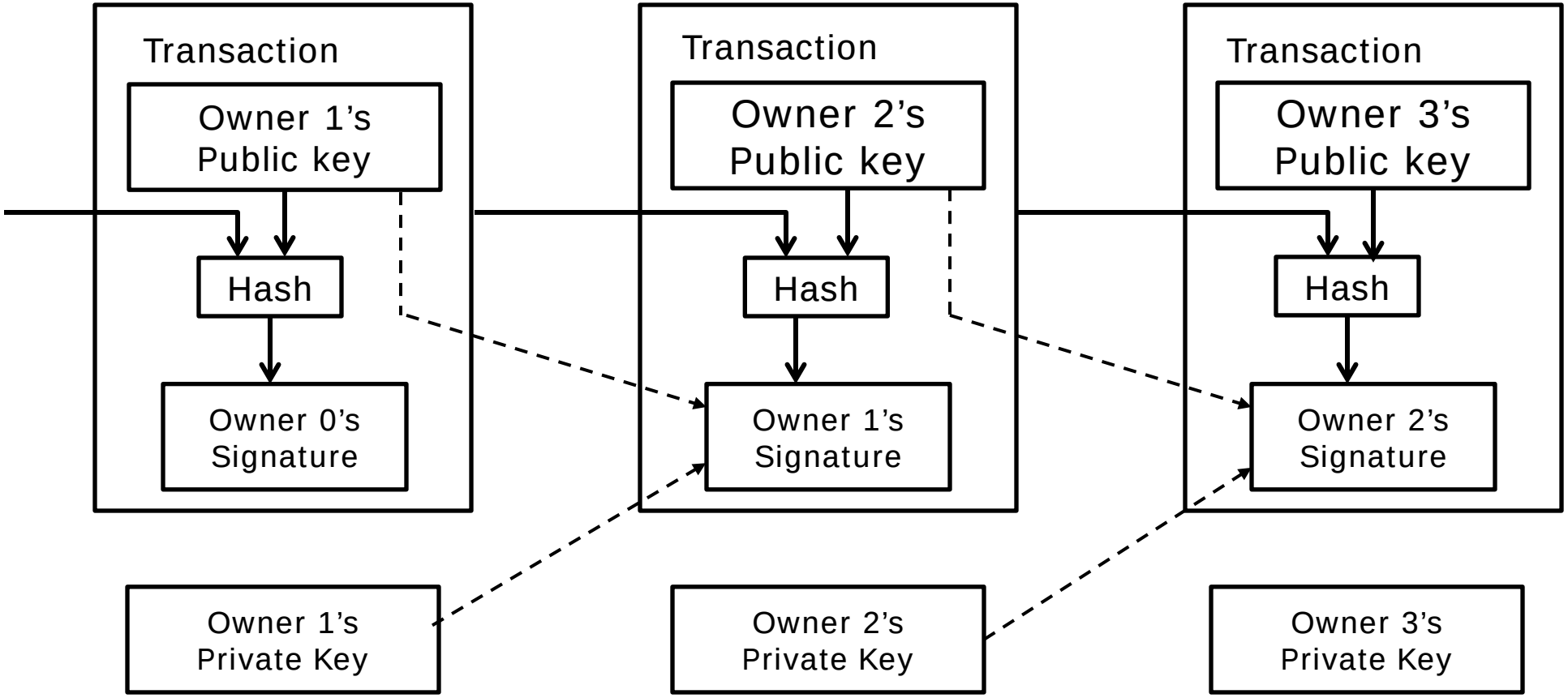
The Money Flower: Examples ~~Past~~, Present and *Future*



A standard font indicates that a system is in operation; an *italic* font indicates a proposal; an *italic and underlined* font indicates experimentation; a ~~strikethrough~~ font indicates a defunct company or an abandoned project.

Source: https://www.bis.org/publ/qtrpdf/r_qt1709z.htm

Bitcoin transfer: Blockchain example



Key considerations around cryptocurrencies

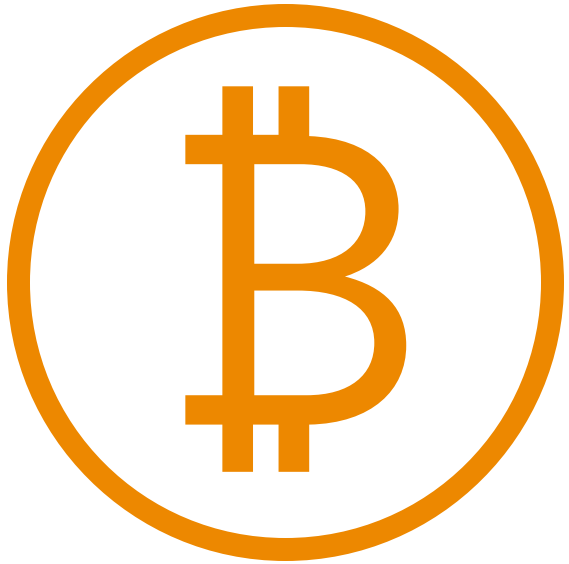
- **Digital assets** and **not currencies**
  - Value token: Bitcoin, Ether, LiteCoin, etc.
  - Utility token: Used to enable access to services
  - Equity token: Acts as a security investment
- 100% speculation
- Extremely volatile
- Intensive integration required for point of sale or accounts receivables/ payables transactions
- Central Bank Digital Currency (CBDC) will eventually emerge, with negative impact on current cryptocurrencies without similar governance or backing

What is the potential path to legitimacy for cryptocurrencies or any tokenized asset?

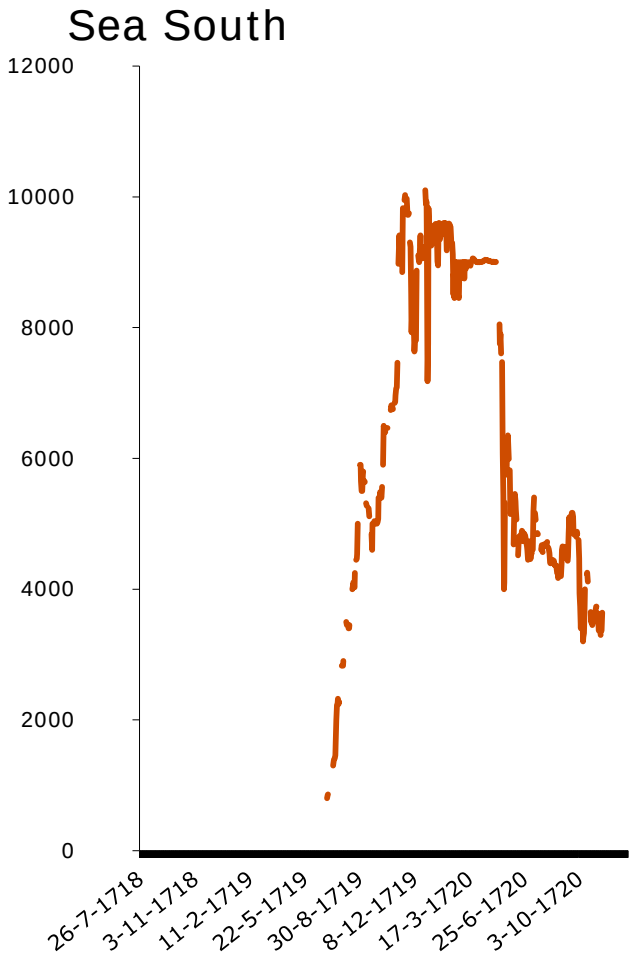
- New Avenues for Value Exchange?
  - Autonomous units of value, for a global audience that wants unlimited access to a fungible digital asset
  - Universal Payment Network, in production for cross border remittances via the Stellar Network
  - xRapid, a possible new RTGS or cross border remittance platform
  - A potential front runner DLT platform for a central bank digital currency (CBDC)
  - Utility Settlement Coin (USC) Project, for tokenized depository receipts at central banks
- Value Stores?
  - ICOs – Intended for access to distributed application services; sadly being wildly misused www.deadcoins.com
  - Tokenized assets – Potential to create liquidity, like digitized paper-based securities
- Value Exchange and Store?
  - Open market crypto exchanges vs Central Bank Digital Currency

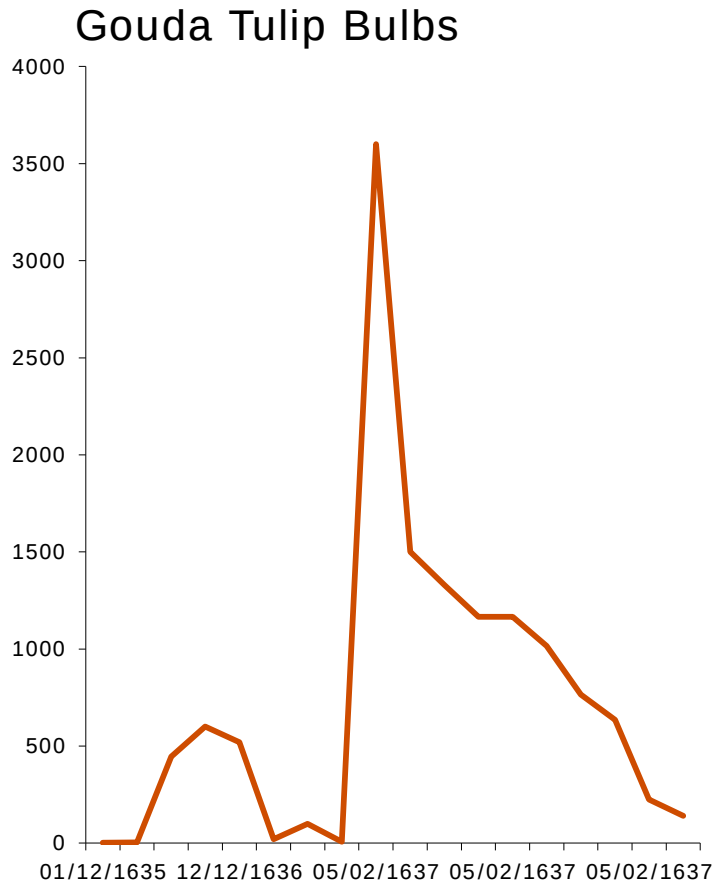
Other cryptocurrencies

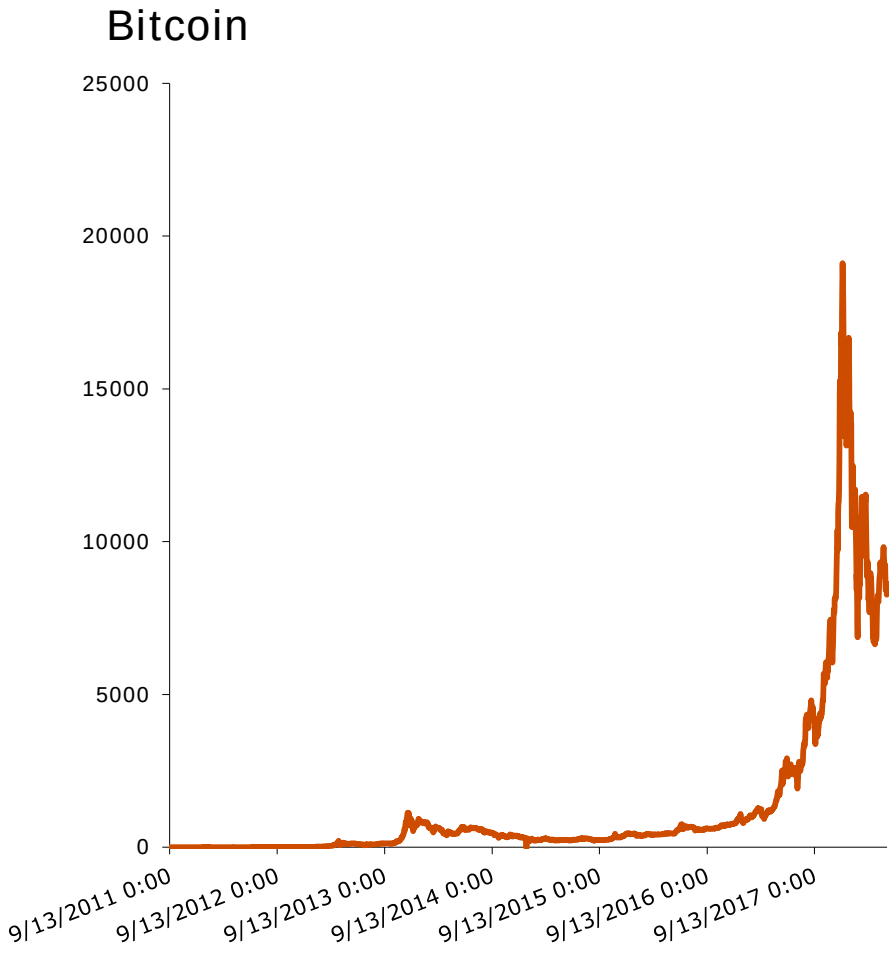
- Ethereum
- Bitcoin Cash
- Ripple
- Litecoin
- Dash
- IOTA
- Monero



The thing about bubbles – they can hang out there for a while...

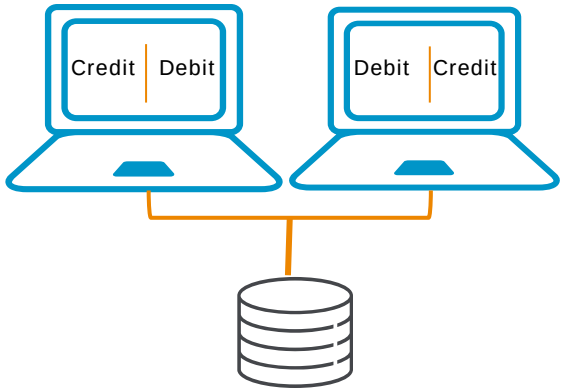






Evolution of Trust and Architectures

Internal Transaction Systems

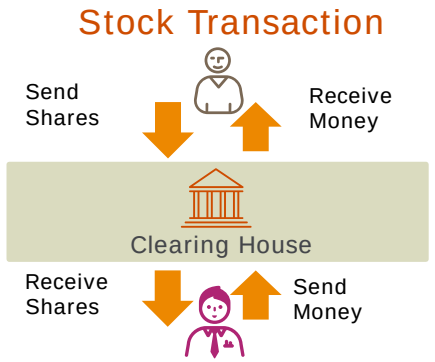


- **Architecture**: Centralized internal database (e.g. IBM, Oracle)
- **Settlement Process:** Internal
- **Speed:** Real-time
- **Transaction Cost:** Internal It
- **Benefits:** Speed, cost and (relative) simplicity
- **Limitations:** Committing transactions with third parties/across network

Middleware/ Messaging

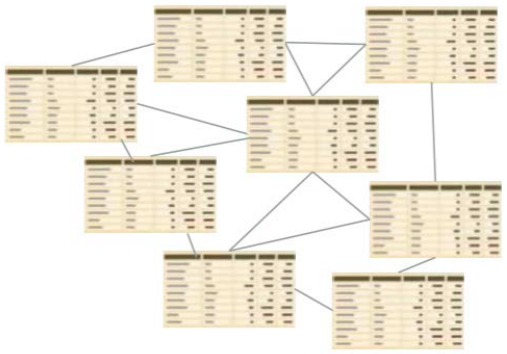
- **Architecture**: Secure inter-party messaging/queue-based middleware
- **Settlement Process:** Independent (but enabled by messaging)
- **Speed:** Up to 3-5 days
- **Transaction Cost:** External provider + settlement costs
- **Benefits:** Secure transaction between external parties, standardized data formats
- **Limitations:** Data errors slow transactions, flexibility

Clearing Houses



- **Architecture**: Third party agent-in-possession
- **Settlement Process:** Via clearing house
- **Speed:** Days (transaction dependent)
- **Transaction Cost:** Third-party service
- **Benefits:** Reduced settlement risk/DVP
- **Limitations:** Complex and cumbersome, expensive

Blockchain



- **Architecture**: Distributed ledger with cryptographic integrity
- **Settlement Process:** Consensus
- **Speed:** Near real-time to minutes
- **Transaction Cost:** Similar to internal databases
- **Benefits:** Enables third-party transaction to be as simple and efficient as internal transactions
- **Issues:** Tech maturity, integration with existing systems/workflows

Source: Magister Advisors

Key Concepts Summary

Concept	Bitcoin	Ethereum	Fabric	Corda	Quorum
Blockchain and/or Distributed Ledger	One blockchain containing all transactions, there are no states	One blockchain containing all transactions and states	Multiple blockchains containing all transactions and states which can be segregated into channels, with each channel having its own ledger	A decentralized database solution but not a blockchain, because by design data is not propagated to all network participants and is not stored in blocks	One blockchain containing all transactions in the *Public* state, where each member also maintains a unique *Private* state about transactions in which it participates
Consensus Mechanism	Proof of Work, with mining	Proof of Work, with mining Proof of Stake soon to be available	Kafka, with other options pluggable	Notaries, with other options pluggable	Public: Proof of Work, with mining Private: RAFT and BFT
State Tracking Model	Stateless, UTXO	Account-based and with states	Agnostic, but uses ordering service with endorsers	Transaction-based with UTXO, and a Notary service	Account-based and with states
Data and Transaction Management	Federally decentralized	Federally decentralized	Channels – assets are on a pre-defined list of selected peers, no one leaves and no ones joins without considerable configuration effort	Flows – states and messages and other network traffic only travels between nodes connected point to point and which are only 'need to know', and a Vault is used to store data	States – Public and Private data are managed separately, with payloads only distributed to transacting parties
Smart Contracts	No	Yes, called Smart Contracts, written in Solidity	Yes, called Chaincode, written in GoLang	Yes, called Smart Contracts, written in Kotlin or Java	Yes, called Smart Contracts, written in Solidity
Native Assets	Bitcoins are the byproduct of mining for the consensus logic, intended to create virtuous action by all participants without requiring trust	Ether is the byproduct of mining for the consensus logic, intended to create virtuous action by all participants without requiring trust Also, the ERC20 specification can be used to tokenize any assets, which are hosted by an Ethereum address and sent by Ethereum transactions	No native asset Assets are a defined as a collection of key-value pairs, with state changes recorded as transactions on a channel in binary and/or JSON form	No native asset Uses a built-in Java type asset called 'Issued' for modeling any issued product (such as cash, or anything quantifiable)	No native asset Similar to Ethereum but without the Ether
Network Type	Permissionless	Permissionless	Permissioned	Permissioned	Permissioned
Participant Management	Anyone can join	Anyone can join	Each participant is managed via X.509 certificates by default, with additional policies that can govern what each can do on the network	Each participant is managed via X.509 certificates	Each node maintains a permissioned-nodes.json file, with a role of: Maker and/or Voter, or Observer
Governance	None	Ethereum Foundation, a Swiss nonprofit	Linux Foundation, a 501(c)(6) nonprofit	R3	JPM

References

https://digital.wf.com/treasuryinsights/portfolio-items/tm13039/

https://p1xhr2w8ts37fbalioe6qfro-wpengine.netdna-ssl.com/treasuryinsights/wp-content/uploads/sites/9/2016/09/infographic-12104.pdf?pdf=tm12104-pdf

https://www.youtube.com/watch?v=SSo_EIwHSd4

https://youtu.be/lik9aaFIsl4

https://youtu.be/kubGCSj5y3k

https://youtu.be/-mgxEhIvSTY

https://global.delaware.gov/2016/06/10/the-delaware-blockchain-initiative-potential-amendements-to-the-delaware-general-corporation-law/