BitCoin

Pete Treese

Is it a Software?

Is Bitcoin a Soap Opera?

It is a Token?

HardFork Teaser Trailer

Ethereum got Forked

Milestones [edit]

Release Date	Code name	Milestones & Hard Forks
July 30, 2015	Frontier	The release of the Ethereum Genesis block.[31]
March 14, 2016	Homestead	The 2nd major release of the Ethereum platform, which introduced EIP-2, EIP-7, and EIP-8.[32]
October 25, 2016	GasReprice	First fork after being renamed "Ethereum Classic". Repriced some operations to prevent DoS attacks affecting both Ethereum and Ethereum Classic networks. Introduced ECIP-1050.[33]
January 14, 2017	Die Hard	Delayed the difficulty bomb which was originally intended to force the network to move from proof-of-work to proof-of-stake and added replay protection to prevent transactions on the Ethereum network being accepted on the Ethereum Classic chain. Introduced ECIP-1010 and EIP-155.[34]
December 11, 2017[35]	Monetary policy change	Change unlimited token emission to a fixed-cap monetary policy similar to bitcoin with a hard cap of around 210 Million.[36]

Blockchain != Bitcoin

There is not one blockchain protocol

Multiple implementations of blockchain related protocols :

- Hyperleger Project @ Linux Foundation
- R3 Corda
- Ethereum
- Ripple
- Stellar
- Factom
- ...and many more

Key differentiating elements between blockchain protocols:

- Permission model (private vs. public)
- Consensus approach
- Smart contracts
- Extensibility & programmability
- APIs
- Scalability & latency
- Resource consumption

Hyperledger Fabric: a step in blockchain evolution

2009
Bitcoin

- **Hard-coded cryptocurrency application w. limited stack-based scripting language**
- **Proof-of-work-consensus**
- **Native cryptocurrency (BTC)**
- **Permissionless blockchain system**

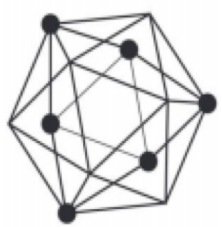
Blockchain 1.0

2014
Ethereum

- **Distributed applications (smart contracts) in a domain-specific language (Solidity)**
- Proof-of-work-consensus
- Native cryptocurrency (ETH)
- Permissionless blockchain system

Blockchain 2.0

2017
Hyperledger
Fabric

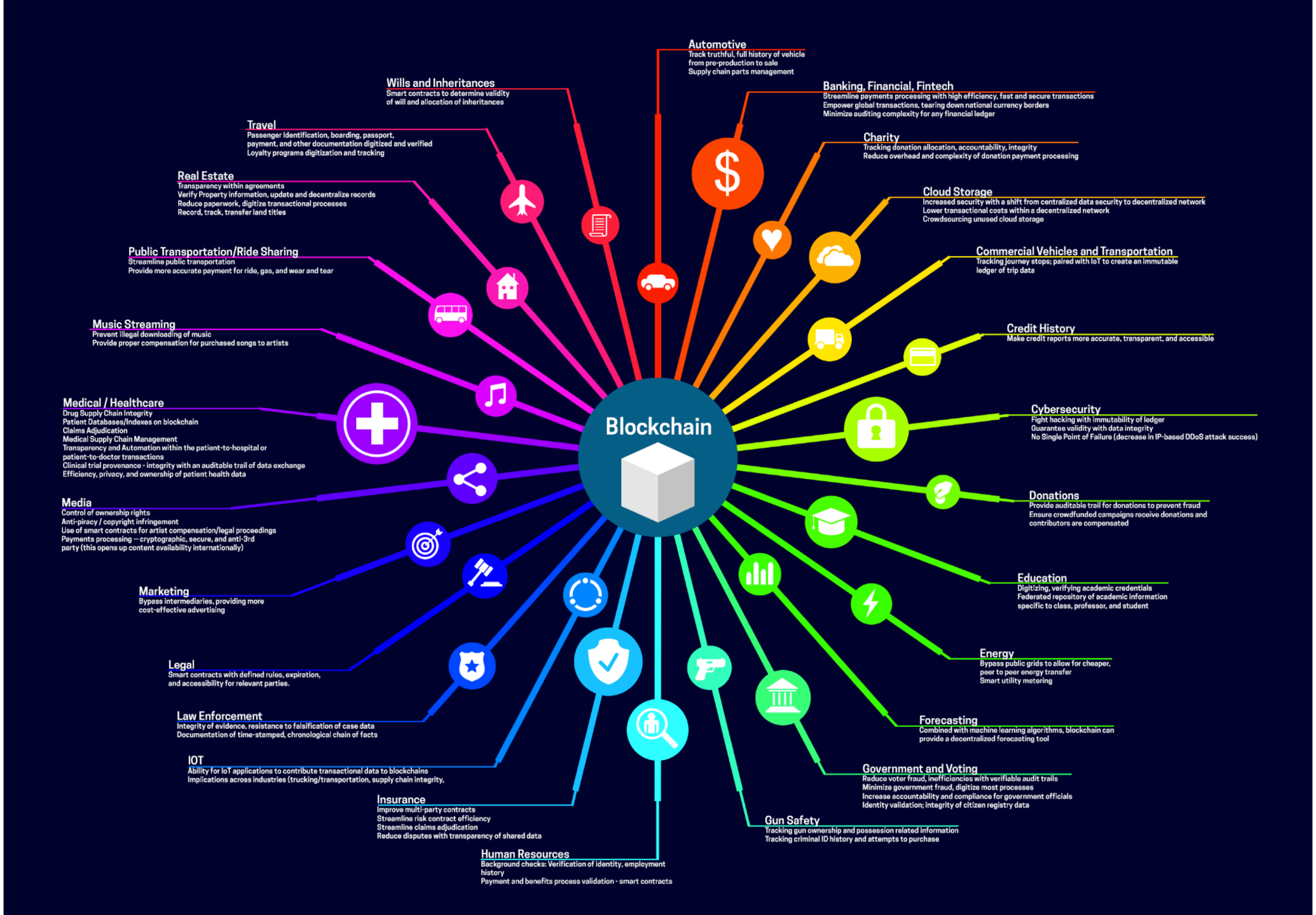


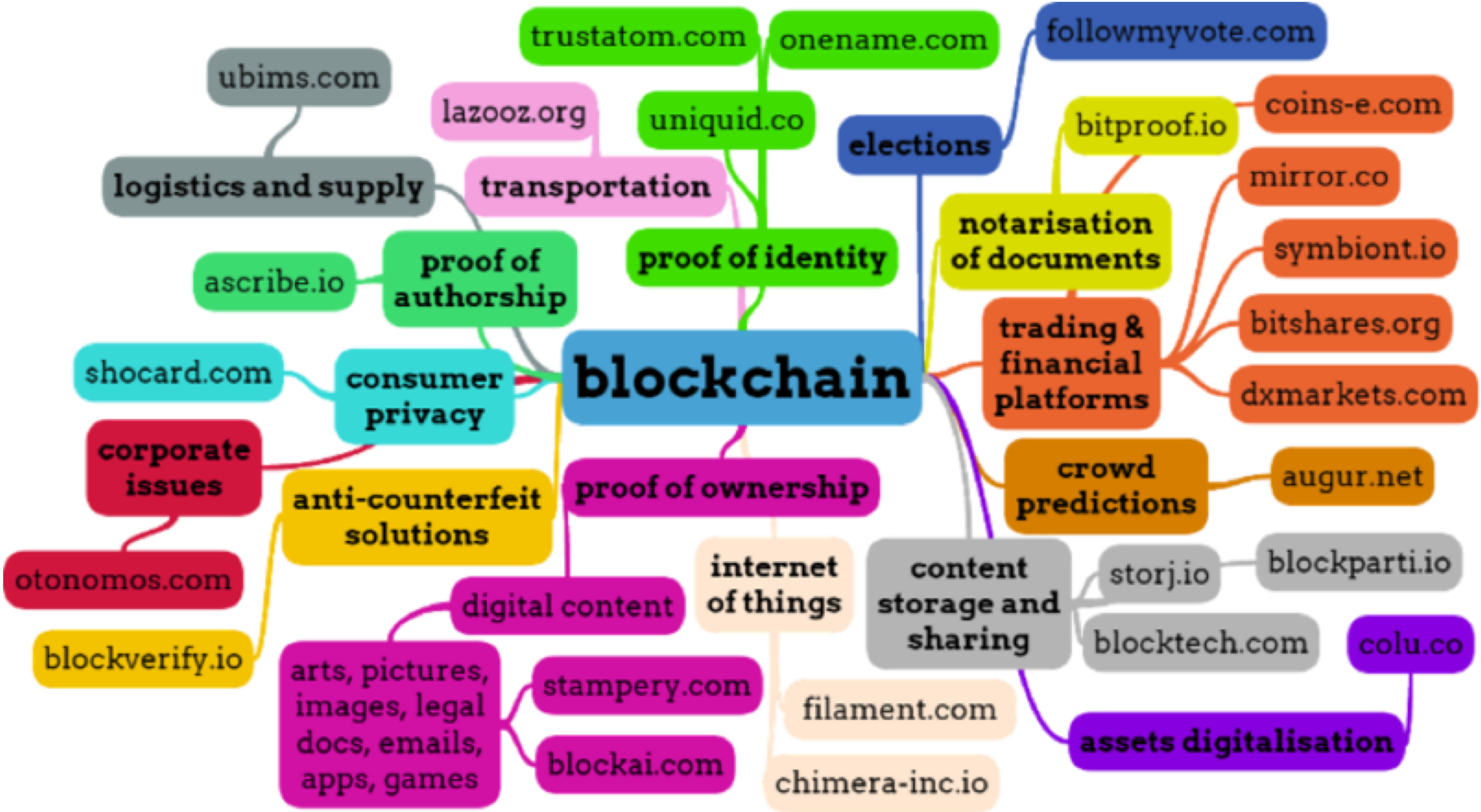
- **Distributed applications (chaincodes) in different general-purpose languages (e.g., golang, Java)**
- **Modular/pluggable consensus**
- **No native cryptocurrency***
- Permissioned blockchain system

Blockchain 3.0

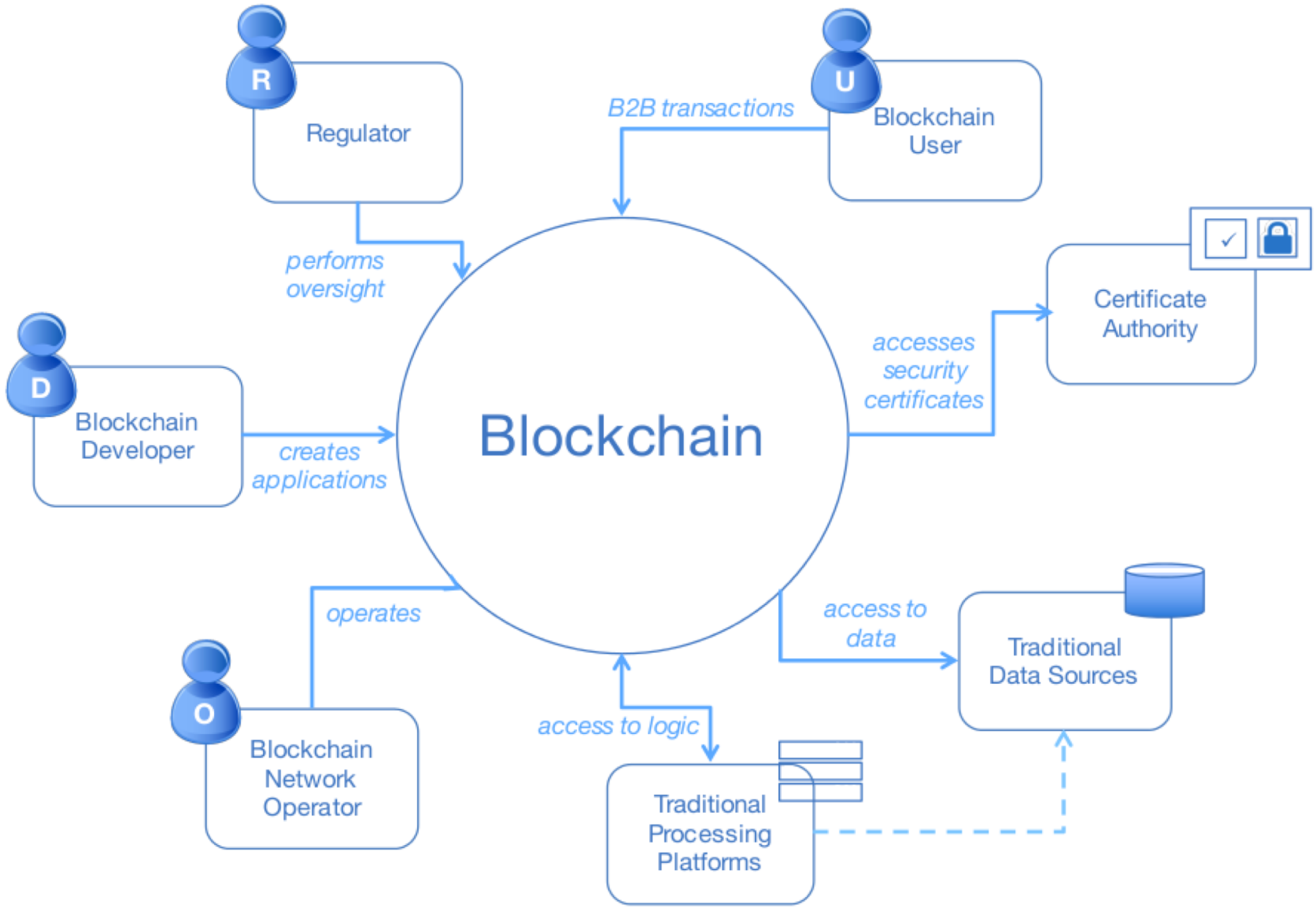
Qualitative View:Hyperledger Fabric, Ethereum, Quorum

Metrics	Hyperledger Fabric	Ethereum	Quorum
Throughput	> 2000 tps	~ 200 tps Some at 16 tps	A few 100s
Consensus	- Pluggable - Trusted Solo - Crash fault tolerant Kafka	Proof of work	- Pluggable - Raft consensus - Istanbul BFT
Database & Query	Get/Put/Range-query over GolevelDB and CouchDB during blockchain transaction	Get/Put over levelDB	Get/Put over levelDB
Access Control	Organization level access control on channels and attribute & role-based access control in smart-contract	Attribute and role-based access control in smart-contract	Attribute and role-based access control in smart-contract
PrivateDB within a chain (data privacy)	Multiple private collections each with a different set of members. A transaction can span both private and publicDB.		Single private DB per node and double spending cannot be identified without using Zero Knowledge Proof. A transaction cannot span both private and publicDB.
Co-hosting of Non-Blockchain Data			
Tokens / Cryptocurrency		Ether	Ether
Zero Knowledge Proof			
Transaction Endorsement			
Multi-tenancy	Supported using channels		
Transaction Privacy	Supported across channels but not within a channel even when using privateDB		Supported even with privateDB
Time Oracle			
Pruning of Blocks and			


Blockchain
Automotive
Track truthful, full history of vehicle
from pre-production to sale
Supply chain parts management
Wills and Inheritances
Smart contracts to determine validity
of will and allocation of inheritances
Banking, Financial, Fintech
Streamline payments processing with high efficiency, fast and secure transactions
Empower global transactions, tearing down national currency borders
Minimize auditing complexity for any financial ledger
Travel
Passenger Identification, boarding, passport,
payment, and other documentation digitized and verified
Loyalty programs digitization and tracking
Charity
Tracking donation allocation, accountability, integrity
Reduce overhead and complexity of donation payment processing
Real Estate
Transparency within agreements
Verify Property information, update and decentralize records
Reduce paperwork, digitize transactional processes
Record, track, transfer land titles
Cloud Storage
Increased security with a shift from centralized data security to decentralized network
Lower transactional costs within a decentralized network
Crowdsourcing unused cloud storage
Public Transportation/Ride Sharing
Streamline public transportation
Provide more accurate payment for ride, gas, and wear and tear
Commercial Vehicles and Transportation
Tracking journey stops; paired with IoT to create an immutable
ledger of trip data
Music Streaming
Prevent illegal downloading of music
Provide proper compensation for purchased songs to artists
Credit History
Make credit reports more accurate, transparent, and accessible
Medical / Healthcare
Drug Supply Chain Integrity
Patient Databases/Indexes on blockchain
Claims Adjudication
Medical Supply Chain Management
Transparency and Automation within the patient-to-hospital or
patient-to-doctor transactions
Clinical trial provenance - integrity with an auditable trail of data exchange
Efficiency, privacy, and ownership of patient health data
Cybersecurity
Fight hacking with immutability of ledger
Guarantee validity with data integrity
No Single Point of Failure (decrease in IP-based DDoS attack success)
Media
Control of ownership rights
Anti-piracy / copyright infringement
Use of smart contracts for artist compensation/legal proceedings
Payments processing -- cryptographic, secure, and anti-3rd
party (this opens up content availability internationally)
Donations
Provide auditable trail for donations to prevent fraud
Ensure crowdfunded campaigns receive donations and
contributors are compensated
Marketing
Bypass intermediaries, providing more
cost-effective advertising
Education
Digitizing, verifying academic credentials
Federated repository of academic information
specific to class, professor, and student
Energy
Bypass public grids to allow for cheaper,
peer to peer energy transfer
Smart utility metering
Legal
Smart contracts with defined rules, expiration,
and accessibility for relevant parties.
Forecasting
Combined with machine learning algorithms, blockchain can
provide a decentralized forecasting tool
Law Enforcement
Integrity of evidence, resistance to falsification of case data
Documentation of time-stamped, chronological chain of facts
Government and Voting
Reduce voter fraud, inefficiencies with verifiable audit trails
Minimize government fraud, digitize most processes
Increase accountability and compliance for government officials
Identity validation; integrity of citizen registry data
IOT
Ability for IoT applications to contribute transactional data to blockchains
Implications across industries (trucking/transportation, supply chain integrity,
Insurance
Improve multi-party contracts
Streamline risk contract efficiency
Streamline claims adjudication
Reduce disputes with transparency of shared data
Gun Safety
Tracking gun ownership and possession related information
Tracking criminal ID history and attempts to purchase
Human Resources
Background checks: Verification of identity, employment
history
Payment and benefits process validation - smart contracts


blockchain
proof of identity
trustatom.com
onename.com
uniquid.co
lazooz.org
transportation
ubims.com
logistics and supply
proof of authorship
ascribe.io
consumer privacy
shocard.com
corporate issues
otonomos.com
anti-counterfeit solutions
blockverify.io
proof of ownership
digital content
arts, pictures, images, legal docs, emails, apps, games
stampery.com
blockai.com
internet of things
filament.com
chimera-inc.io
elections
followmyvote.com
notarisation of documents
bitproof.io
coins-e.com
trading & financial platforms
mirror.co
symbiont.io
bitshares.org
dxmarkets.com
crowd predictions
augur.net
content storage and sharing
storj.io
blockparti.io
blocktech.com
assets digitalisation
colu.co

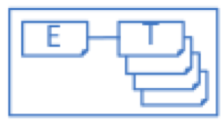
Participants in Hyperledger Blockchain Network



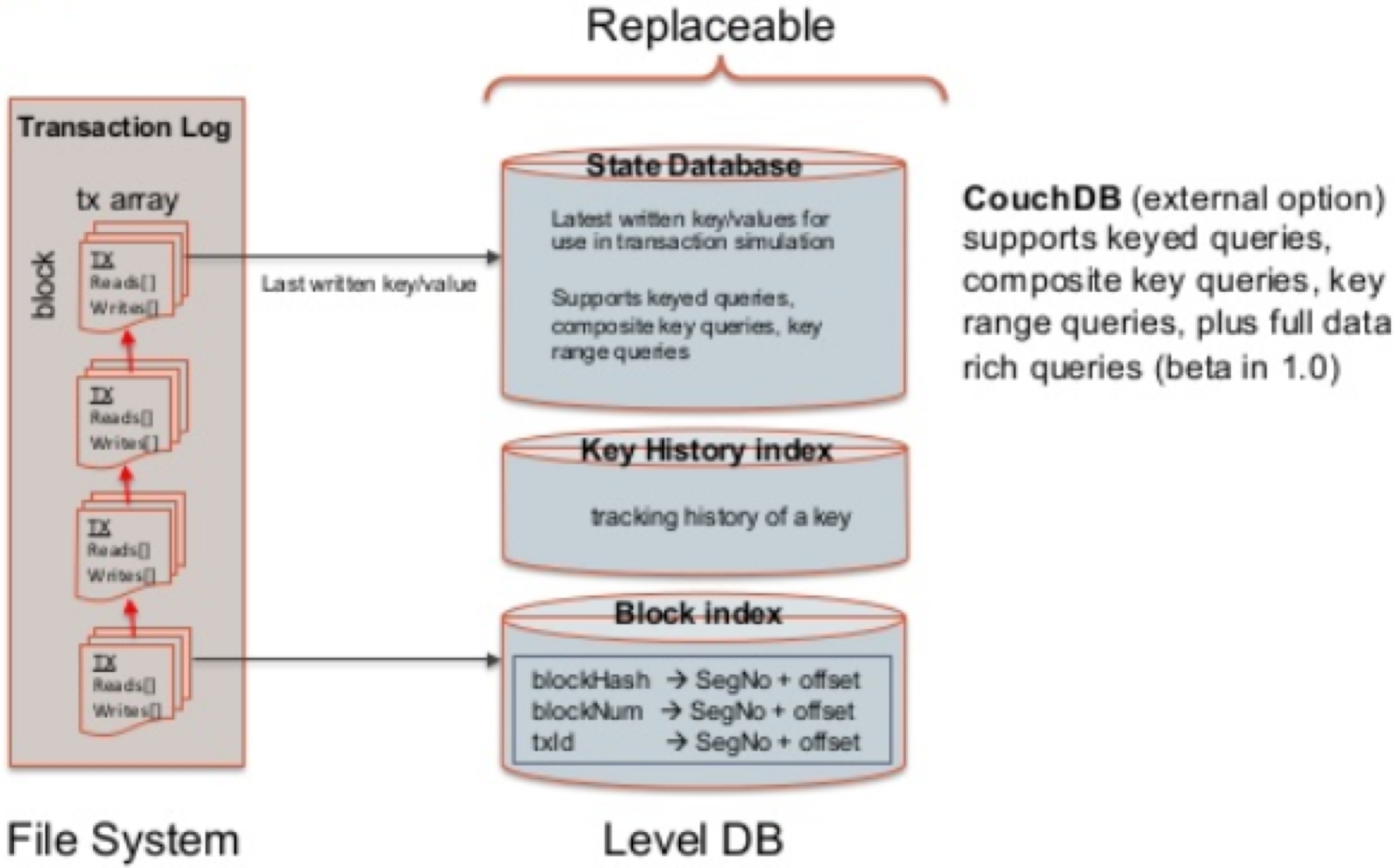
Blockchain Participants

Blockchain User		the business user, operating in a business network. This role interacts with the Blockchain using a LOB application. They are not aware of the Blockchain.
Blockchain Regulator		the overall authority in a business network. Specifically, regulators may require broad access to the ledger's contents.
Blockchain Developer		the developer of applications and smart contracts that interact with the Blockchain and are used by Blockchain users.
Blockchain Network Operator		defines, creates, manages and monitors the Blockchain network. Each business in the network has a Blockchain Network operator.
Certificate Authority		manages the different types of certificates required to run a permissioned Blockchain.
Traditional Processing Platform		an existing computer system which may be used by the Blockchain to augment processing. This system may also need to initiate requests into the Blockchain.
Traditional Data Sources		an existing data system which may provide data to influence the behaviour of smart contracts.

Blockchain Components

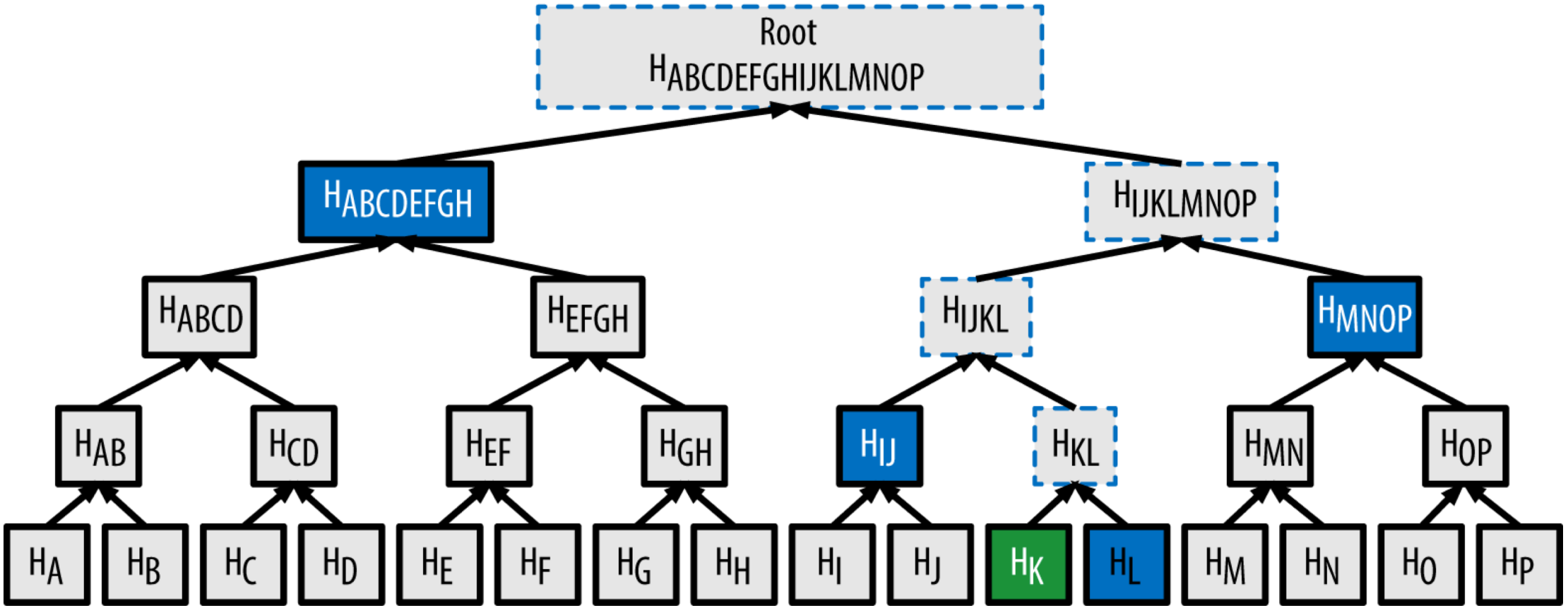
Ledger		contains the current world state of the ledger and a Blockchain of transaction invocations
Smart Contract		encapsulates business network transactions in code. transaction invocations result in gets and sets of ledger state
Consensus Network		a collection of network data and processing peers forming a Blockchain network. Responsible for maintaining a consistently replicated ledger
Membership		manages identity and transaction certificates, as well as other aspects of permissioned access
Events		creates notifications of significant operations on the Blockchain (e.g. a new block), as well as notifications related to smart contracts. Does not include event distribution.
Systems Management		provides the ability to create, change and monitor Blockchain components
Wallet		securely manages a user's security credentials
Systems Integration		responsible for integrating Blockchain bi-directionally with external systems. Not part of Blockchain, but used with it.

Ledger

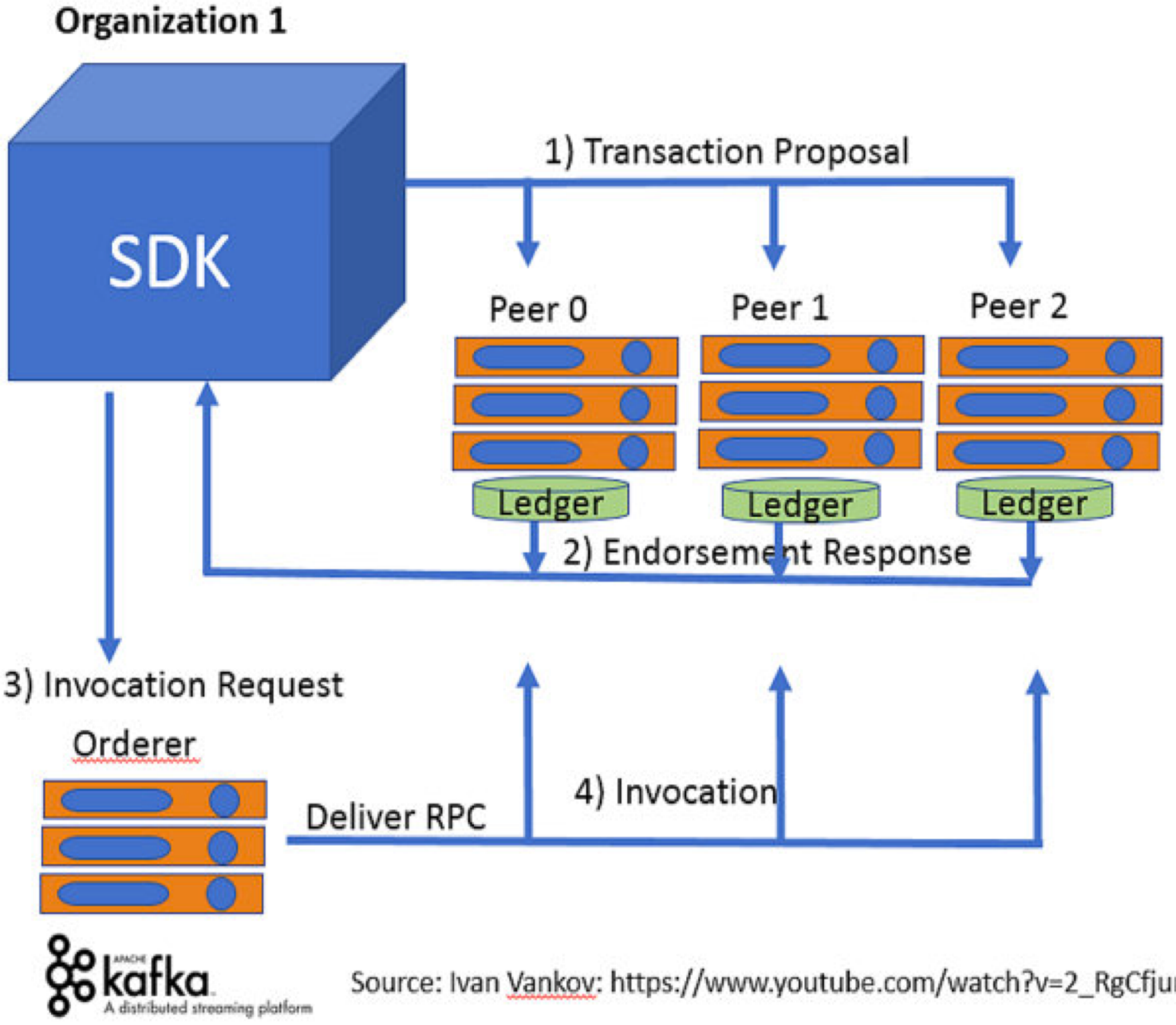


CouchDB (external option) supports keyed queries, composite key queries, key range queries, plus full data rich queries (beta in 1.0)

Merkle Tree and Merkle Root?




Number
PreviousHash
DataHash
Block Header
Tx-1 Type
Version
Timestamp
Channel Id
TxId
Epoch
PayloadVisibility
Chaincode Path (deploy tx)
Chaincode Name (invoke tx)
Chaincode Version
Creator Identity (certificate, public key) - Client
Signature
Chaincode Type
Input (chaincode function and arguments)
Timeout
Endorser-1 Identity (certificate, public key)
Endorser-1 Signature
Endorser-2 Identity (certificate, public key)
Endorser-2 Signature
...
Endorser-N Identity (certificate, public key)
Endorser-N Signature
Proposal Hash
Chaincode Events
Response Status
Namespace
Read Set: List of <Key, Version> read by the transaction
Write Set: List of <Key, Value, IsDelete>
Start Key
End Key
List of <Key, Version> read
Merkel Tree Query Summary
...
Tx-m Type
Version
Timestamp
Channel Id
TxId
Epoch
PayloadVisibility
Chaincode Path (deploy tx)
Chaincode Name (invoke tx)
Chaincode Version
Creator Identity (certificate, public key) - Client
Signature
Chaincode Type
Input (chaincode function and arguments)
Timeout
Endorser-1 Identity (certificate, public key)
Endorser-1 Signature
Endorser-2 Identity (certificate, public key)
Endorser-2 Signature
...
Endorser-N Identity (certificate, public key)
Endorser-N Signature
Proposal Hash
Chaincode Events
Response Status
Namespace
Read Set: List of <Key, Version> read by the transaction
Write Set: List of <Key, Value, IsDelete>
Start Key
End Key
List of <Key, Version> read
Merkel Tree Query Summary
Block Data (contains 'm' number of transactions)
Creator Identity (certificate, public key) - Orderer
Signature
Last configuration block#
Creator Identity (certificate, public key)
Signature
Flag for each transaction
Last offset persisted: Kafka
Creator Identity (certificate, public key)
Signature
Block Metadata

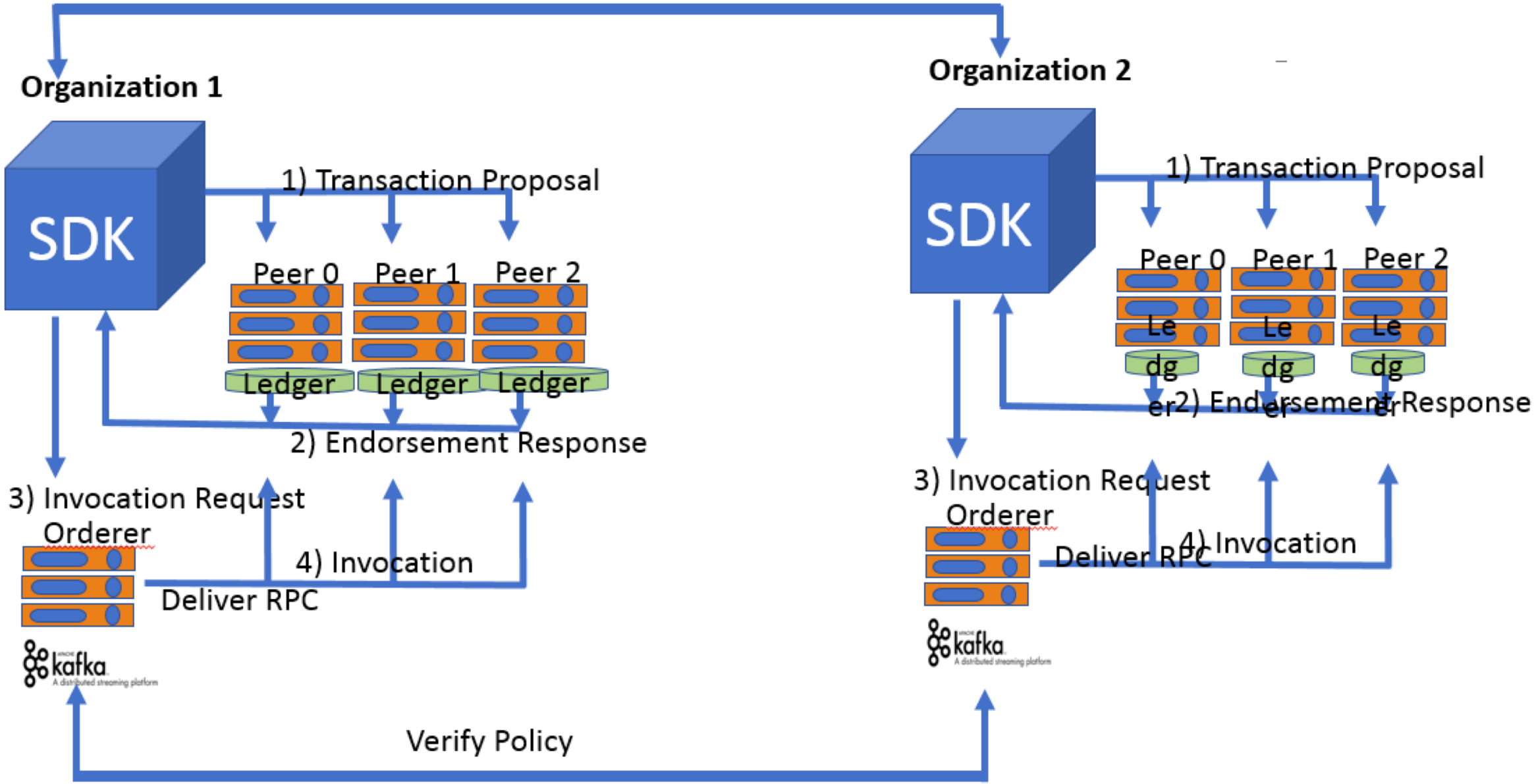


The Ledger provides a verifiable history of all valid and invalid transactions occurring during operation of the system.

The Ledger is constructed by the ordering Service and is kept at all Peers and, optionally, at a subset of orderers. http://bit.ly/2f06q07

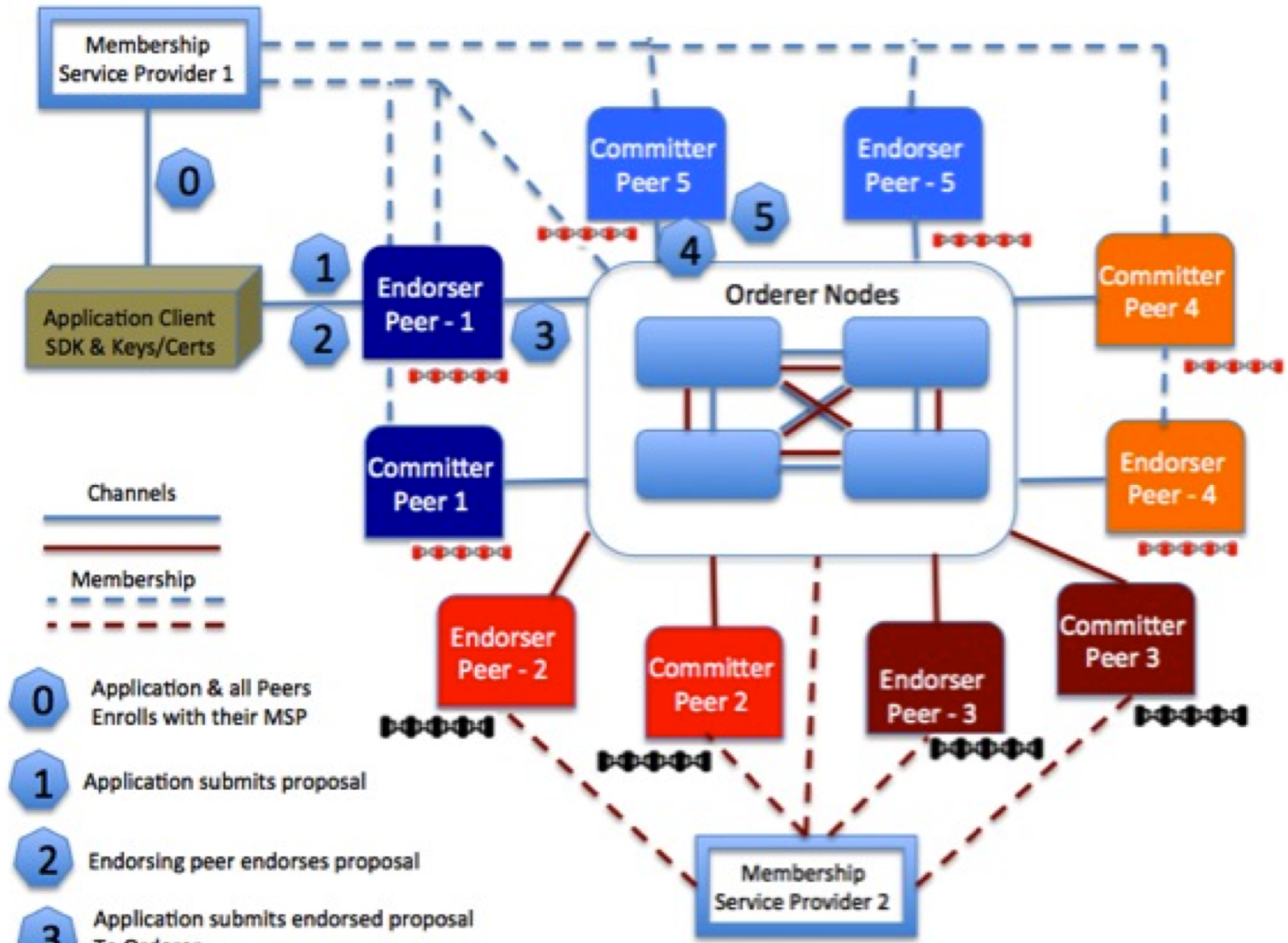
http://bit.ly/2f013xX

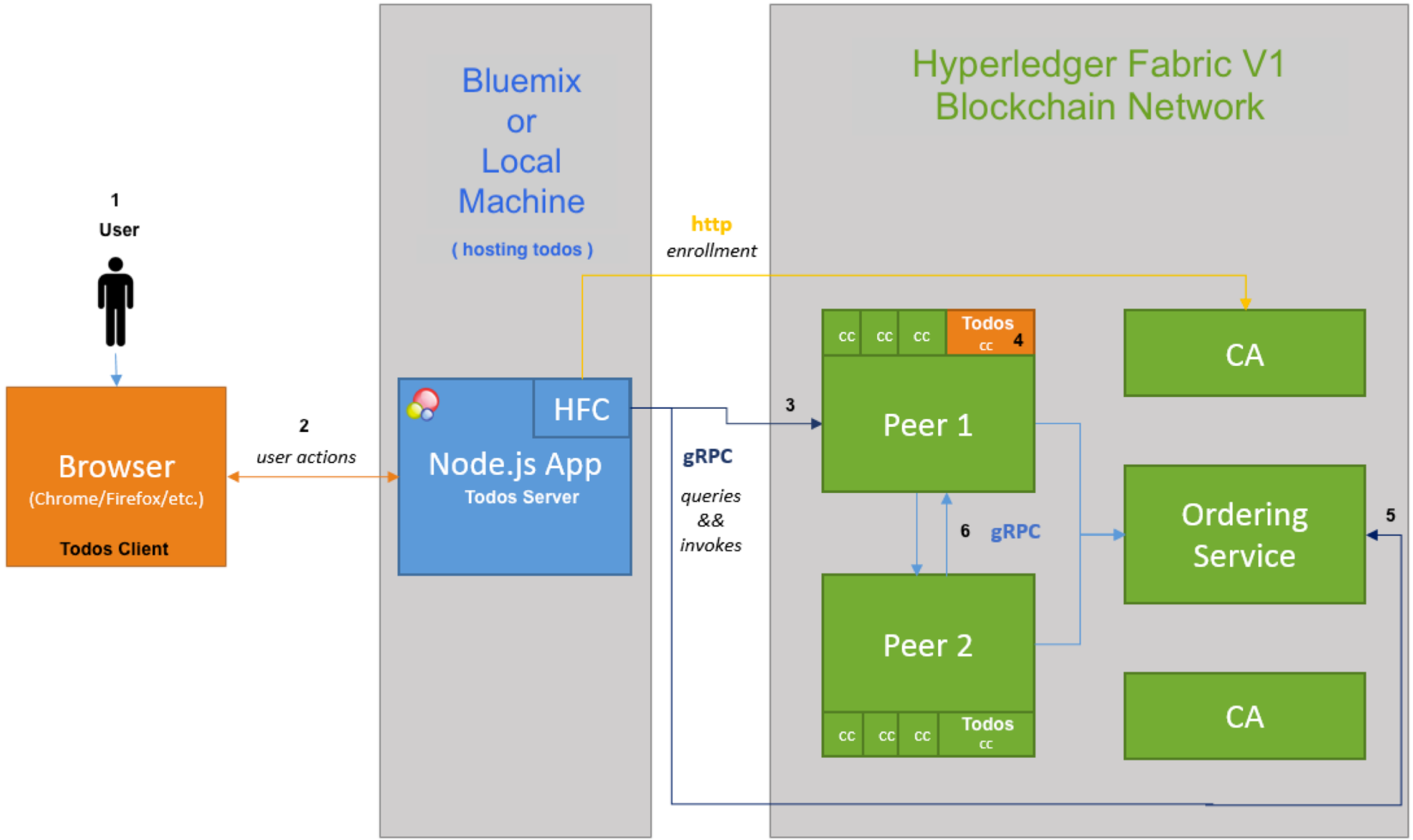
Source: Ivan Vankov: https://www.youtube.com/watch?v=2_RgCfjunEU&t=398s



Source: Ivan Vankov: https://www.youtube.com/watch?v=2_RgCfjunEU&t=398s

HyperLedger Fabric 1.0 : Private Permissioned Blockchain




Bluemix
or
Local
Machine
(hosting todos)
Hyperledger Fabric V1
Blockchain Network
1
User
Browser
(Chrome/Firefox/etc.)
Todos Client
2
user actions
HFC
Node.js App
Todos Server
http
enrollment
gRPC
queries
&&
invokes
3
cc
cc
cc
Todos
cc
4
Peer 1
6
gRPC
Peer 2
cc
cc
cc
Todos
cc
CA
Ordering
Service
5
CA