Blockchain matters

Why does blockchain matter?

Balázs Héder, Ph.D.

December 2021

PART 8

Have you ever heard these phrases?

Blockchain matters

Blockchain is going to change the World!

Bitcoin bubble has been popped!

Bitcoin is a bubble!

Bitcoin is the money of criminals!

Bitcoin bubble is going to be popped!

Bitcoin is dead! Bitcoin Obituaries, url

Blockchain is immutable!

Bitcoin is the blockchain!

Blockchain is not Bitcoin!

Blockchain contains the truth!

Smart contracts are running on the blockchain.

Cryptocurrencies are useless, but blockchain is good!

Blockchain is secure!

Have you ever heard these phrases?

Blockchain matters

Blockchain is going to change the World!

Bitcoin bubble has been popped!

Bitcoin is a bubble!

Bitcoin is the money of criminals!

Bitcoin bubble is going to be popped!

Bitcoin is the blockchain!

Blockchain is immutable!

Blockchain contains the truth!

Smart contracts are running on the blockchain.

Cryptocurrencies are useless, but blockchain is good!

Blockchain is secure!

Confusing, isn't it? To get better understanding and to be able to decide which statement is true, follow this presentation series!

Outline of the whole series

Blockchain matters

- Little steps to the beginning
- The born of the technology
- Bitcoin, why is it so important?
- OK, so what is blockchain? And what is DLT?
- Consensus mechanisms
- Oracles
- Ethereum, the world computer
- Smart contracts
- Tokens and the digitization of physical objects, NFTs, SFTs
- The tsunami of cryptocurrencies
- ICO, IEO, STO, CeFi/DeFi, DID and other buzzwords
- The enterprise answer: consortium/private blockchain solutions
- When can/should I use blockchain? - The blockchain solution feasibility chart
- Possible use cases

Notation of references

Blockchain matters

References related to a slide are listed at the bottom of the slide, or right next to the text.

Visual Capitalist, G. Bhutada, “Purchasing Power of the U.S. Dollar Over Time”, 2021, url.

EOS, url

Solana, url

CertiK, “The Blockchain Trilemma: Decentralized, Scalable, and Secure?”, 2019, url

Blockchain matters

Part 8 – Enterprise blockchain

Types of enterprise blockchain

Blockchain matters

- Private blockchain: only one distinguished participant, or all nodes are at the same company (not always make sense)
- Consortium blockchain: more distinguished participants, several consortium members

What is private blockchain?

Blockchain matters

- All notes operate at the same company, or only one distinguished node (centralized blockchain)
- Not available for public.
- Practically it doesn’t really make sense, a simple database is a cheaper solution.

What is enterprise blockchain?

Blockchain matters

- Several consortium members.
- Not available for public.
- Semi trusted: consortium members know each other.
- Usually permissioned blockchains.
- Customizable access rights.
- Public or private transactions.
- No cryptocurrency, no cryptoeconomics (tokenomics).

Several enterprise solutions

Blockchain matters

- Platforms
  - Enterprise Ethereum Alliance
  - Quorum
  - Ripple
  - R3 Corda
  - Interlegder
  - Parity Substrate
  - Hyperledger Indy/Ursa/Fabric/Besu
- Blockchain-as-a-Service
  - Azure
  - AWS

Comparing platforms

Blockchain matters



D. Szegő, Nordic Blockchain Association, Solidity Services, “Consortium Blockchains á la Hyperledger”

Enterprise Ethereum

Blockchain matters

- Ethereum Enterprise Alliance
  - PoA (proof of authority)
  - Increased performance
  - Increased privacy
- Quorum
  - J.P. Morgan
  - Open sources
  - Up to 100 tx/s
  - Privacy





Ethereum Enterprise Alliance, url

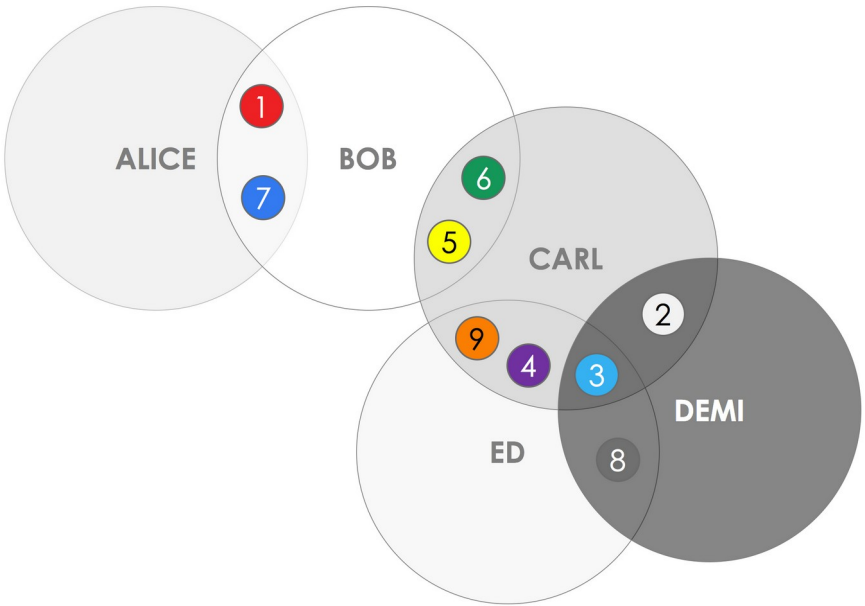
Quorum, url

R3 Corda

Blockchain matters

- Created for financial institutes.
- Shared facts.
- No global ledger. Instead each node maintains its own database of those facts that it is aware of. (Local or multi-party ledgers)
- None of the peers see the entire ledger.
- No global broadcasts, but programmed communication paths.
- Optimized for contracts between peers (atomic prose = digitized usual contracts not smart contracts, e.g. I owe you 5 USD.)
- UTXO model built on contract states.

corda



Corda Ledger, url

The Hyperledger project

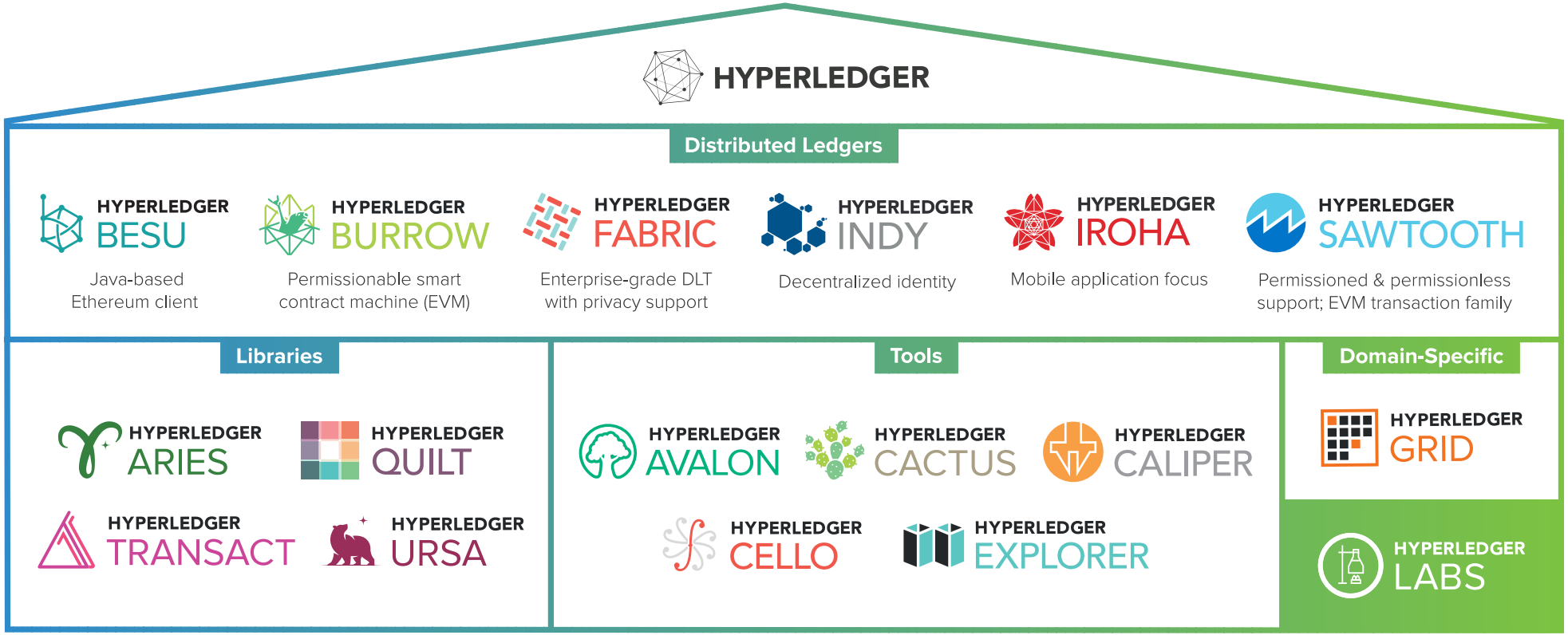
Blockchain matters

- Umbrella project of open source blockchains and related tools.
- Started by the Linux Foundation in Dec 2015.
- Several contributors
  - IBM
  - Intel
  - SAP Ariba

Hyperledger, url

The Hyperledger greenhouse

Blockchain matters



HL_Greenhouse_Current, url

Hyperledger greenhouse

Blockchain matters

A bit detailed overview

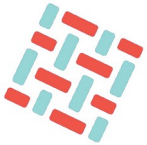
- Libraries
  - Aries: digital credential library (derived from Indy)
  - Ursa: shared cryptographic library
  - Transact: design and execute smart contracts
- Tools
  - Caliper: benchmarking tool
  - Cello: on demand as-a-service deployment
  - Explorer: blockchain explorer
- Distributed ledgers
  - Besu: EVM client designed for private and public networks and in application in enterprise environment
  - Fabric: general purpose modular blockchain
  - Indy: designed for decentralized and self-sovereign identity on distributed ledgers

N. Gaur et al., “Blockchain with Hyperledger Fabric, Second Edition, 2020, url

Hyperledger Fabric

Blockchain matters

- Open source project from the Linux Foundation initiated by IBM.
- Modular blockchain framework uses plug-and-play components.
- General smart contract platform.
- More than 120000 contributing organizations.
- Increased performance: 800 tx/s.
- Increased tx speed: 1-2s tx validation.



HYPERLEDGER FABRIC

Hyperledger Fabric, url

Hyperledger Fabric

Building blocks 1/2

- Peer (node)
  - Fundamental element of a blockchain network, they communicate with each other P2P and they host ledgers and smart contracts.
  - Each peer has its own identity given by a MSP.
- Members (organizations): are collaborating with each other, operating peers.
- Channel
  - A mechanism by which members can collaborate (do txs among themselves)
  - Defined by members (organizations), anchor peers per member, the shared ledger, chaincodes and the ordering service node(s).
- Ledger
  - Transaction log (blockchain)
  - World state
  - Separate ledger belongs to each channels
  - Any peer can manage multiple ledgers (channels)

A Blockchain Platform for the Enterprise, url

Hyperledger Fabric

Building blocks 2/2

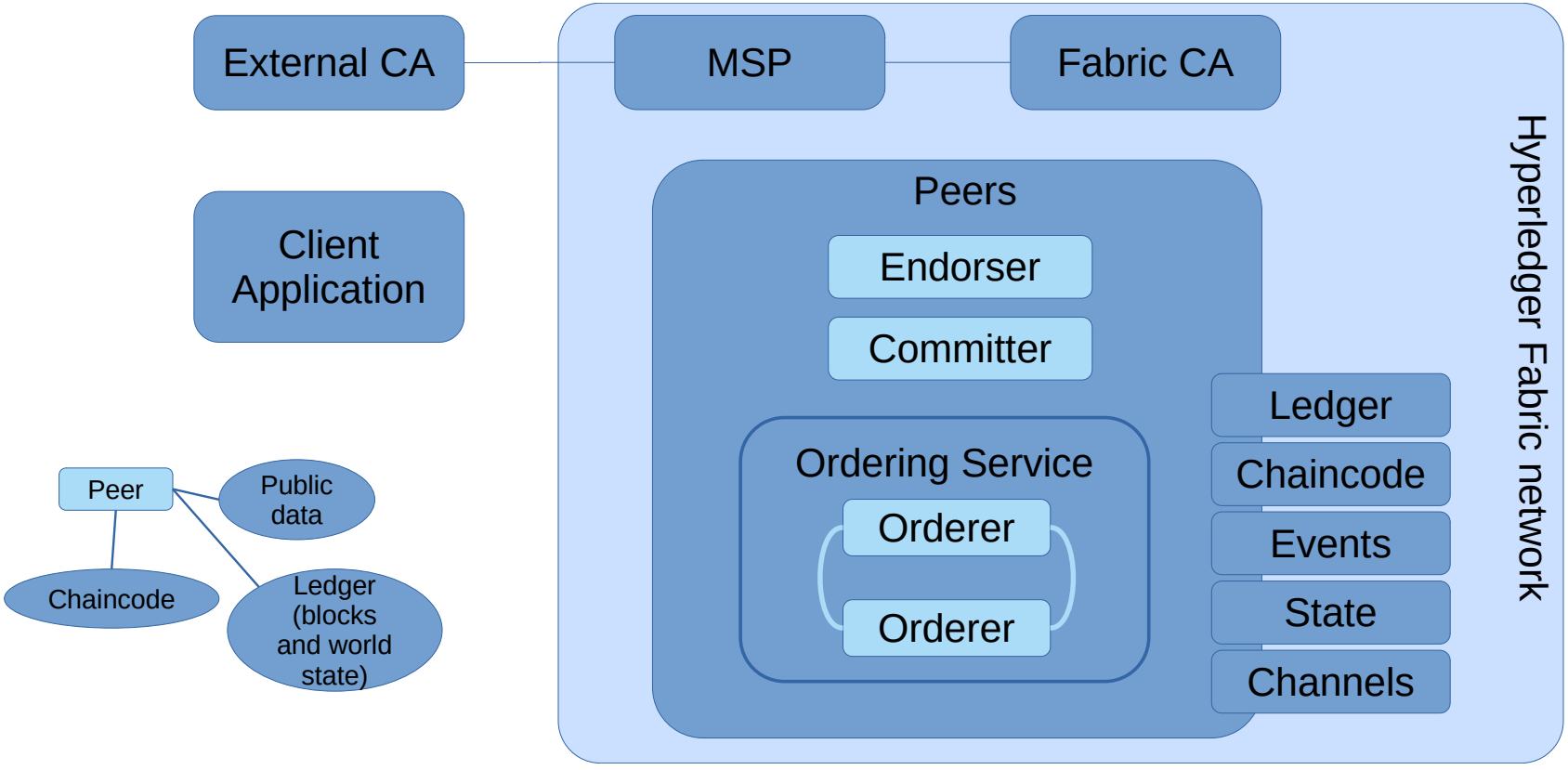
- Chaincodes
  - are smart contracts in Hyperledger Fabric
  - are installed directly on the peers and belong to a channel
  - are used to write the channel's ledger
- RW (read-write) set
  - read set: a list of unique keys and their committed version numbers (but not values) that the transaction reads during simulation.
  - write set (state updates): a list of unique keys and their new values that the transaction writes.
- PDC (private data collection)
  - Peers can define PDC. Only the hash of PDC not the data itself is stored in the shared ledger.

A Blockchain Platform for the Enterprise, url

Hyperledger Fabric

Blockchain matters

Architecture



MSP: Membership Service Provider
CA: Certificate Authority

Hyperledger Fabric, url

Hyperledger Fabric

Blockchain matters

Membership services

- Membership Service Provider
  - Per channel
  - User identity verification
  - User registration
  - Permission handling
  - Implements Fabric CA
- Certificate Authority issues X.509 certificates which are necessary for peers to join Hyperledger network
  - Internal (Fabric CA)
  - External
- Certificates
  - Enrolment Certificates (E-Certs, EC) – identity of the client
  - Temporary Certificates (T-Certs) – used for one-time transactions

N. Gaur et al., “Blockchain with Hyperledger Fabric”, 2nd Edition, url

I. Bashir, “Mastering Blockchain”, 3rd Edition, url

X.509, url

Hyperledger Fabric

Consensus

- Splitted consensus algorithm (endorsing, ordering, committing)
- Players
  - Committer peer
  - Endorser peer. Special type of committer peer, endorser peer is also a committer peer. Pluggable endorsement policy.
  - Ordering peers (orderers) run the Ordering Service. Ordering Service is pluggable, different types:
    - SOLO – for testing
    - Kafka – CFT (crash fault tolerant) only, this is acceptable in a permissioned network.
    - Raft – CFT only, this is acceptable in a permissioned network.
    - PBFT (Practical Byzantine Fault Tolerance)
- Transaction flow
  - Transaction proposal
  - Transaction simulation
  - Ordering
  - Committing
  - Notification

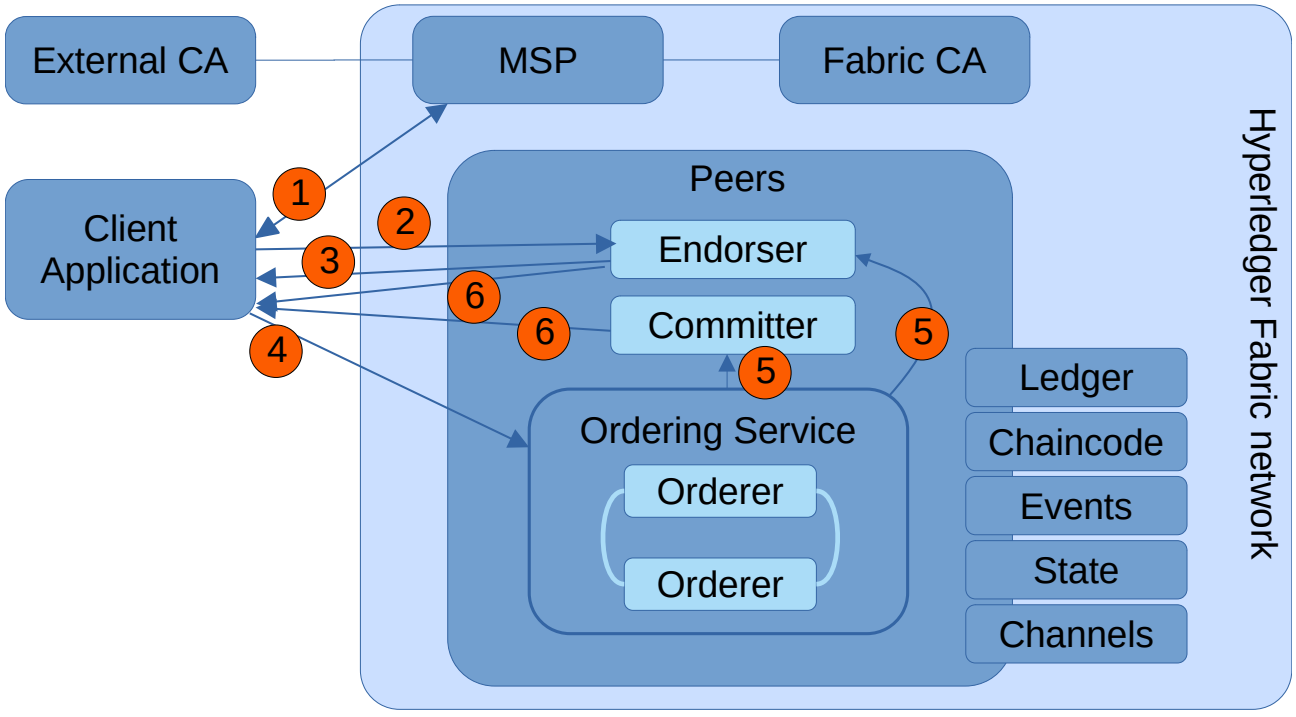
Hyperledger Fabric, url

Hyperledger Fabric

Blockchain matters

Transaction flow

1. Client registration at MSP.
2. Transaction proposal: client sends transaction proposal to endorser peers.
3. Transaction simulation: endorser peers simulate transaction, compute RW sets, endorse the transaction proposal and sends it back to the client.
4. Ordering: client submits transaction to the ordering service, which (chronologically) orders transactions and put them into a block.
5. Committing: the Ordering Service delivers the new block to the committer peers which validate each transaction in the block, applies write sets and then append the block to the blockchain.
6. Notification: committer peers notify client application about the result of the transaction.



Hyperledger Fabric, url

Endorsement

- Endorsing transaction.
  - The endorser peer verifies
    - the tx proposal format
    - the client signature
    - if tx is submitted for the first time
    - if the client is authorized correctly
  - The endorser peer simulates the transaction (executes the tx by calling the chaincode) and generate RW sets.
  - The endorser peer write endorsement result (ENDORSED, REJECTED) into transaction proposal, signs the transaction proposal, and sends it back to the submitting client.
- Endorsement policy
  - Set of rules or conditions based on which the transaction endorsement criteria is determined. The submitting client considers transaction proposal endorsed if the endorsement criteria is satisfied.
  - Chaincode-level endorsement policies by default, the chaincode-level endorsement policy belongs to a chaincode.
    - Specified at the time of chaincode deployment.
    - Example: (Org1.peer & Org2.peer), which means any peer from Org1 and any peer from Org2 must endorse the transaction.
  - Key-level endorsement policies can override chaincode-level policies.

Hyperledger Fabric, url

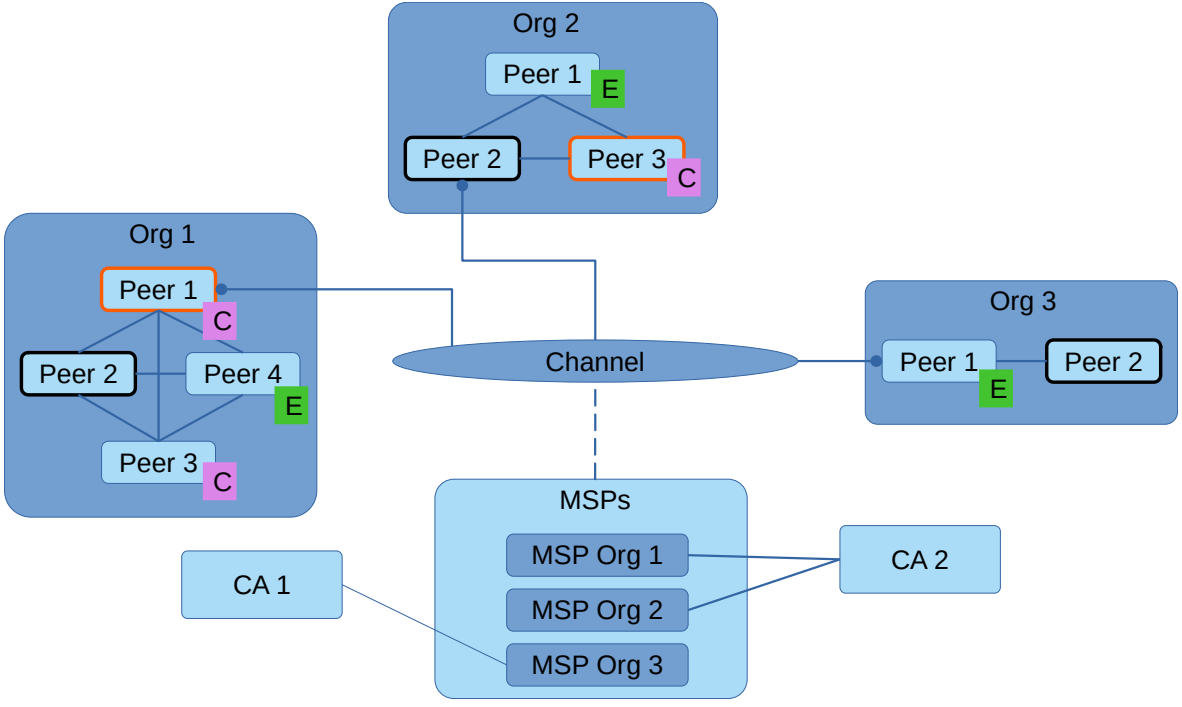
Validation

- Committer peers do transaction validation.
- Check if tx endorsement is valid.
- Check if there is no violation in read set, e.g. the keys' value in the read set = keys' version in the state.
- If transaction is valid, committer peer marks it with '1' and applies write set to the ledger.
- If transaction fails, committer peer marks it with '0'.
- Block is then appended to the ledger.

Hyperledger Fabric

Blockchain matters

Fabric network example



Hyperledger Fabric, url

Peer 3 C : Committer peer

Peer 1 E : Endorser peer

Peer 2 : Orderer peer

Peer 1 : Anchor peer (organization's gate to the outside world)

Peer 3 : Leader peer (directly communicates with the Ordering Service)

BaaS solutions

Blockchain matters

- Blockchain as a Service
  - Automatic installation
  - Monitoring
  - Identity management
- BaaS solutions
  - Microsoft Azure
  - Amazon AWS
- Blockchain platforms
  - Ethereum Enterprise
  - R3 Corda
  - Hyperledger Fabric

Azure Blockchain, url

Blockchain on AWS,url

Blockchain matters

Coming up next: Use cases

Blockchain matters

Thank you!

If you liked this material you can tip me

Blockchain matters

- Bitcoin: *3FvgmYScorEje3WTrdDn5synEU6j917SZz*
- Litecoin: *ltc1qs457h3899qj4yry8k6u5xva79wa8f6xspant4e*
- Ethereum: *0xdF7eAab54BC9070a140D0251247406cEe40029B7*
- QTUM: *MGo31aQ74yHJ9Lan4tgYeFy5XhtHZuoimQ*
- Tezos: *tz1VpDWz45fvqv69Laa6YVa3h6MtkCoq1BDc*

Blockchain

matters

Thank you again!