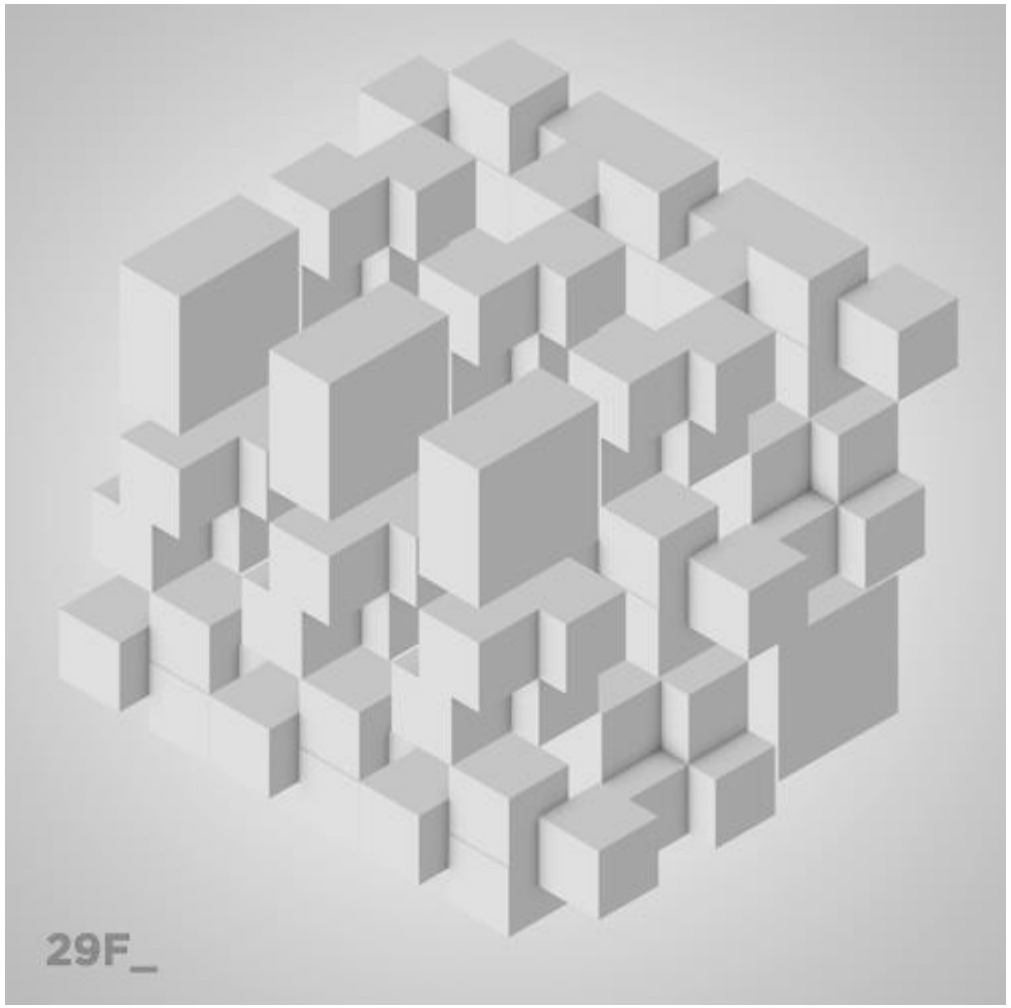
Blockchain!



What consultants should know about it.

Daniel Karzel @ SENACOR

Workshop Overview

Quick overview of what is planned for the workshop.

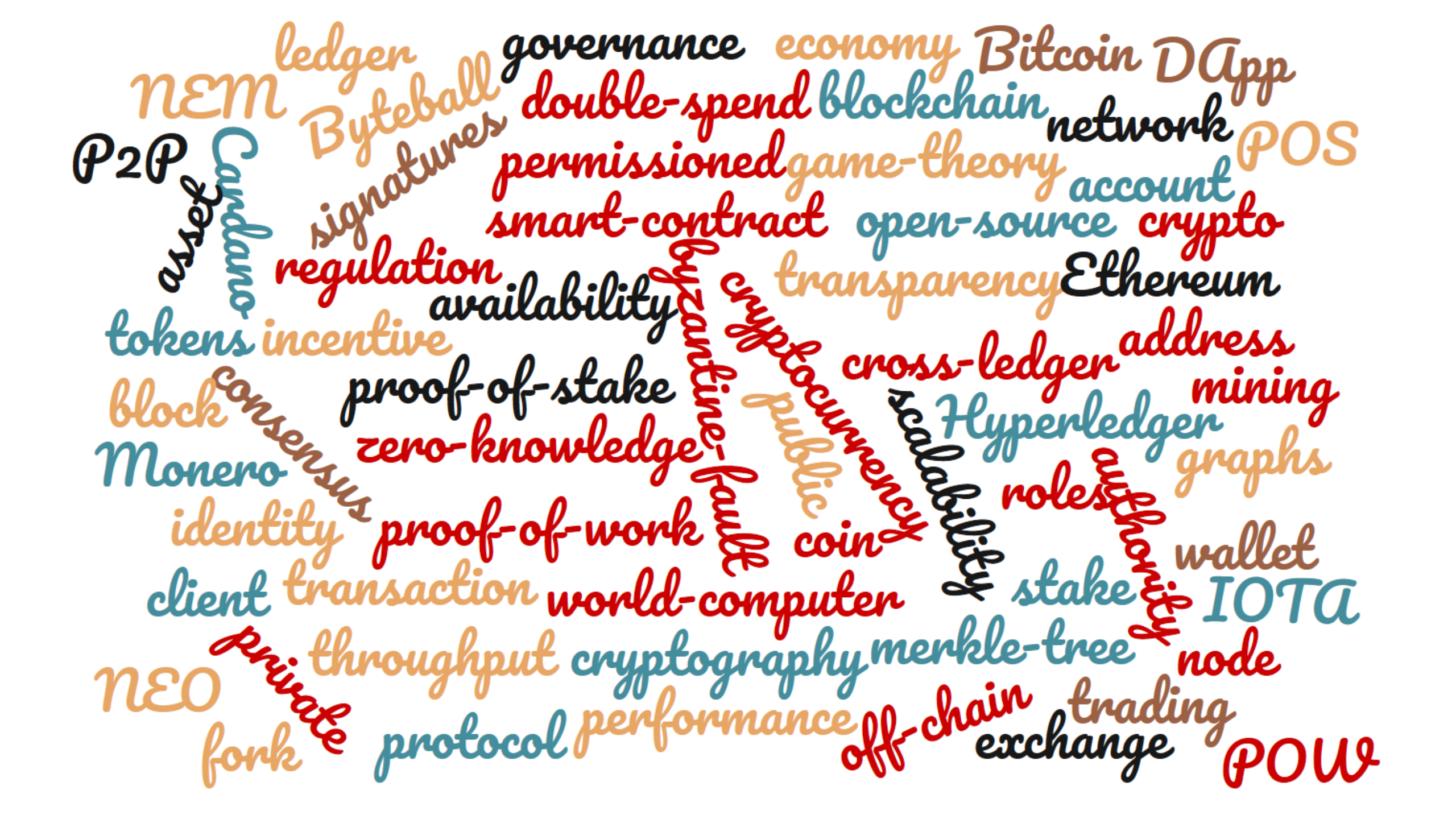
Workshop goals

- Understand what's behind the term "**Blockchain**".
- Basic understanding of current **Platforms** and their goals.
- Understand what **Use Cases** & **Characteristics** fit certain platforms.
- Very basic understanding of **Tokens** and **Cryptocurrencies**.
- (Very basic understanding of **Smart Contracts**.)

Presentation (~45 minutes)	**Open Discussion** (~30 minutes)

Blockchain…

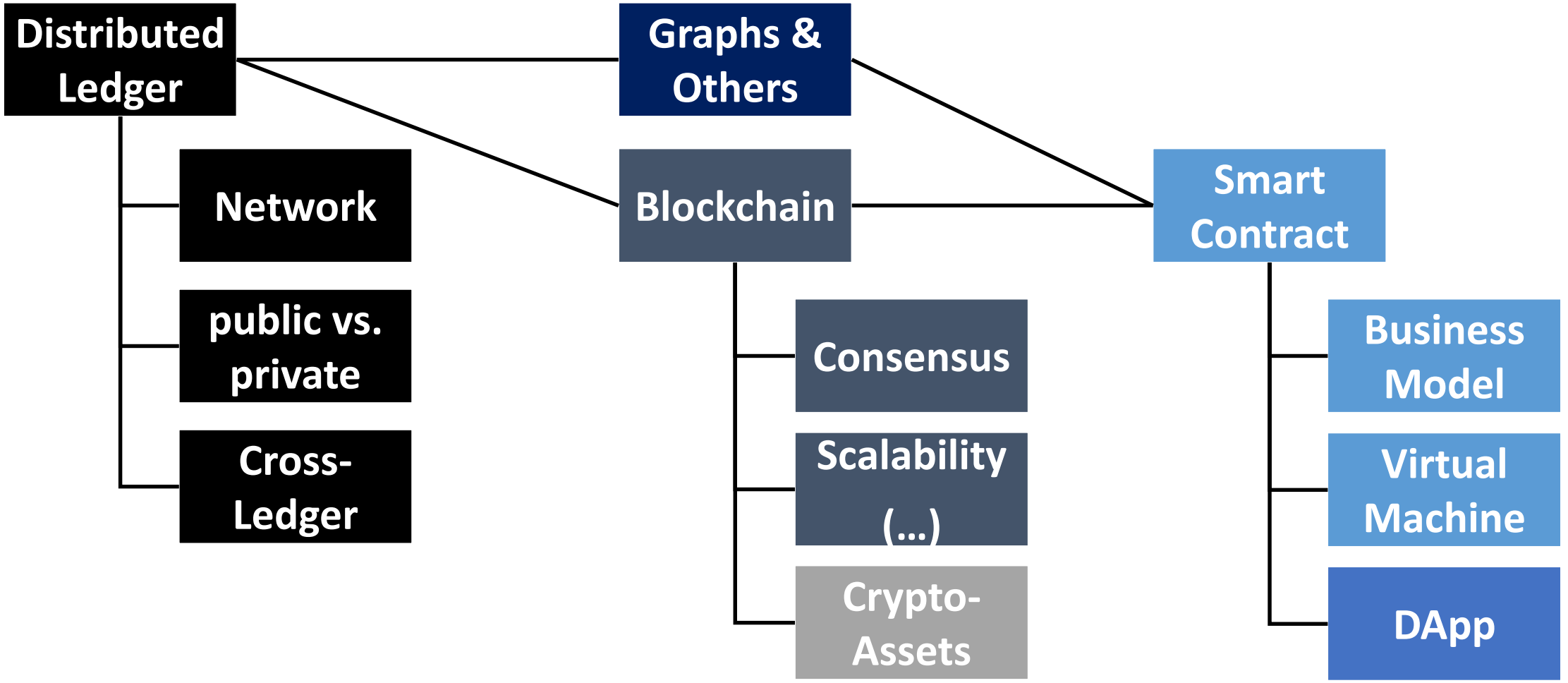
… an overloaded buzzword!


governance
economy
Bitcoin
DApp
ledger
NEM
Byteball
double-spend
blockchain
network
POS
signatures
P2P
permissioned
game-theory
account
asset
Cardano
smart-contract
open-source
crypto
regulation
transparency
Ethereum
availability
byzantine-fault
cryptocurrency
tokens
incentive
address
cross-ledger
proof-of-stake
mining
block
consensus
public
scalability
Hyperledger
zero-knowledge
graphs
Monero
roles
authority
identity
proof-of-work
coin
wallet
client
transaction
world-computer
stake
IOTA
throughput
cryptography
merkle-tree
node
private
NEO
fork
protocol
performance
off-chain
trading
exchange
POW

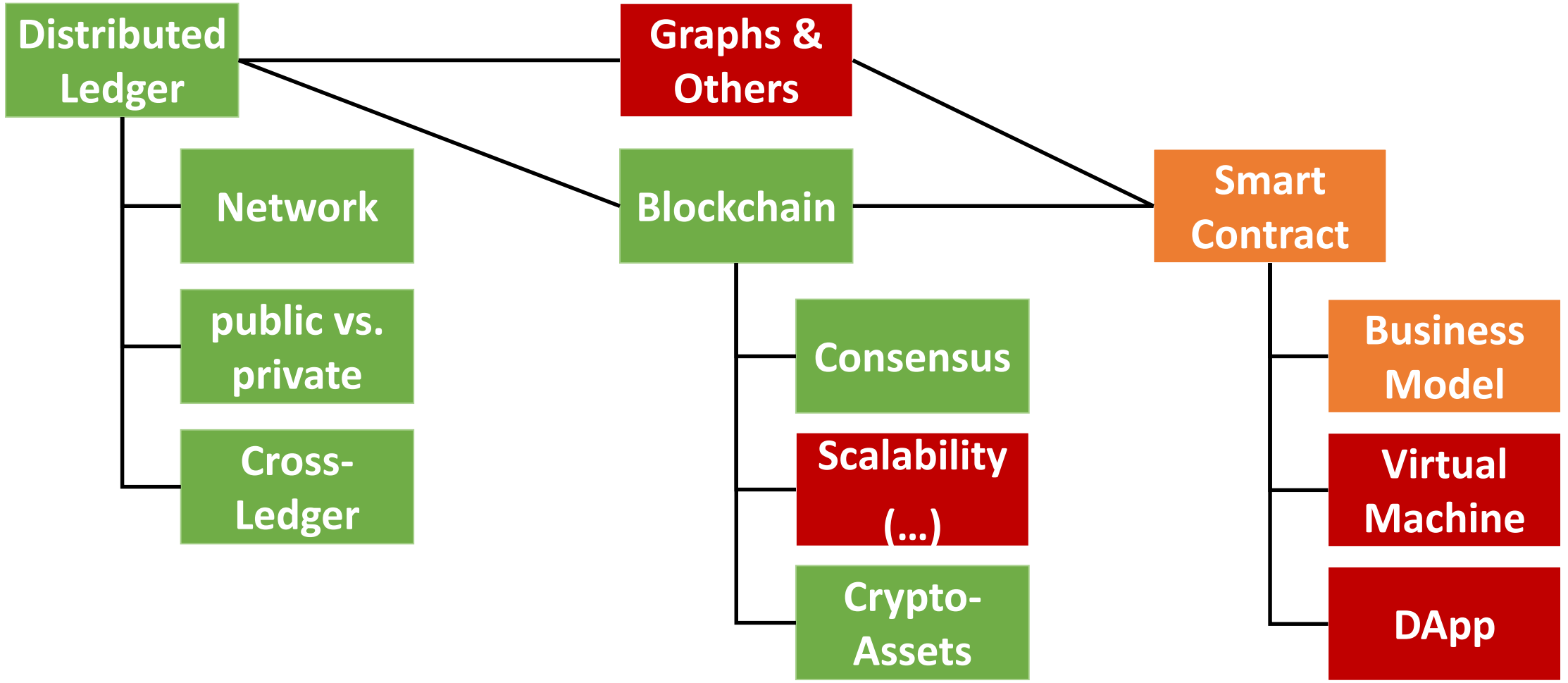
Why Blockchain?
It’s all about **trust**.

Moving trust from humans to the machine.

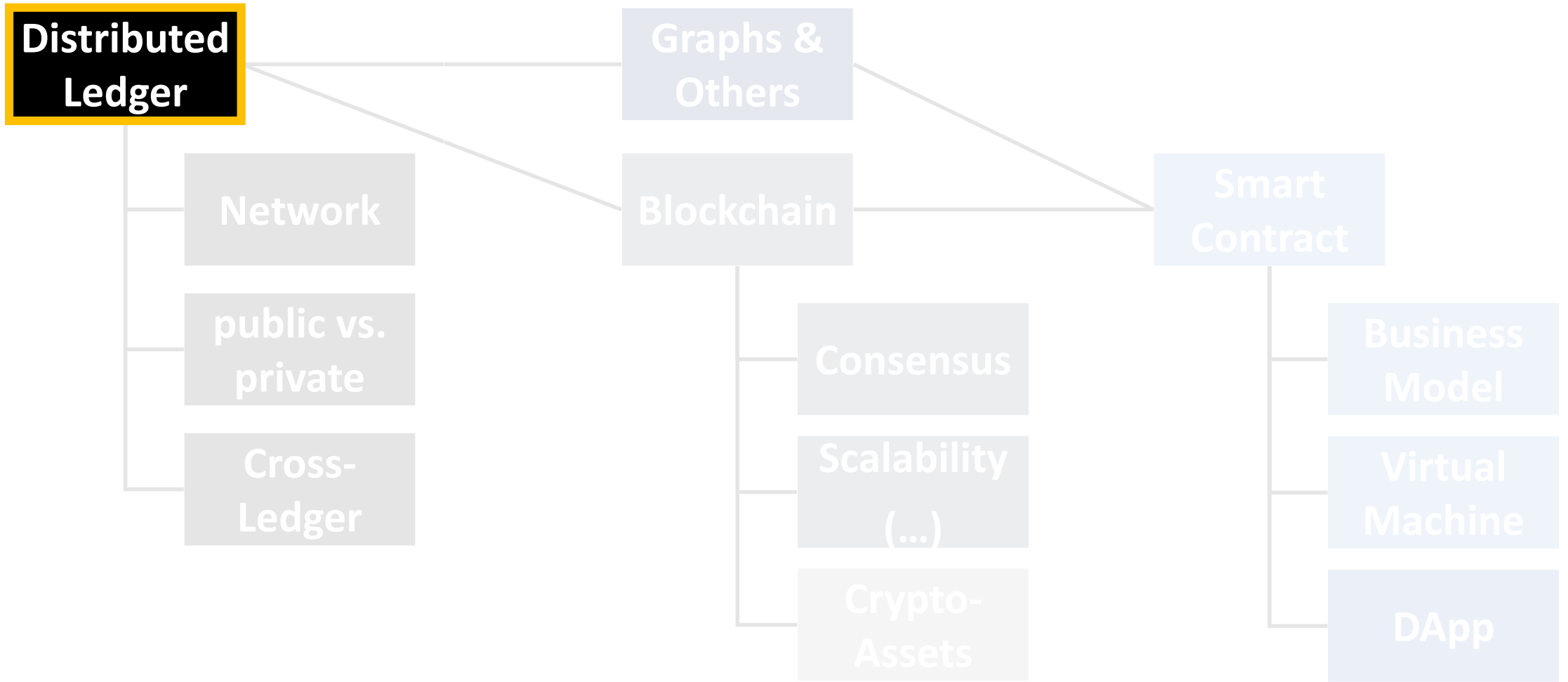
Fields of Interest



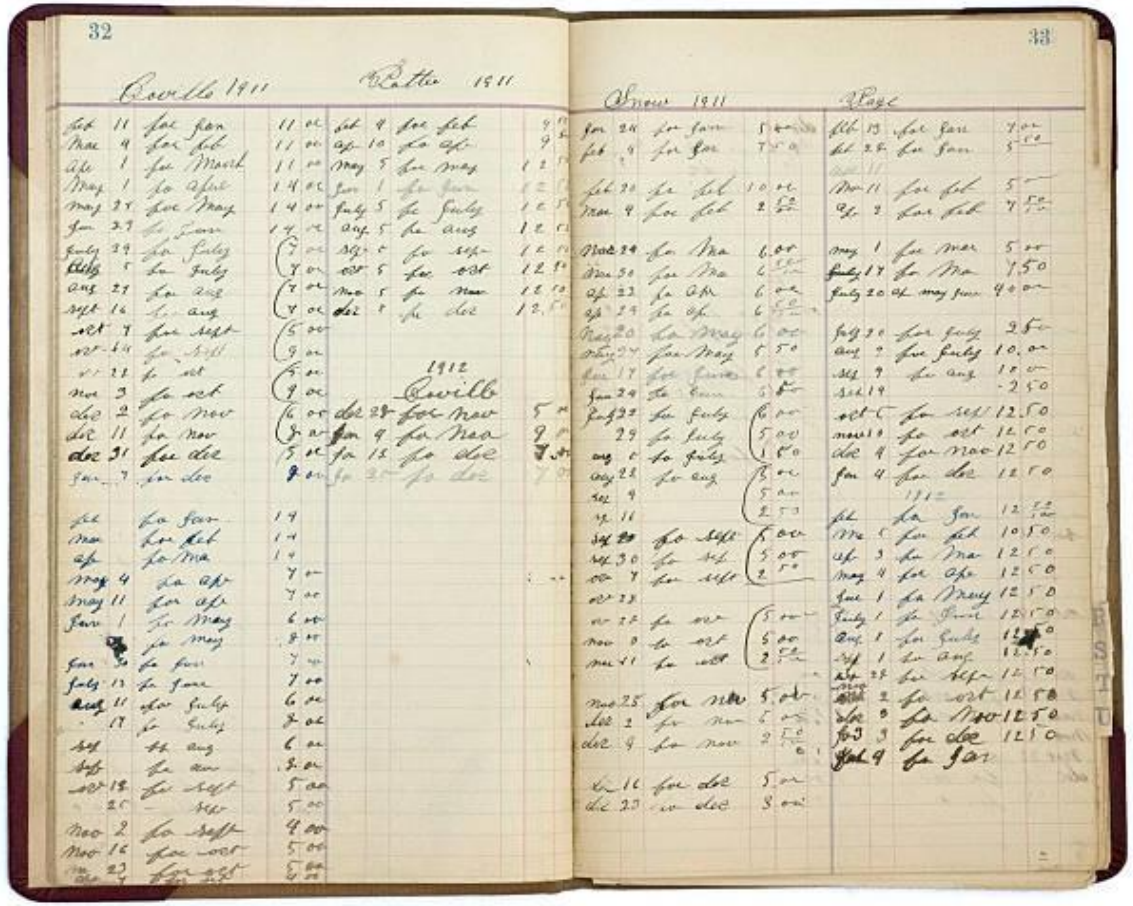
What will be covered in this workshop?



Let‘s focus on…



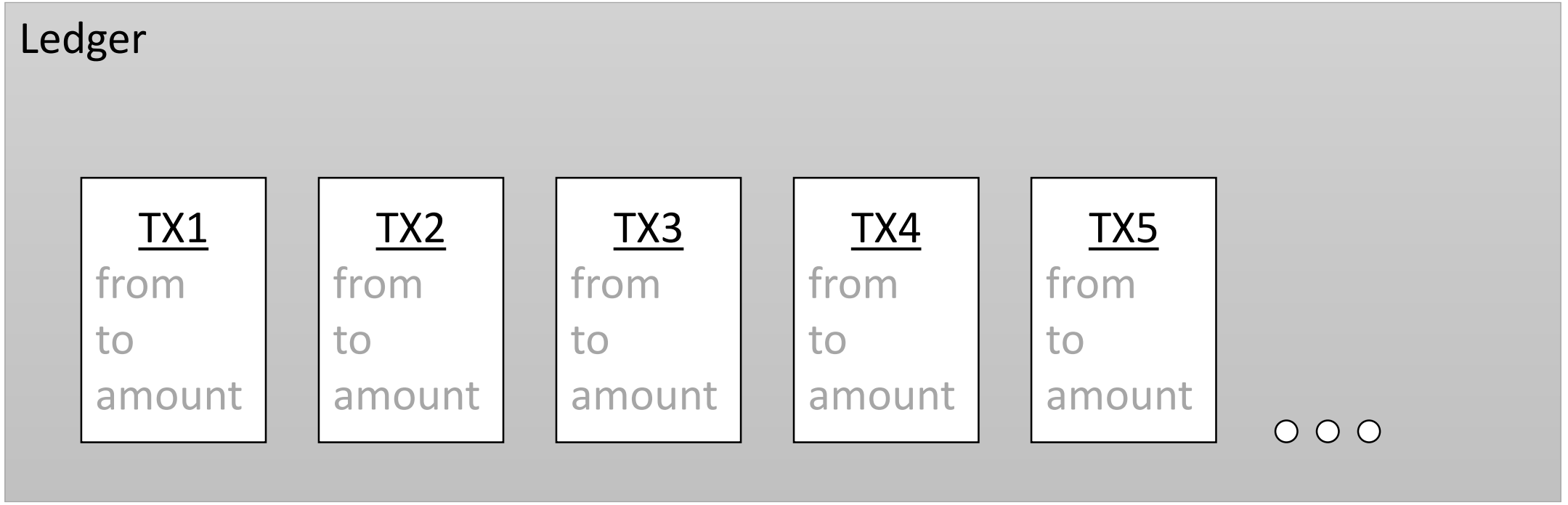
What is a ledger?



What is a ledger?

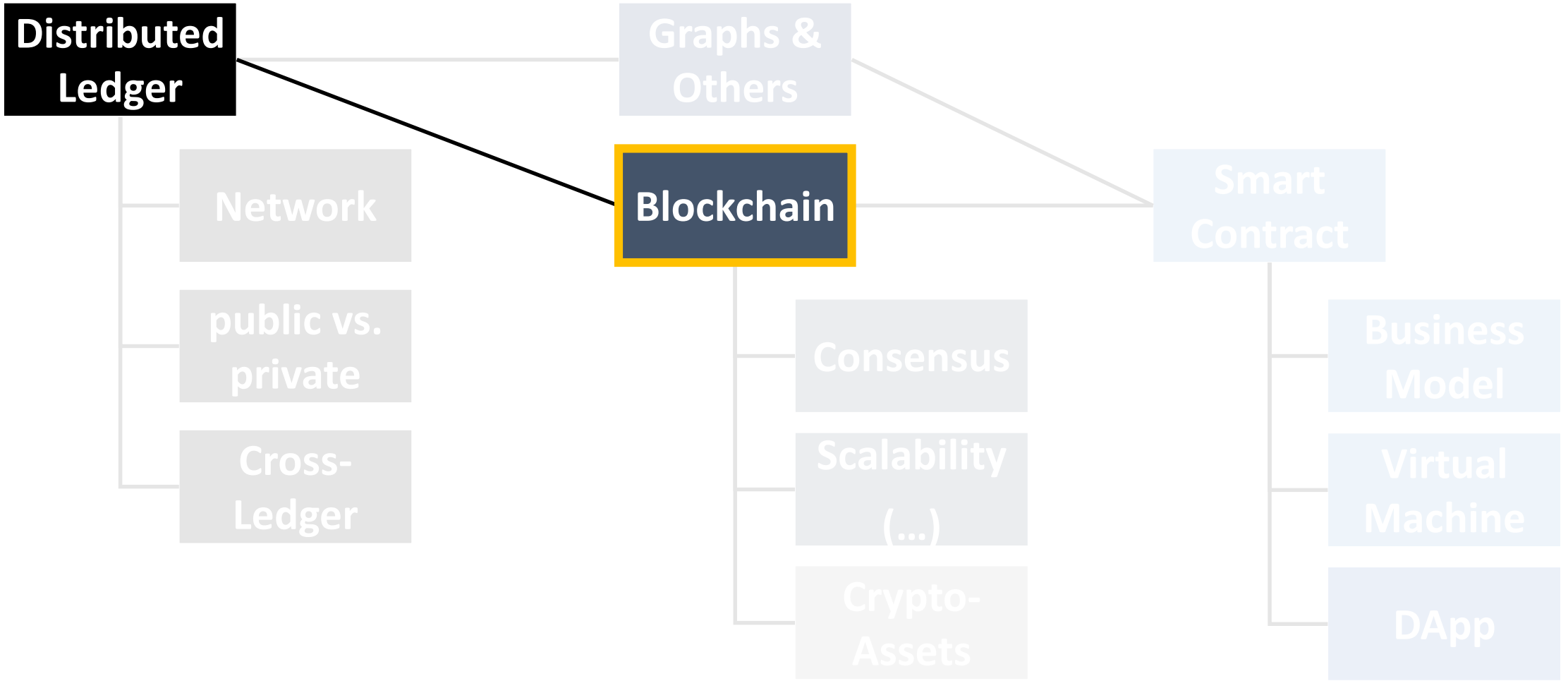
Bank Ledger					
Bank Name: Big Money Bank					
Date	**From**	**To**	**Amount**	**Balance From**	**Balance To**
19.09.2017	DE44 1…	DE44 2…	500 €		500 €
20.09.2017	DE44 2…	DE44 3…	200 €	300 €	600 €
21.09.2017	DE44 2…	DE44 4…	100 €	200 €	400 €

What is a ledger?

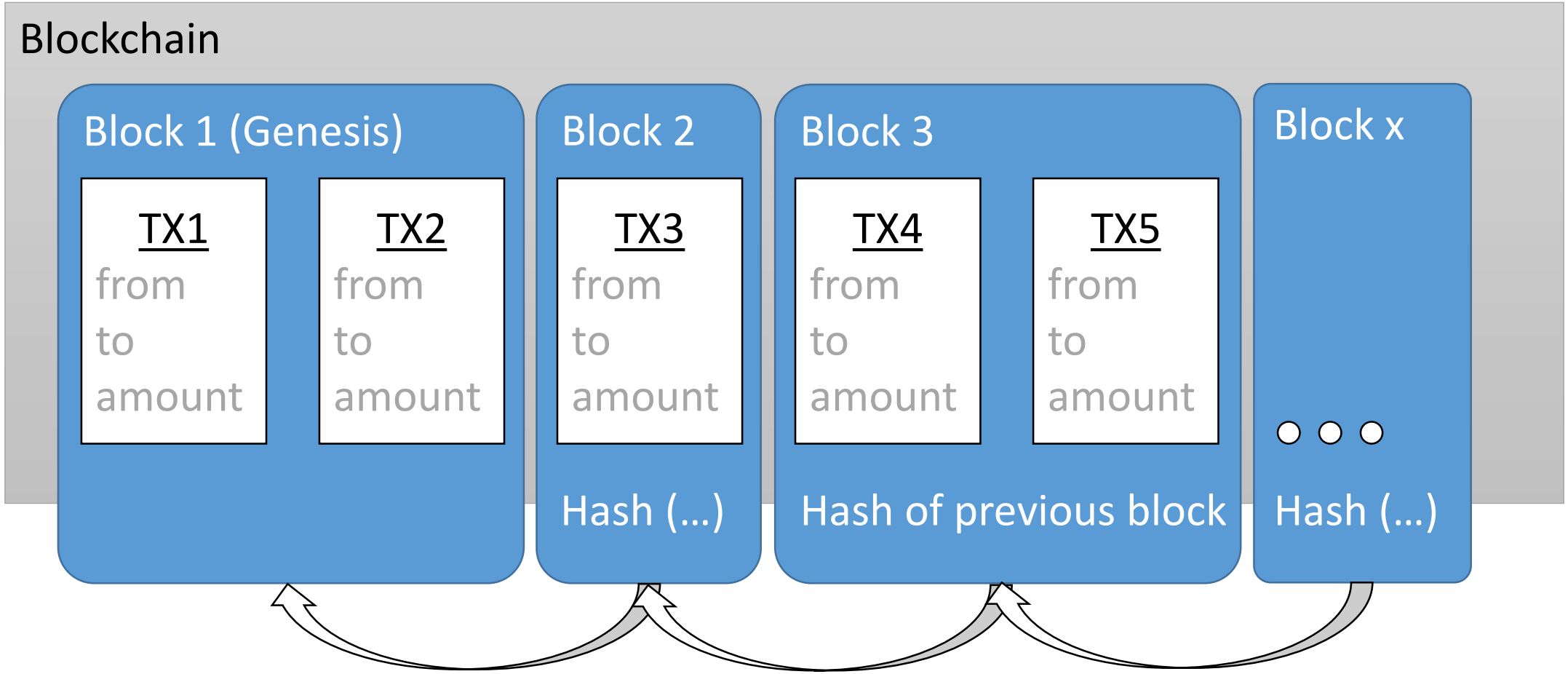


You cannot just „delete“ a transaction in a bank, you can just add transactions.

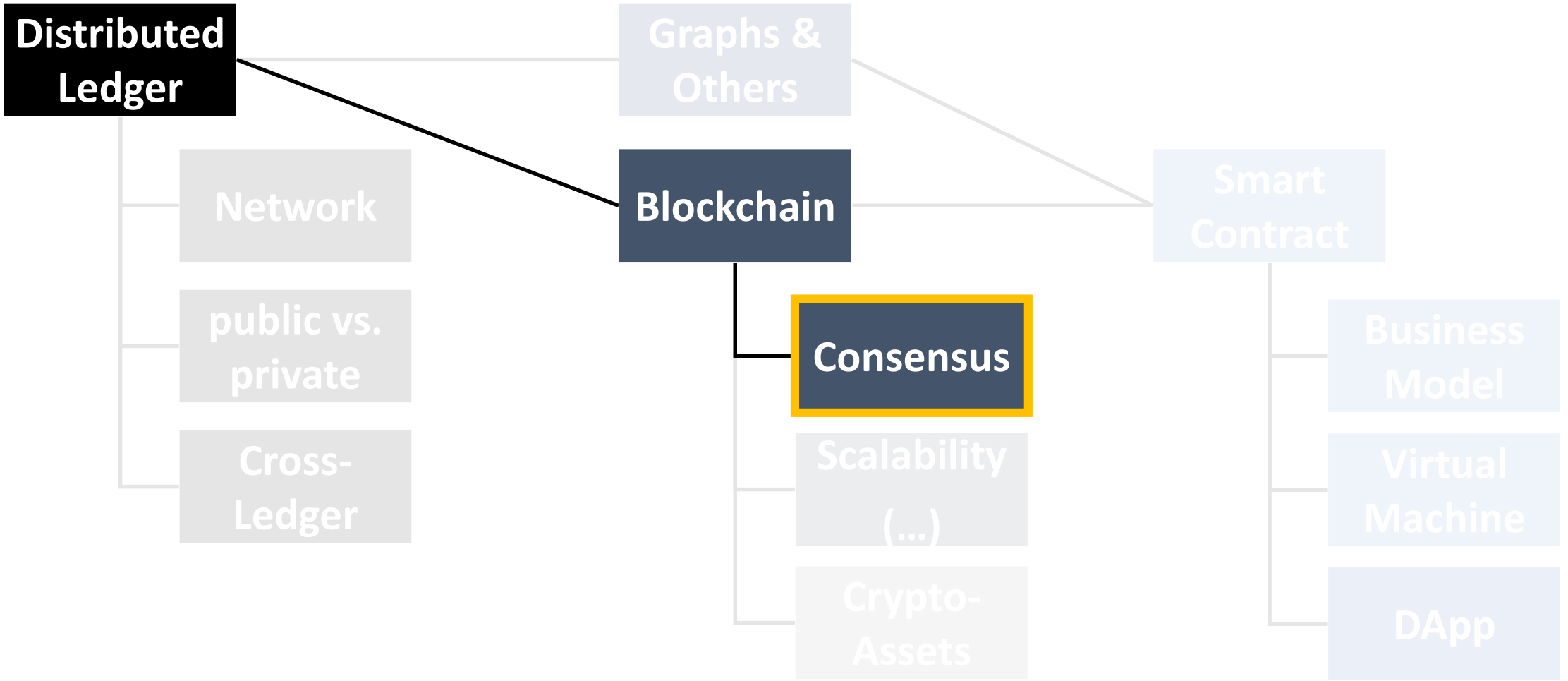
Let‘s focus on…



What is the Blockchain?



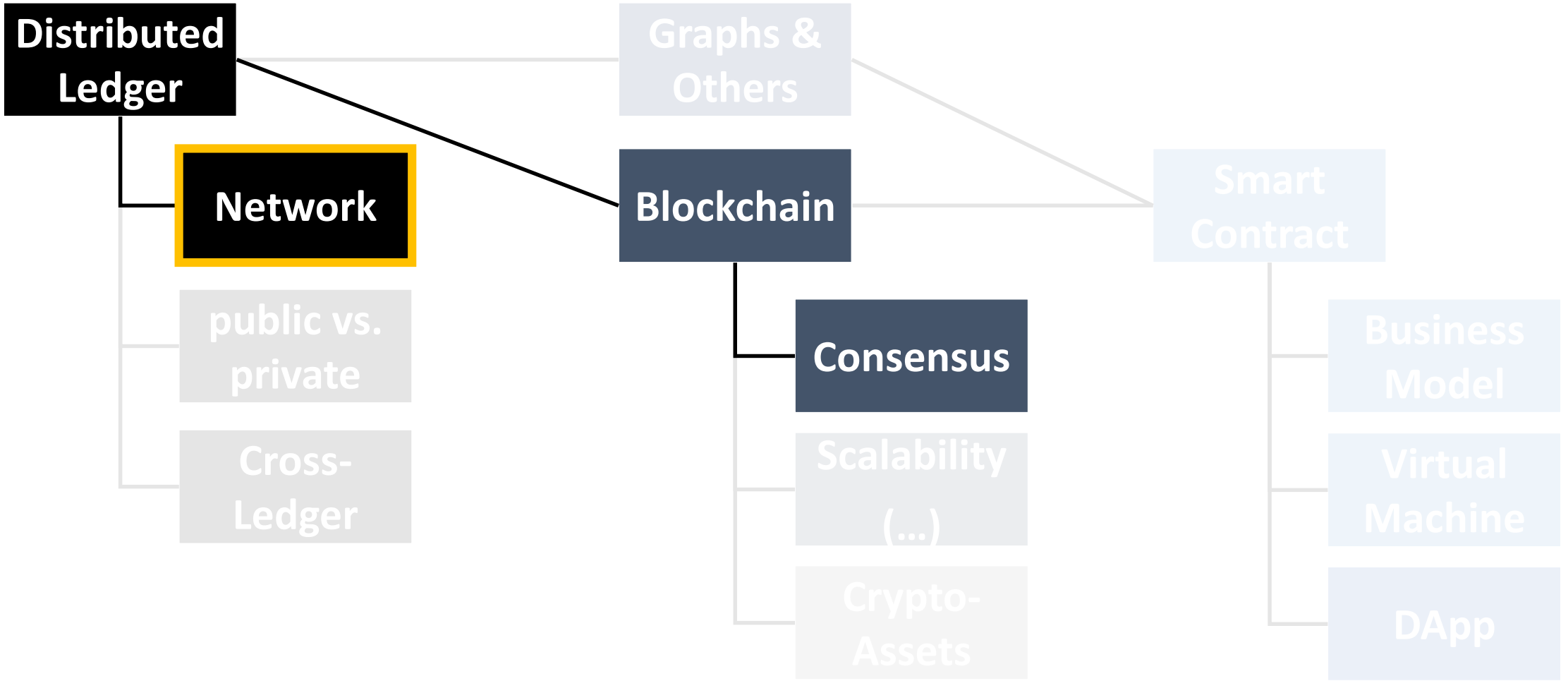
Let‘s focus on…



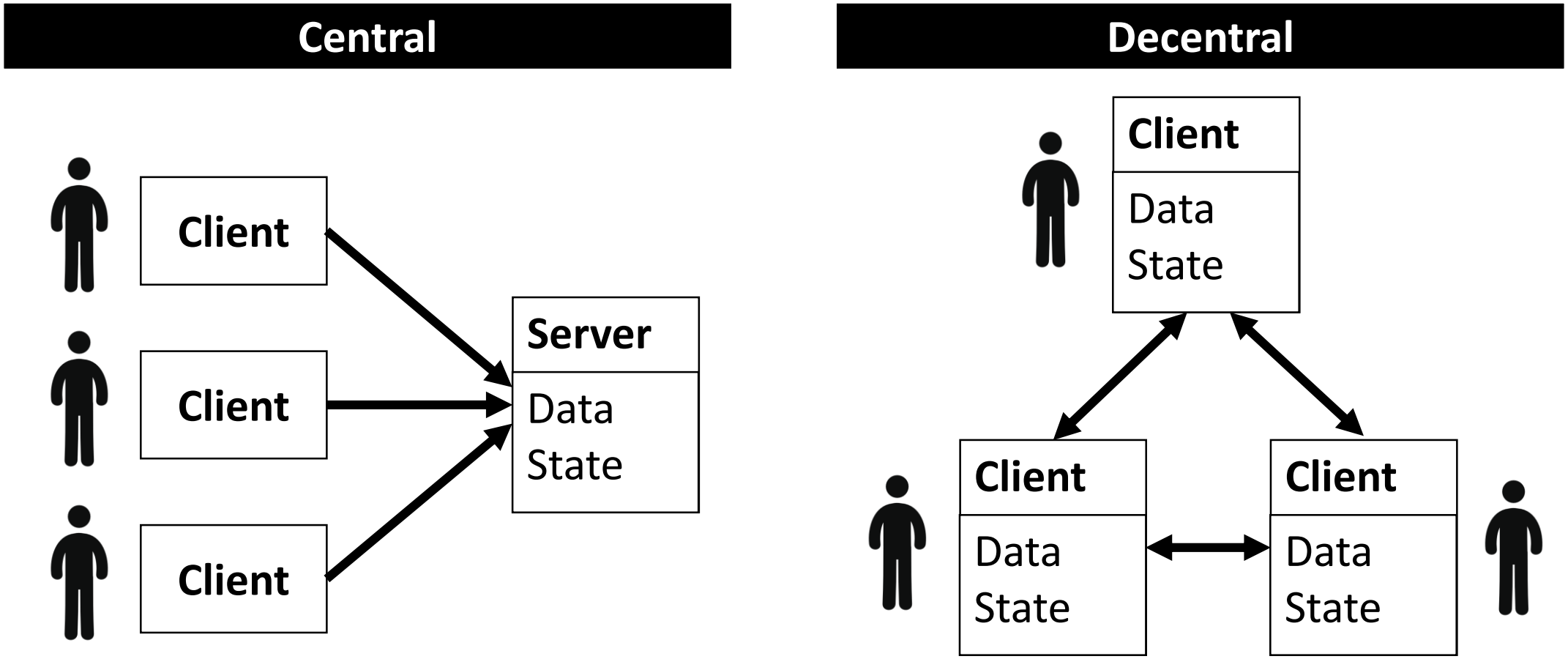
What is the Consensus?

- **Parties** that **don‘t trust** each other **agree** on the **state** of a system at a certain **time**.
- Reaching an Agreement:
  1. Collect state-changes (transactions)
  2. Define a “truth-giver“
  3. Truth-giver validates state-changes
  4. Truth-giver publishes new truth (state) to all others
  5. At least 51% of the nodes confirm the truth

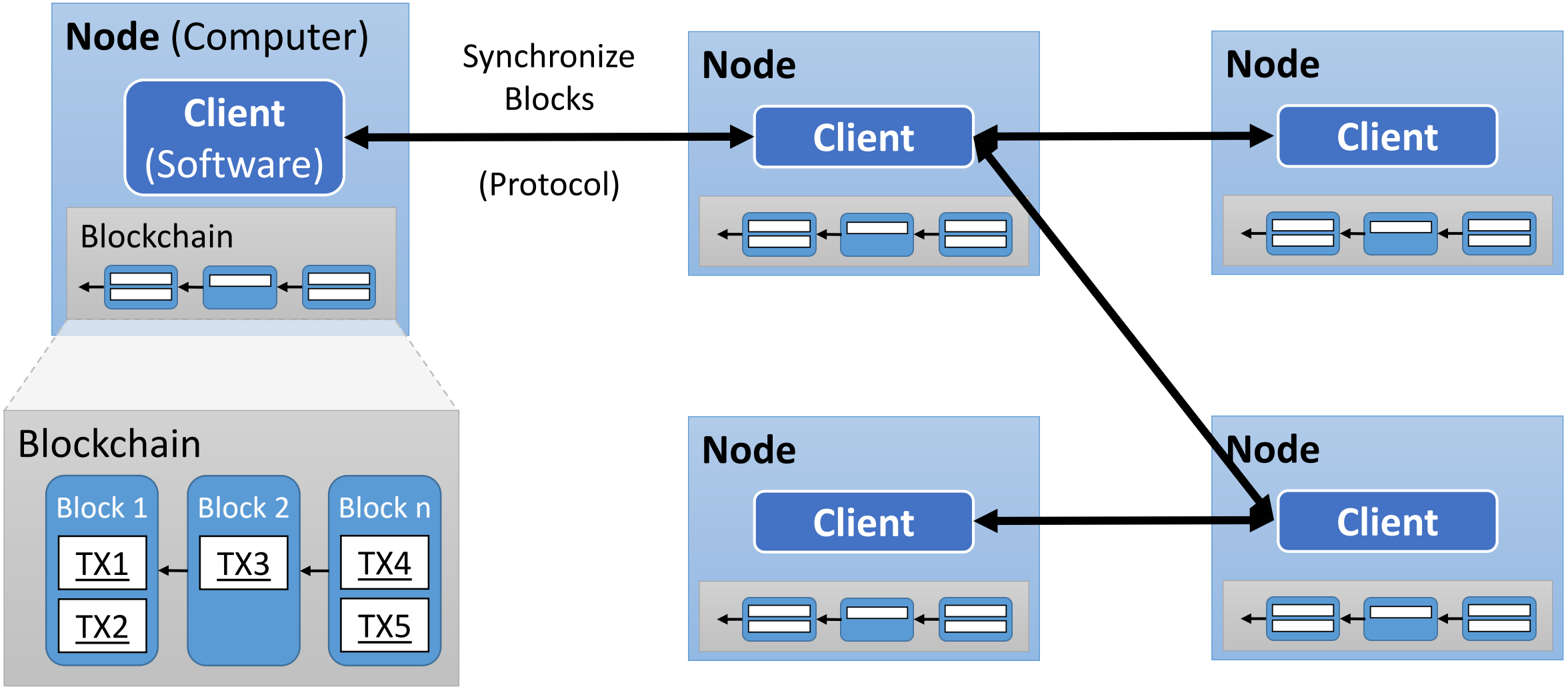
Let‘s focus on…



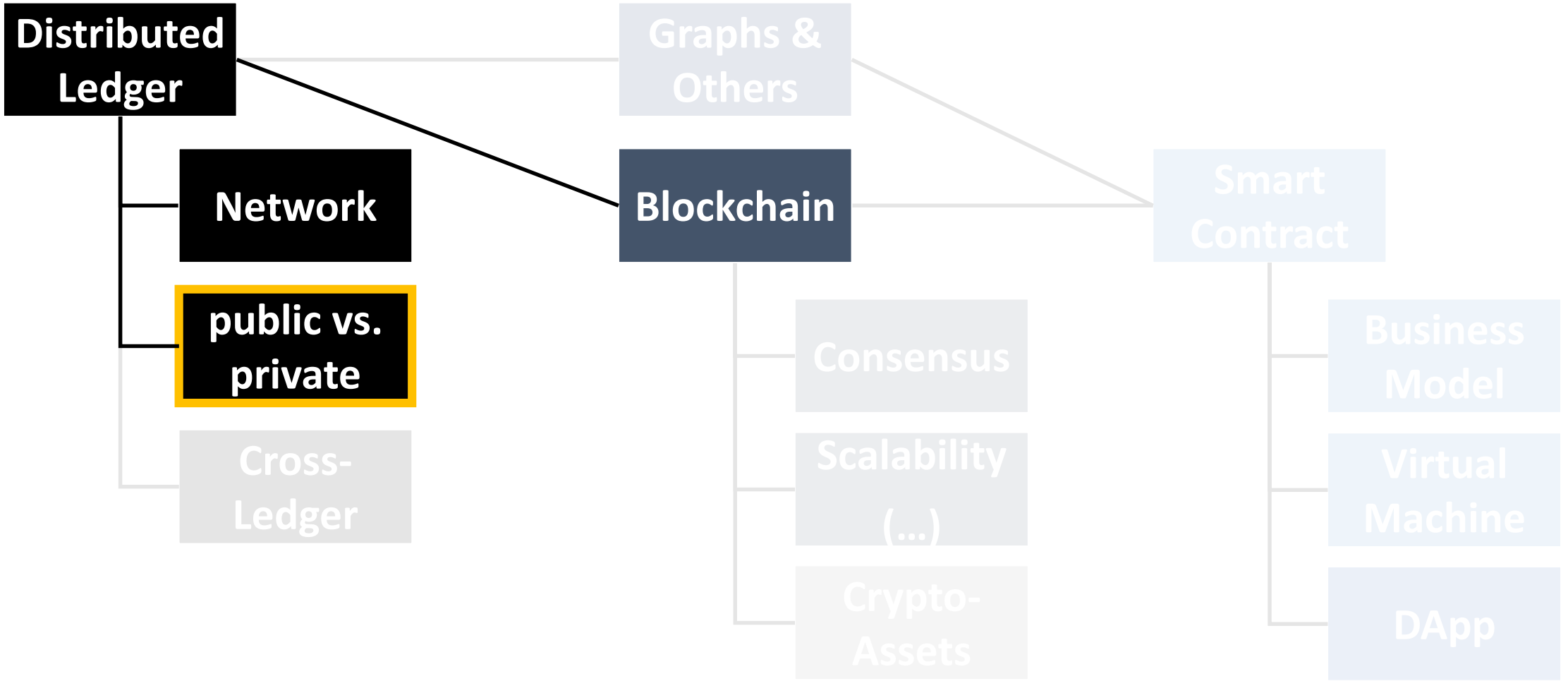
From Central to Decentral



Blockchain & P2P Network



Let‘s focus on…



Public Network

- Highest Goal: **Transparency**

- Users-base
  - Anybody can participate, no restrictions
  - Transparency might have restrictions through encryption

- Suitable for:
  - Financial Products (financial assets, financial transactions)
  - Auditing & Certification solutions

Blockchain Generations (public)

Generation 1	Generation 2	Generation 3
– Pure Currencies	– Smart Contracts – Smart “Assets”	– Tackling Scalability – “New ways”
– Bitcoin, Lightcoin, …coin	– Ethrereum, NEM, NEO, Cardano, …	– IOTA, Interledger, Cardano, Ethereum
– Use cases (almost) limited to coin exch.	– Smart “assets” as use-case enabler	– “Faster, lighter, …” – More use-cases

Disclaimer: These “generations” are highly opinionated! This is just a current overview, not the “ultimate truth”!

Permissioned (Consort.) & Private Networks

- Highest Goal: **Process Optimization & Digitalization**

- Users-base
  - Only selected (certified) parties can participate
  - Different “roles”, possibility to “ban” users

- Suitable for:
  - Connecting industry partners (tracking of assets, e.g. within a supply chain)
  - Standardizing/harmonizing & securing processes within an ecosystem

Blockchain Generations (permissioned)

Generations 1 →	Generation 2 →	“Generation 3”
– Big companies cook up own solutions	– Open Source – Linux Foundation	– Adoption by industry partners
– IBM, Intel, …	– Hyperledger umbrella project	– Hyperledger Project + Industry Partner
– Everything is quite “experimental”…	– Various platforms for different purpose	– Filling the platforms with life

Disclaimer: Permissioned networks were not classified in “generations” yet, this is a personal attempt to do so.

Mixtures…

- Highest Goal: **Tackle problems of public/permissioned solutions**

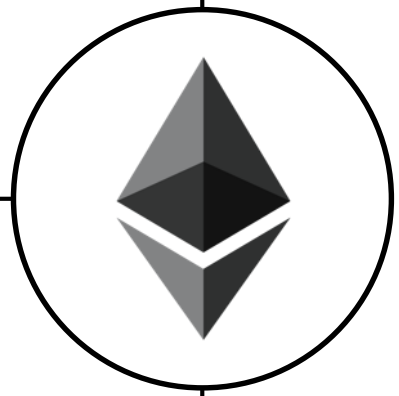
- Suitable for:
  - Additionally to already existing systems, e.g. to meet regulation
  - E.g. adding an identity proof solution to a public network

The Public Network crown goes to…

Ethereum

Key Feature

- Currency: ETH
- Smart Contracts
- EVM
- Proof of Work/Stake (Casper)
- Wisper (Messaging)
- Swarm (Distributed File Exchg.)



Key People / Community

- Ethereum Foundation (excerpt)
  - Vitalik Buterin
- Ethcore (excerpt)
  - Gavin Wood
- Ecosystem: geth, parity, eth, (…)

Status

"Production Ready"

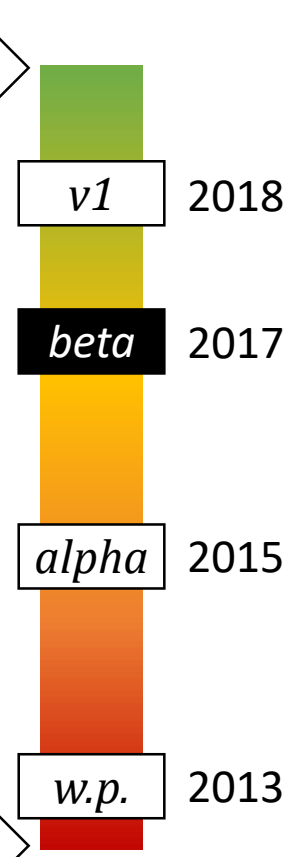
Version Name:
- Metropolis-Byzantium (since 16.10.2017)

Main-Net, Test-Net(s)

Market Cap:
- 28 Bio. US$

Funding/Assets:
- ~200 Mio. US$

Nothing implemented yet

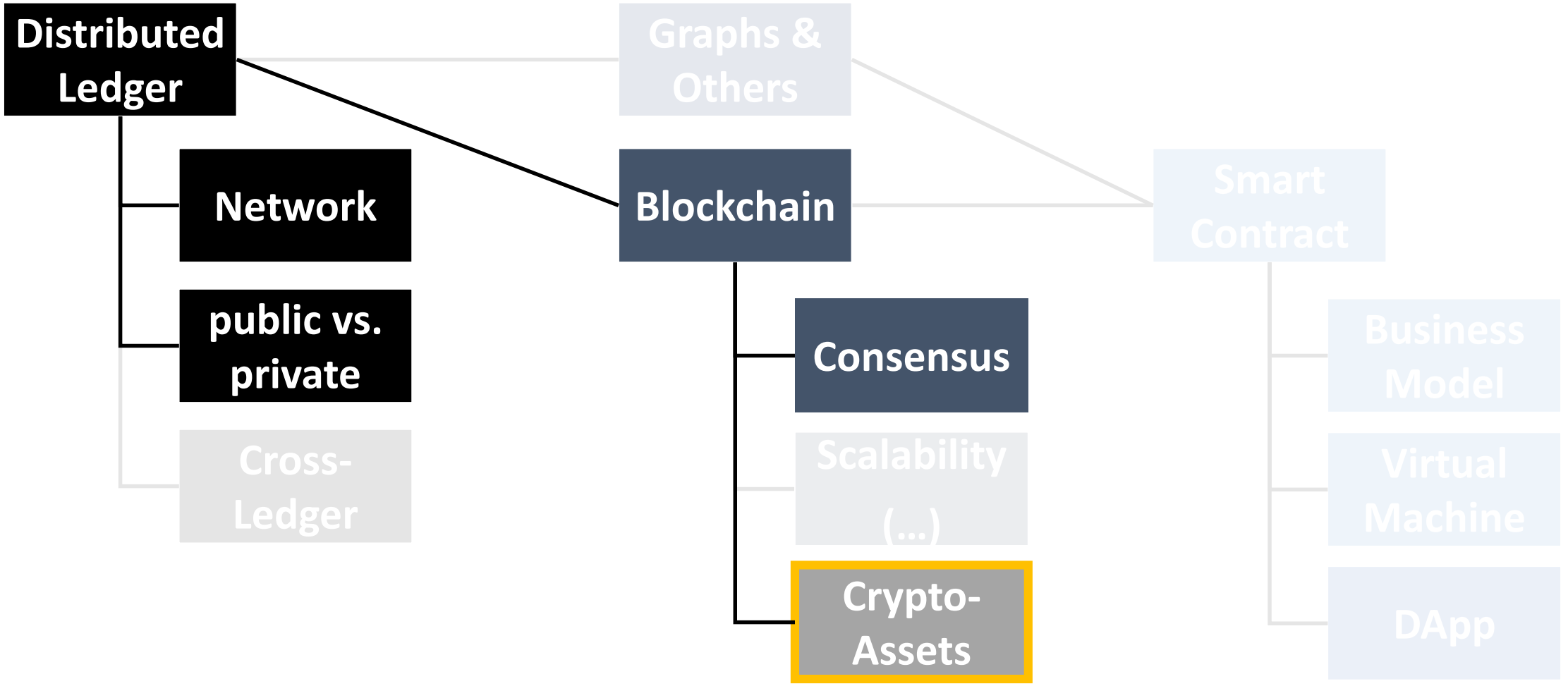


Link Ethereum video.

Basic introduction video by Vitalik Buterin.

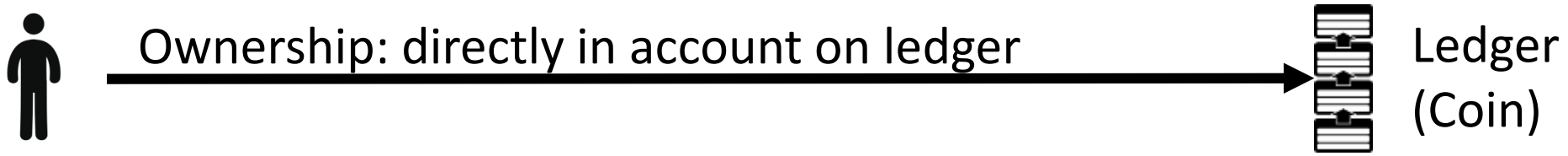
http://y2u.be/TDGq4aeevgY

Let‘s focus on…

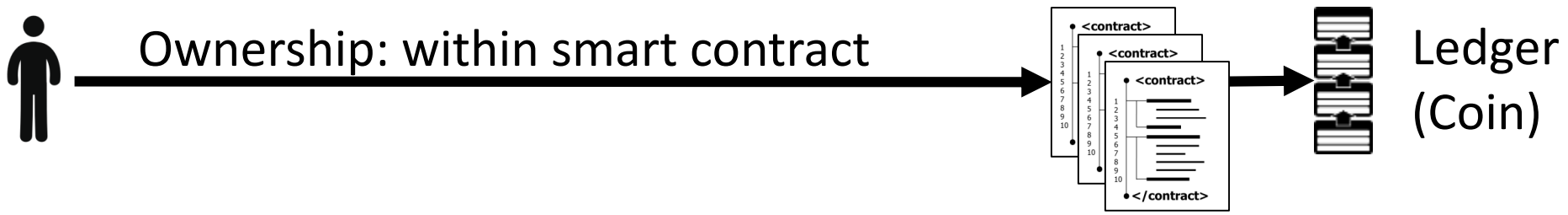


Coins vs. Tokens

- **Coin:** Money Creation through consensus protocol (ledger as base)



- **Token:** Money Creation through generation (smart contract as base)



- **ICO** (Initial Coin Offer) vs. **Token Sale**
  - Problem: Coins and Tokens are not distinguished clearly

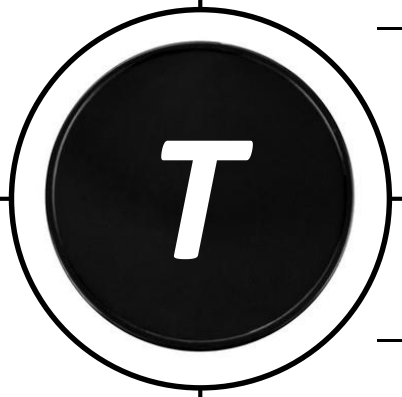
Tokens

Asset as “stock”

- Refers to value in real world (company, product)
- Initial Sale followed by Trade
- Not burnable

Asset as “reward”

- Reward for behavior in real world
- Unlimited supply, Trade possible
- Burnable against “real values”



Asset as “voting right”

- Refers to a virtual value
- (Un)Limited Supply, No Trade
- Burnable against an “action”

Currency on-top of currency

- Implement consensus protocol with smart contracts
- Theoretical concept (not practicable)

Ethereum “Killer Use Case”…

(currently)

ERC20 Token Standard

Use Case

- Smart Contract Token Standard
- Mostly used by Startups as alternative to stock (unregulated)

Technology

- Ethereum Smart Contracts (standard)

ERC20

Team / Links

Ethereum Foundation, Ethereum Developers
https://theethereum.wiki/w/index.php/ERC20_Token_Standard
https://etherscan.io/tokens

Status

Status: Productive

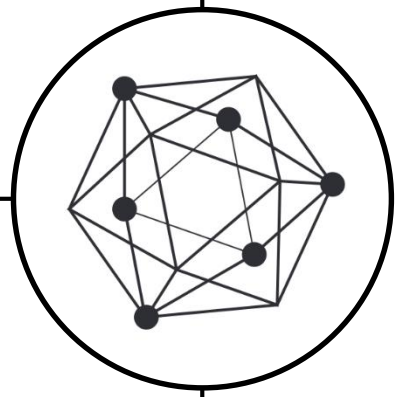
2018/05: > 83,400 ERC20 token contracts (main-net)

The Permissioned Network crown goes to…

Hyperledger Fabric

Key Feature

- Permissioned / Private Network
- For the “industries”
- Not focused on currencies, no tokens
- Swap of consensus mechanisms
- Flexible identity management (integration with Indy possible)



Key People / Community

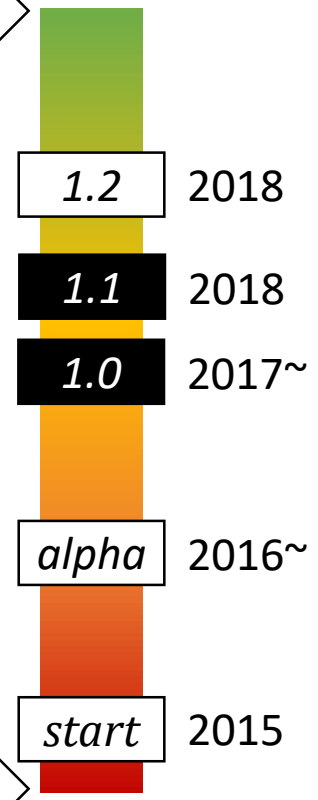
- Linux Fundation (Hyperledger umbrella project)
- IBM
- Digital Asset

Status

“Production Ready”

Currently in v1.0
Working on experimental features of v1.1

V1.2 planned for June 2018



Nothing implemented yet

Link Hyperledger Fabric video.

Basic introduction video with simple use case.

http://y2u.be/js3Zjxbo8TM

Hyperledger Fabric “Killer Use Case”…

(currently)

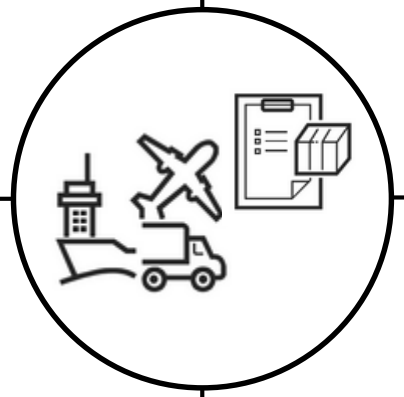
Maersk – IBM shipping industry platform

Use Case

- Trading & Certification
- Global trade digitization platform
- Open standards
- Global shipping ecosystem

Technology

- Hyperledger Fabric
- Hyperledger Indy (possible)

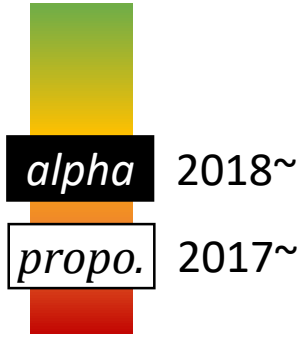


Team / Links

A.P. Moller-Maersk
IBM

Status

Status: Announced
(16.01.2018)

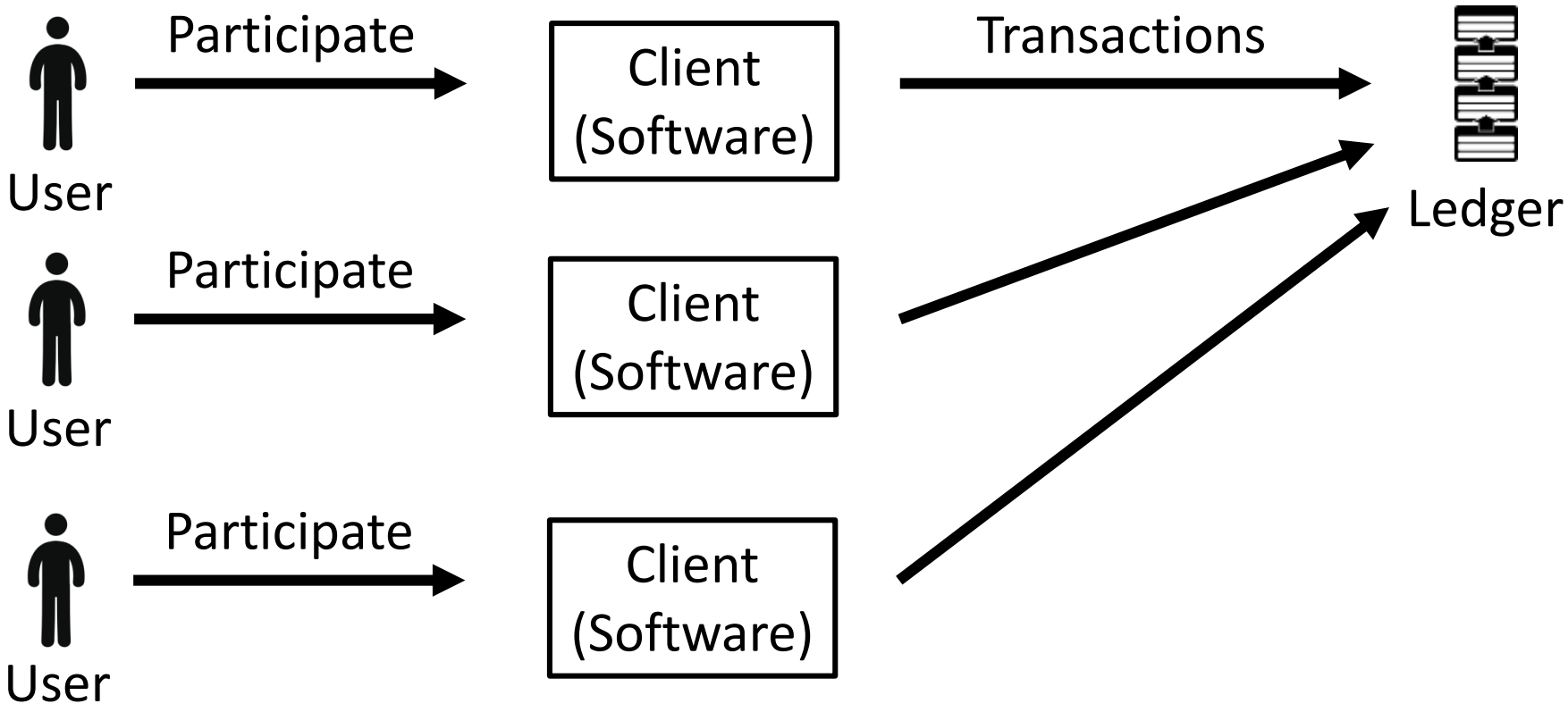


We’ve got a basic overview…

… let’s dive a little deeper!

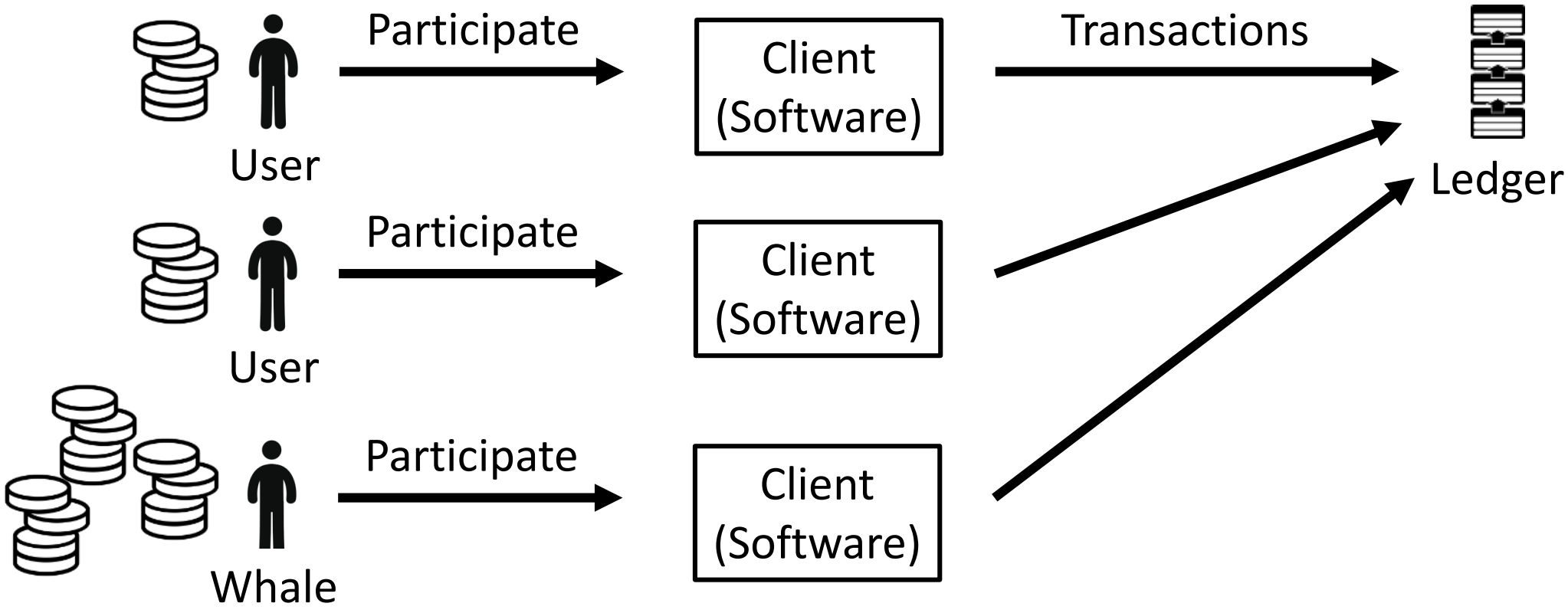
User

- **Users:** Use the network by creating transactions



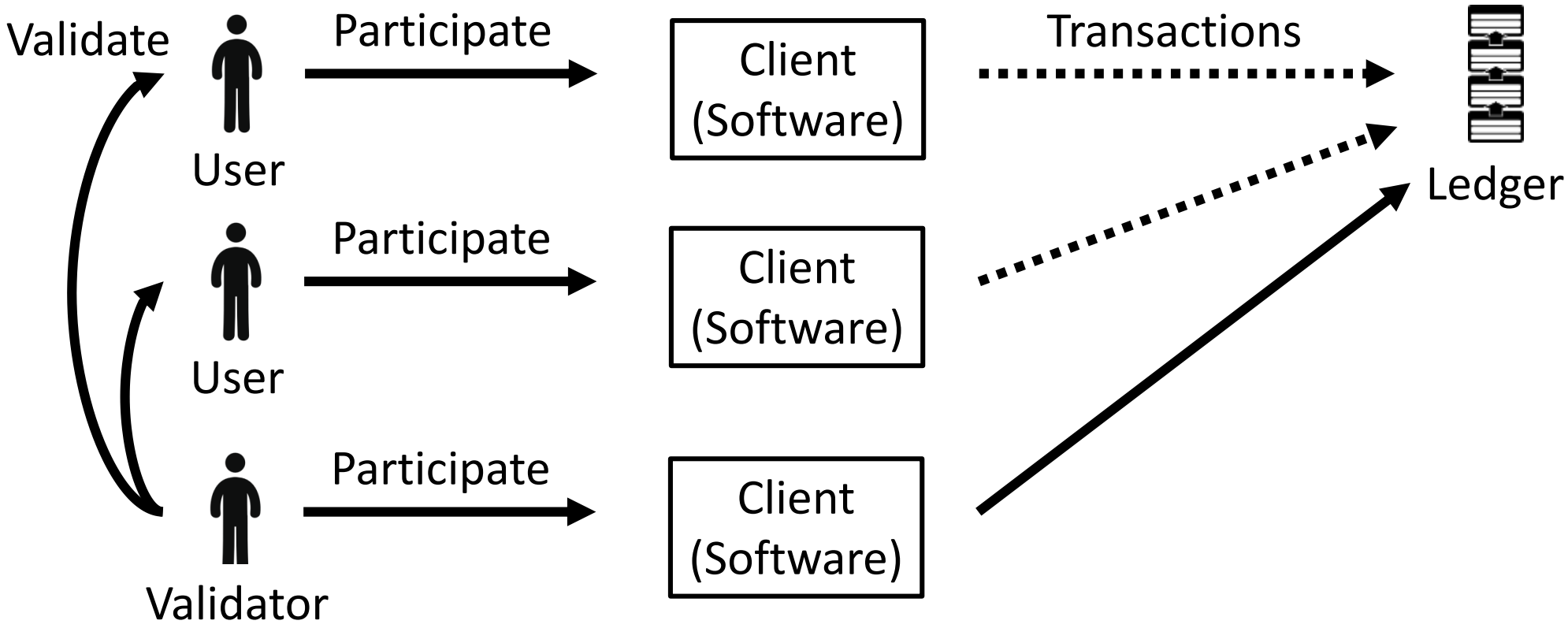
User in public networks

- **Users & Whales:** Users with many crypto-assets are called whale



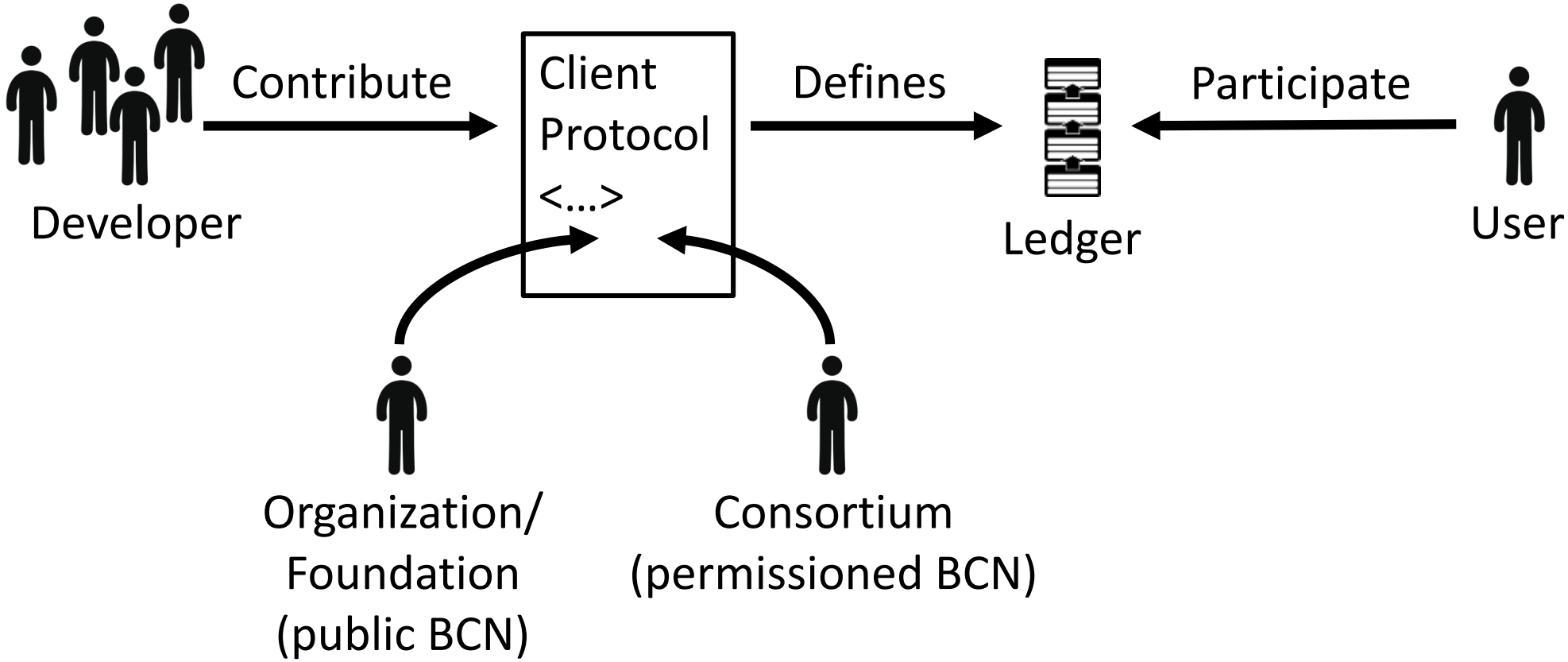
User in permissioned networks

- **Users have roles:** Users can have e.g. right to validate transactions or not



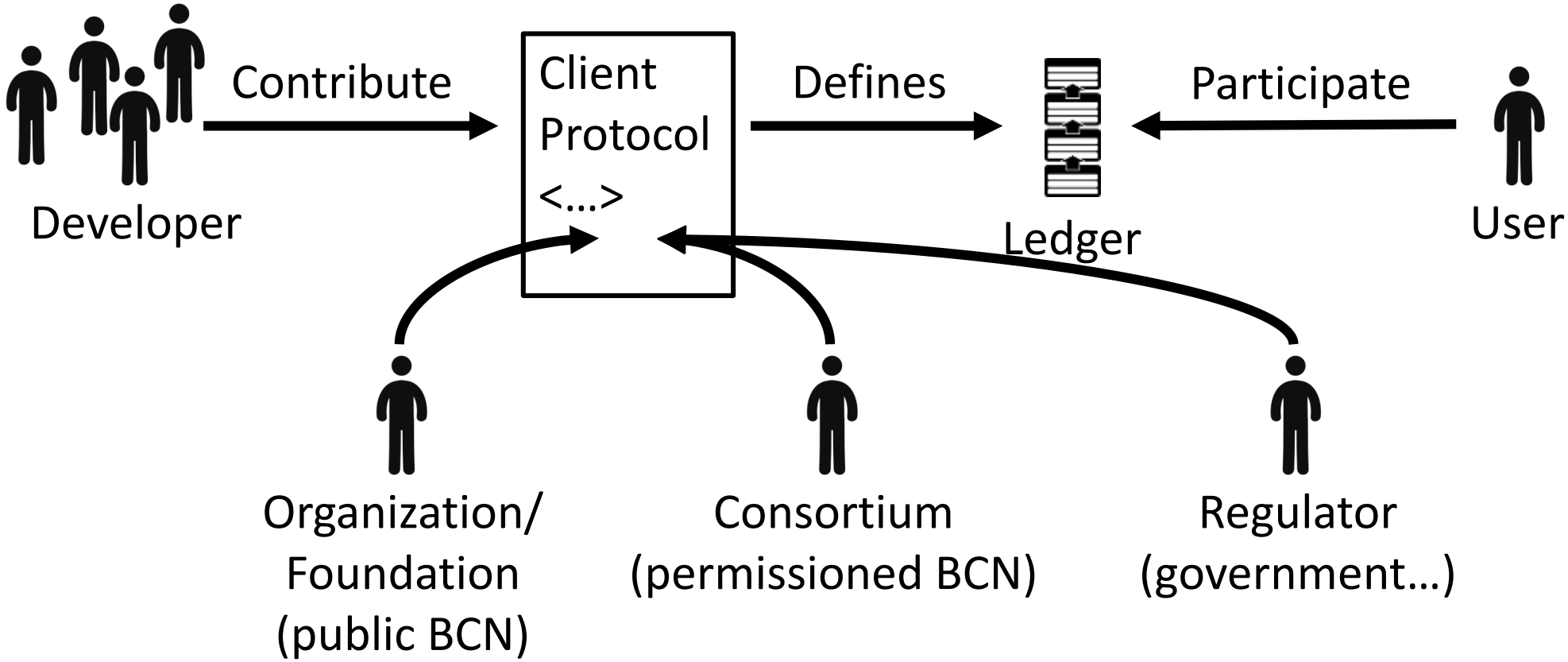
Developer

- **Developers:** Developers implement the protocol → all Open Source



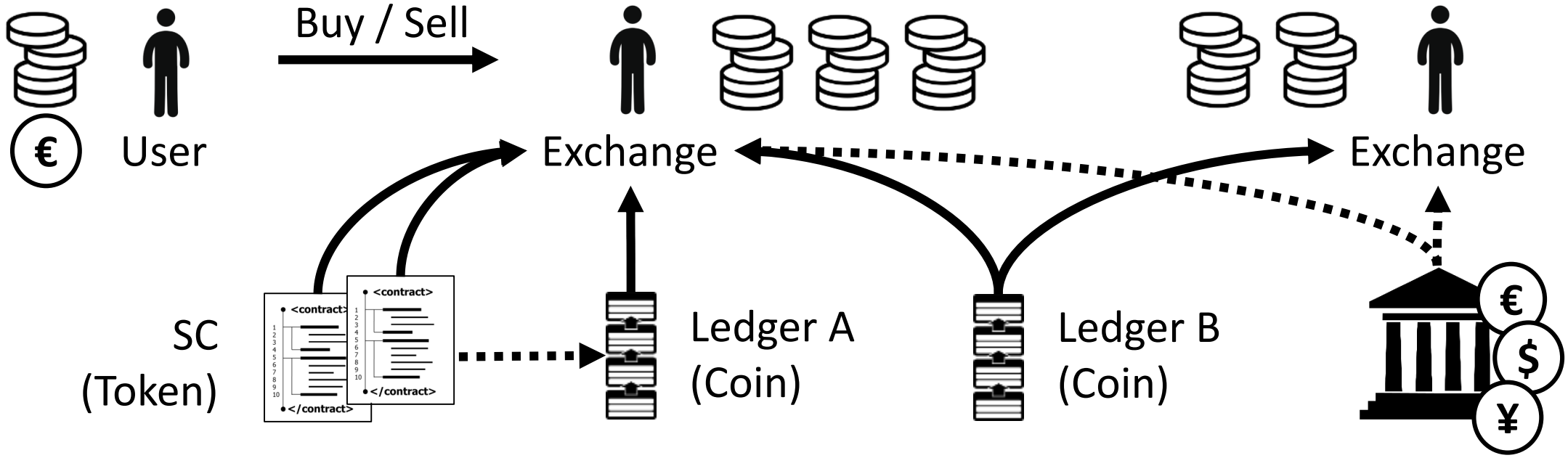
Regulators (?)

- **Regulators:** In the future regulators might interfere with implementation



Exchange of crypto-assets

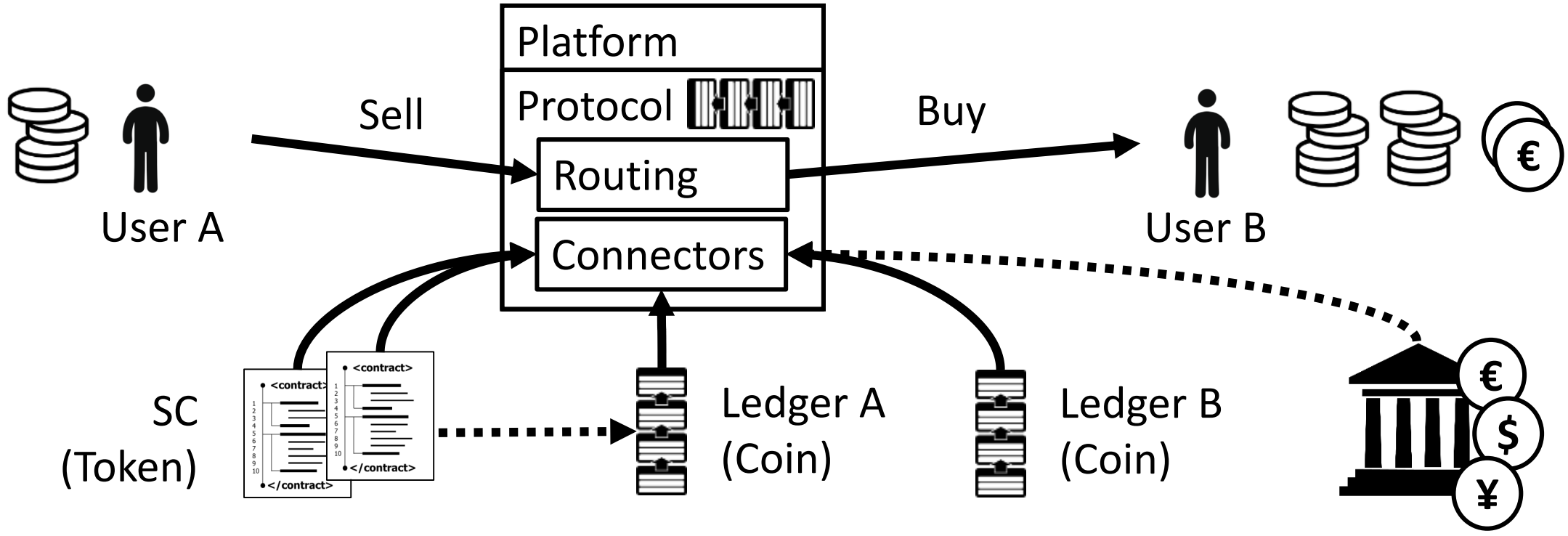
- **Exchange:** Central instance in a decentral network



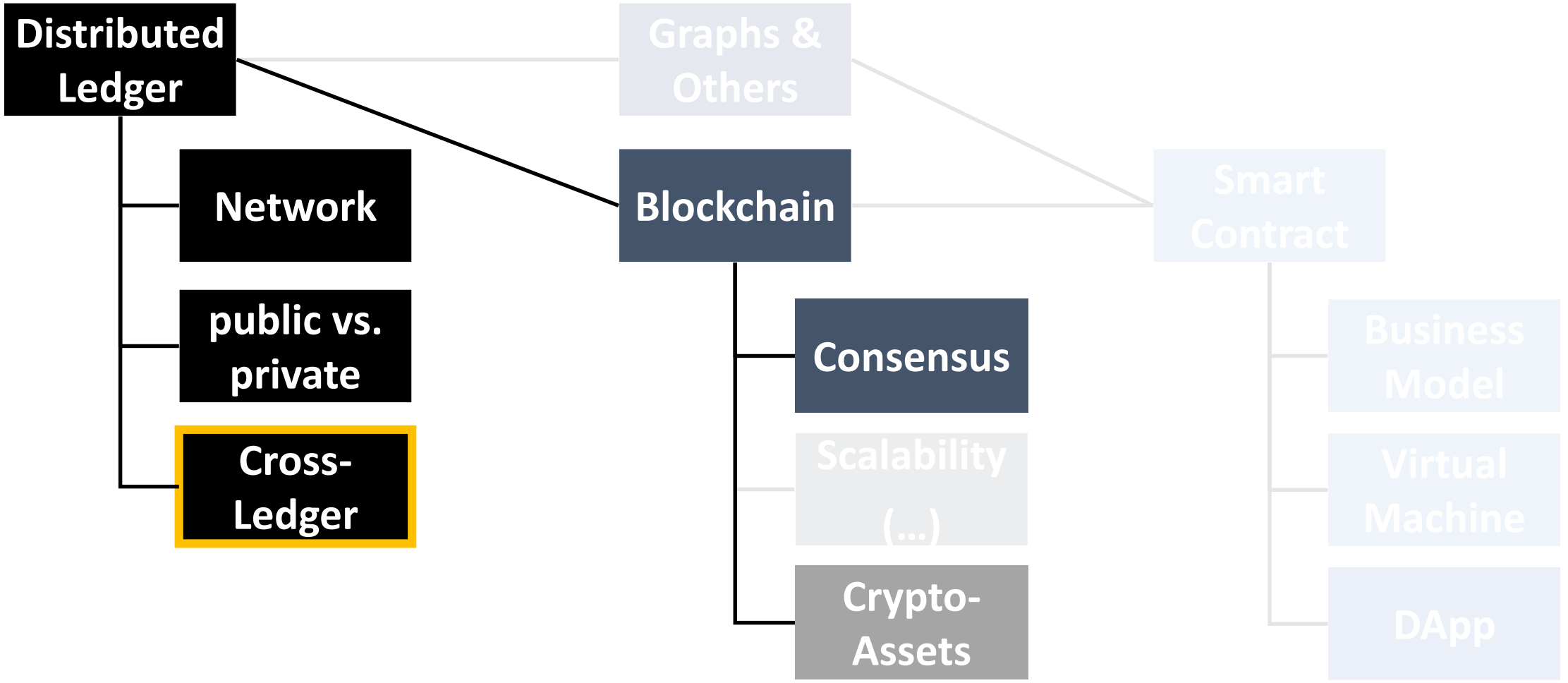
- **Supply & Demand:** Value of crypto-assets defined by supply & demand

Future of Exchanges

- **Decentralization:** No central exchange, but a platform (protocol + ledger)



Let‘s focus on…



Interledger

Key Feature

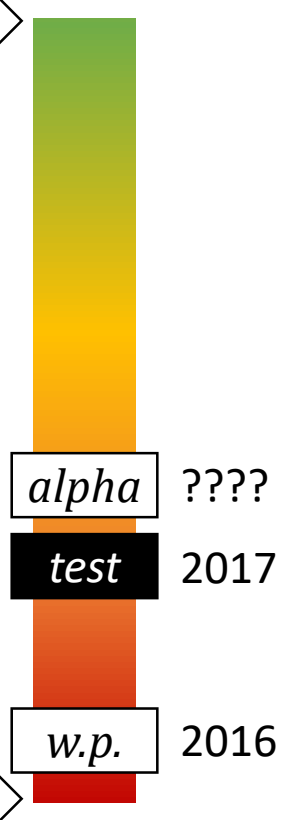
- The “exchange of exchanges”
- IL Payment Protocol
- Anybody can be a “connector”
- Connector defines exchange rate
- Routing

Status

“Production Ready”

Test-Wallets
No UI yet
Not much info on roadmap

Current version: ILP v4



Nothing implemented yet

Key People / Community

- Ripple
- Interledger W3C Community Group

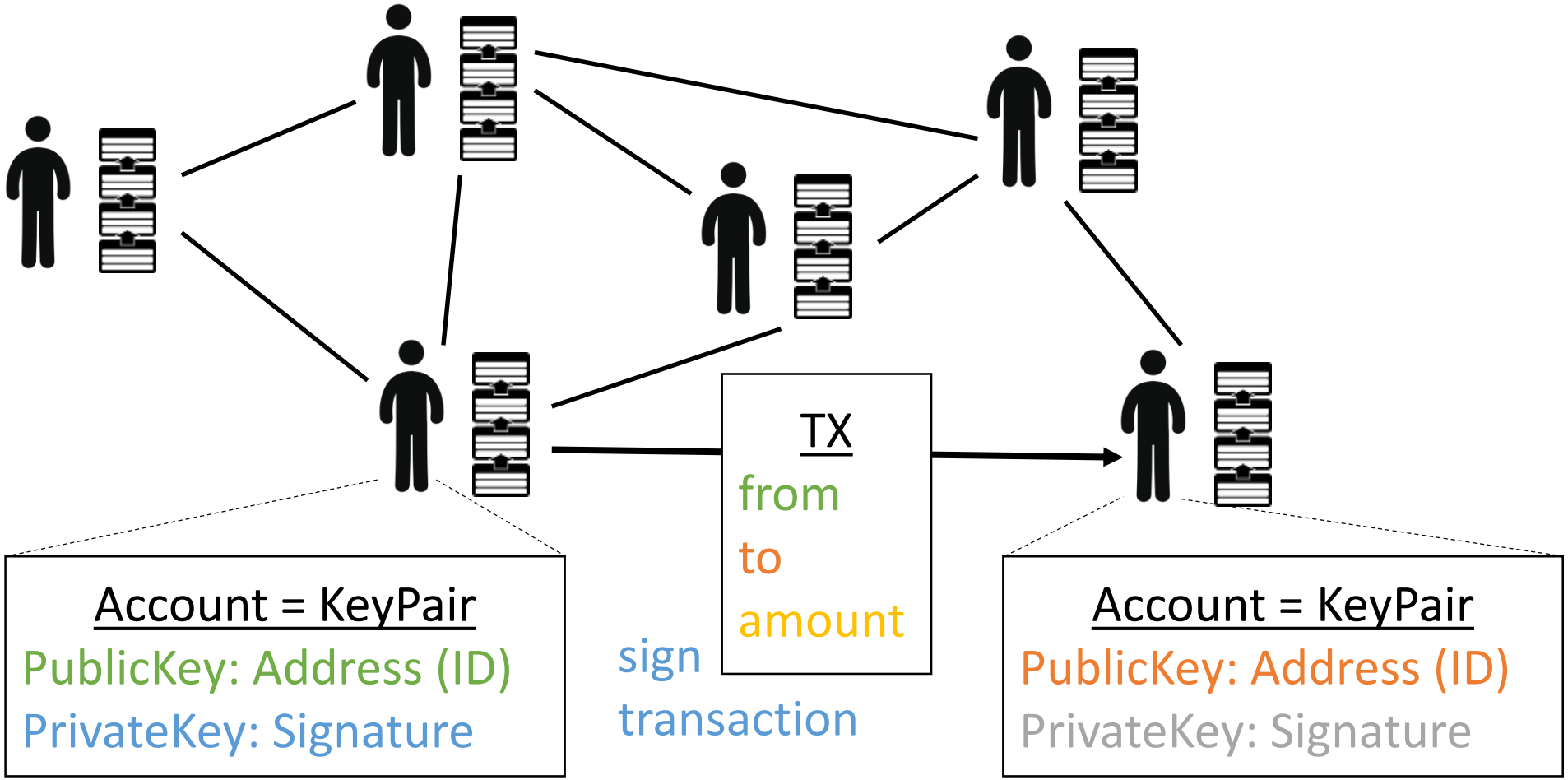
Identity – and why it matters

- Ability to hold a person liable
- Anonymity ++ → Trust --

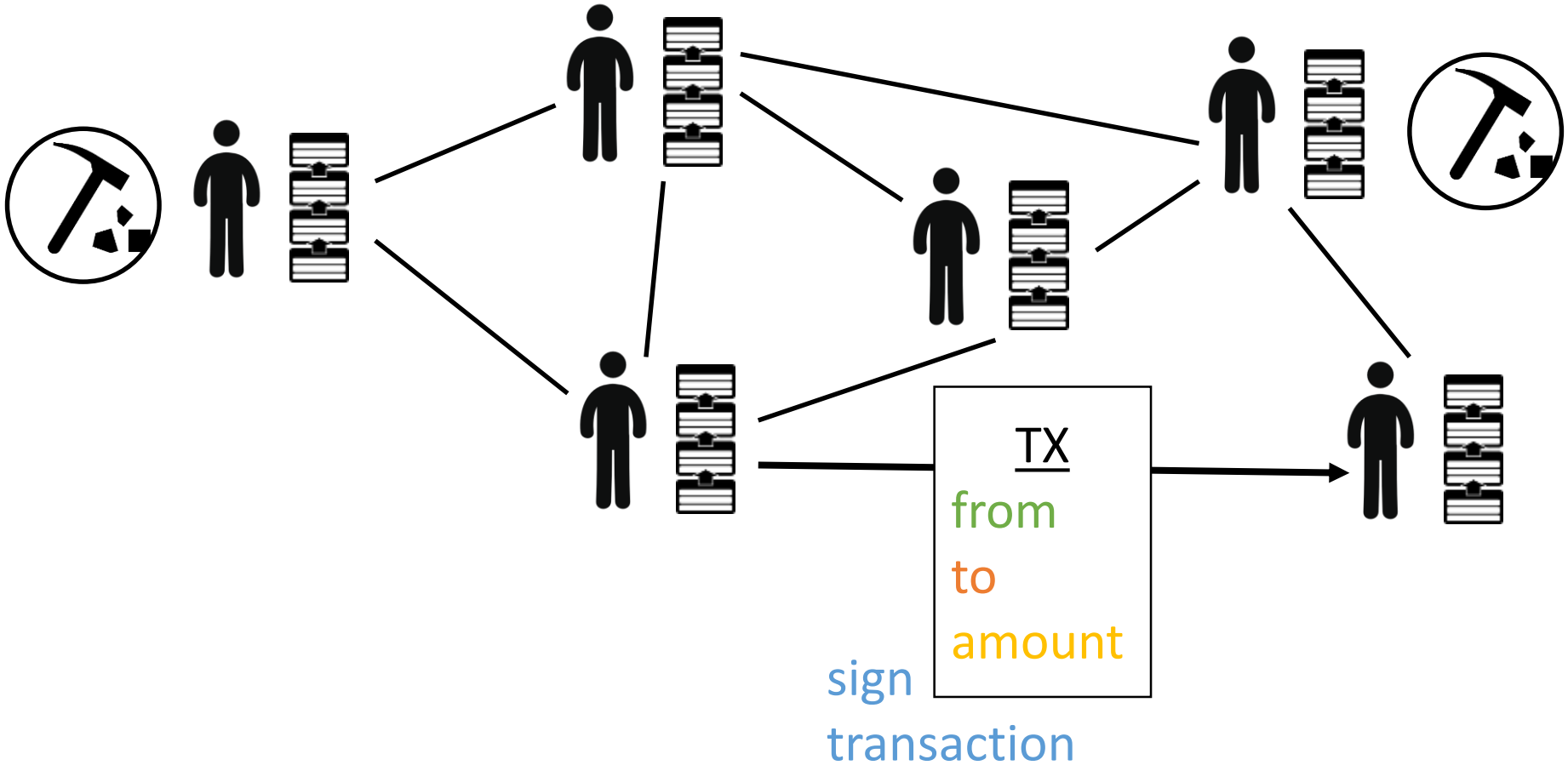
- Level of anonymity of a person depends on the use-case!

- And what about privacy…?

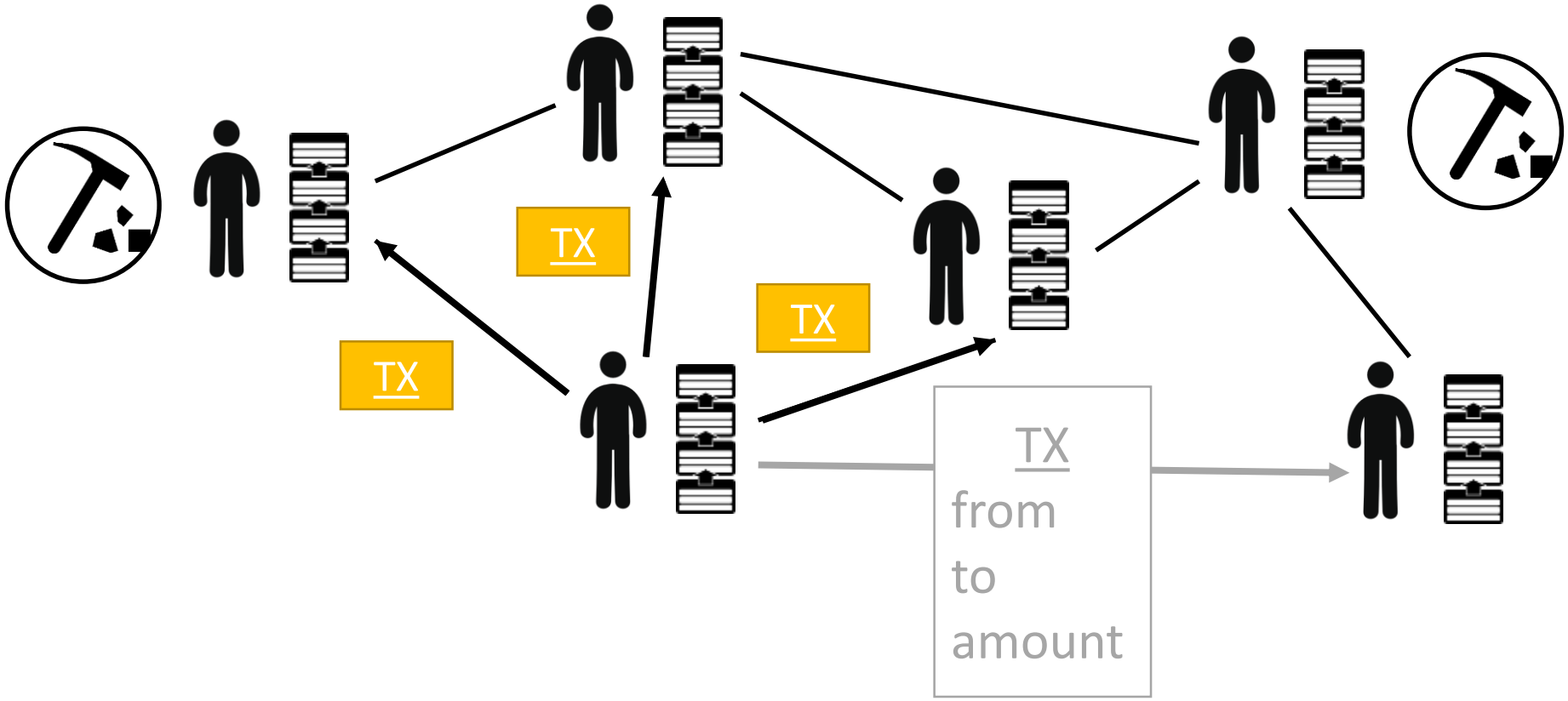
Identity in public networks



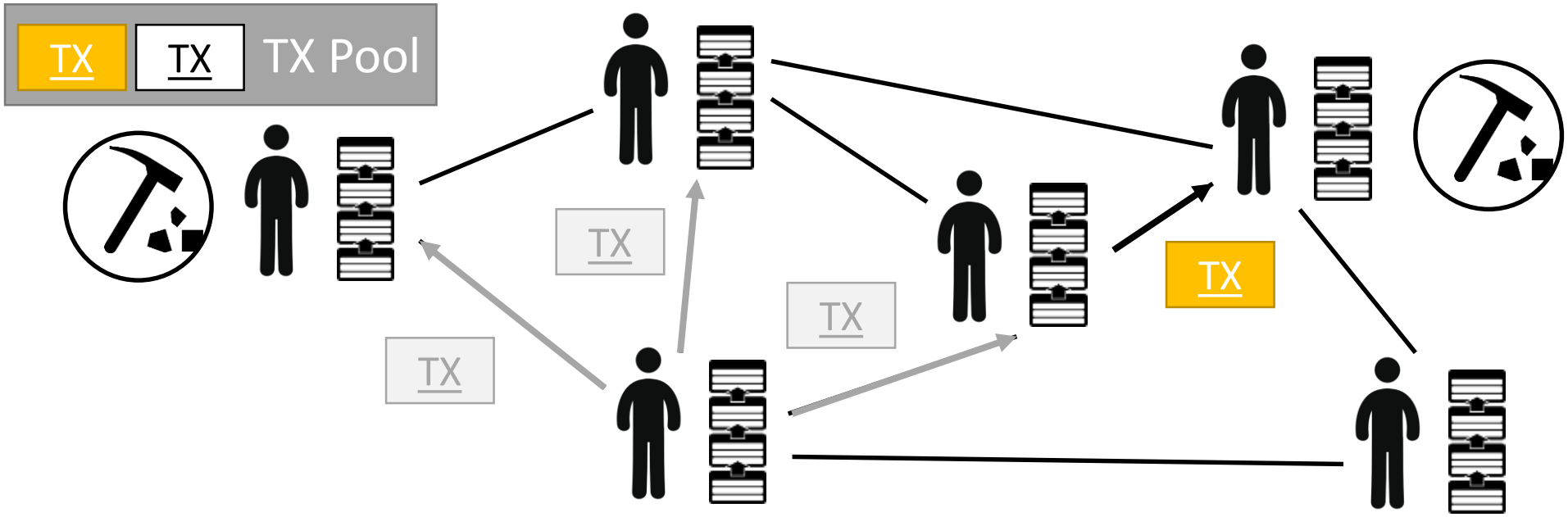
Proof of Work



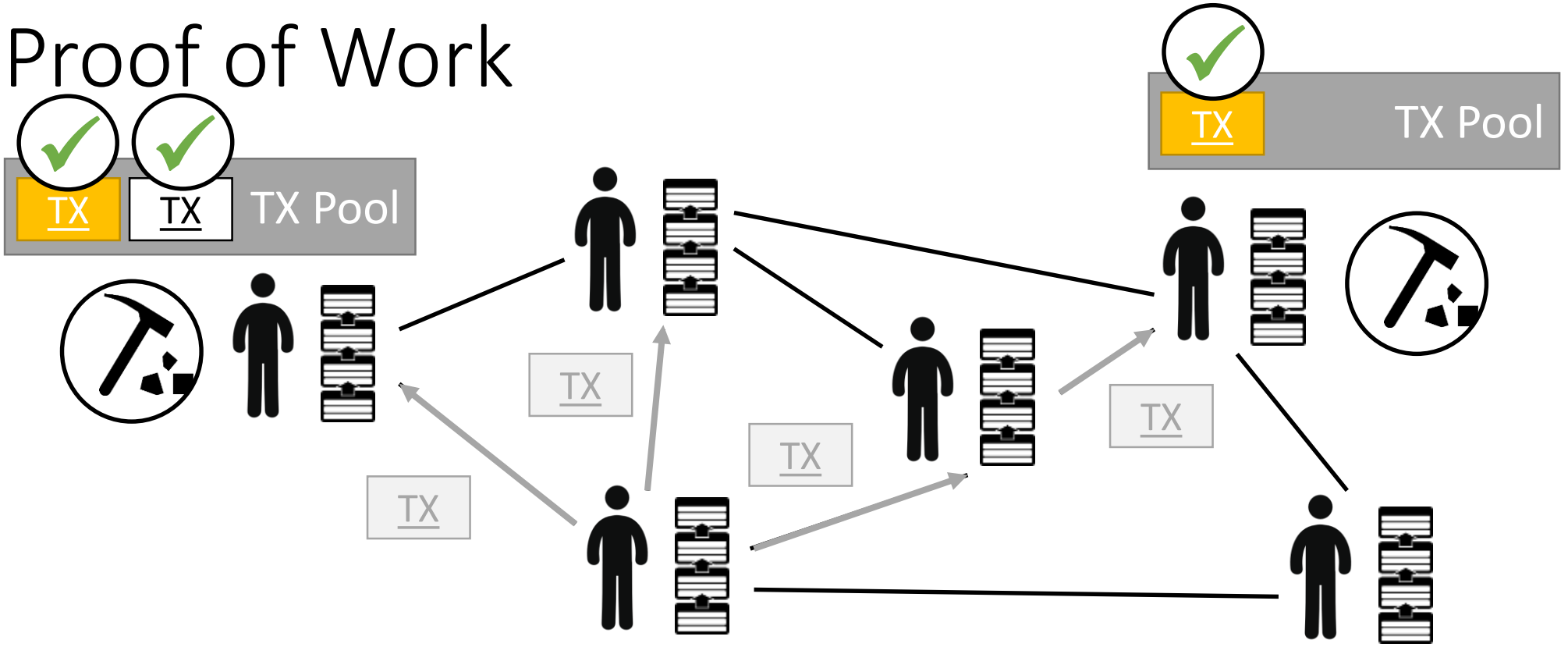
Proof of Work



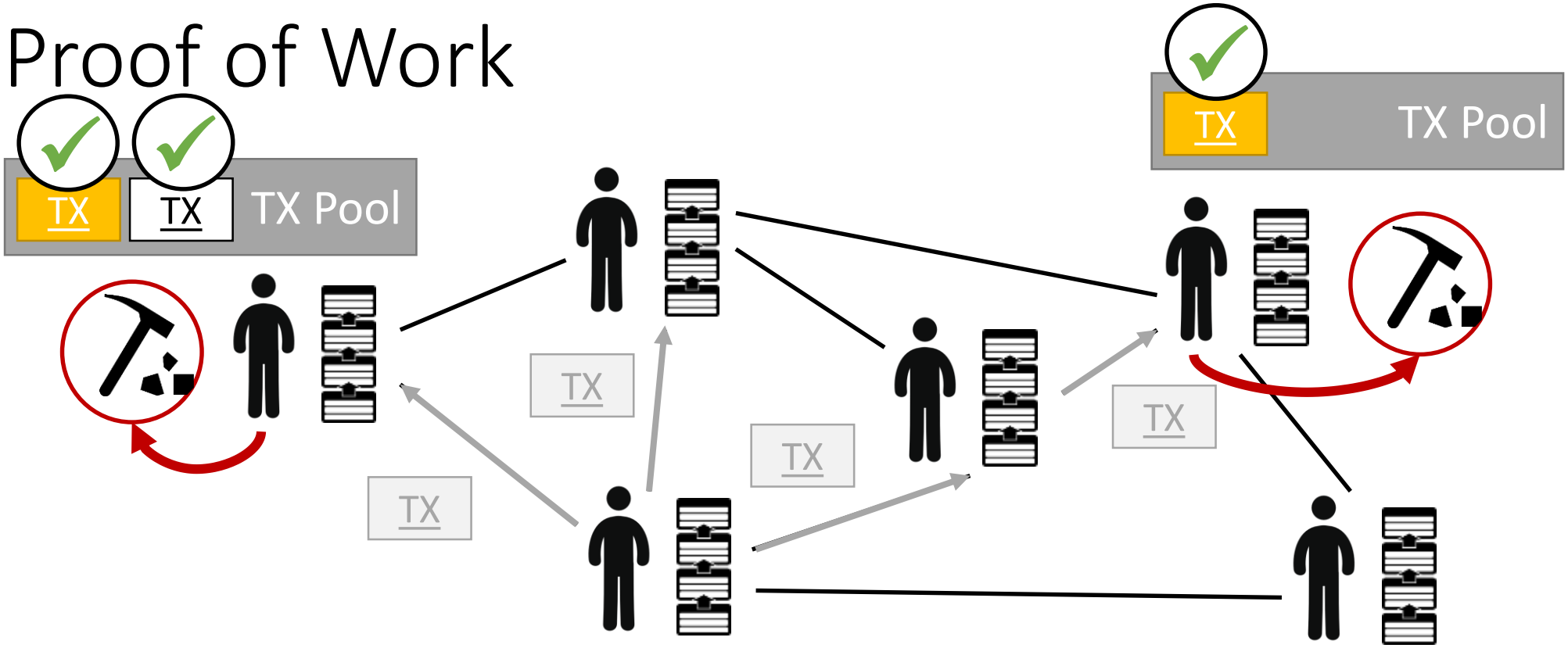
Proof of Work



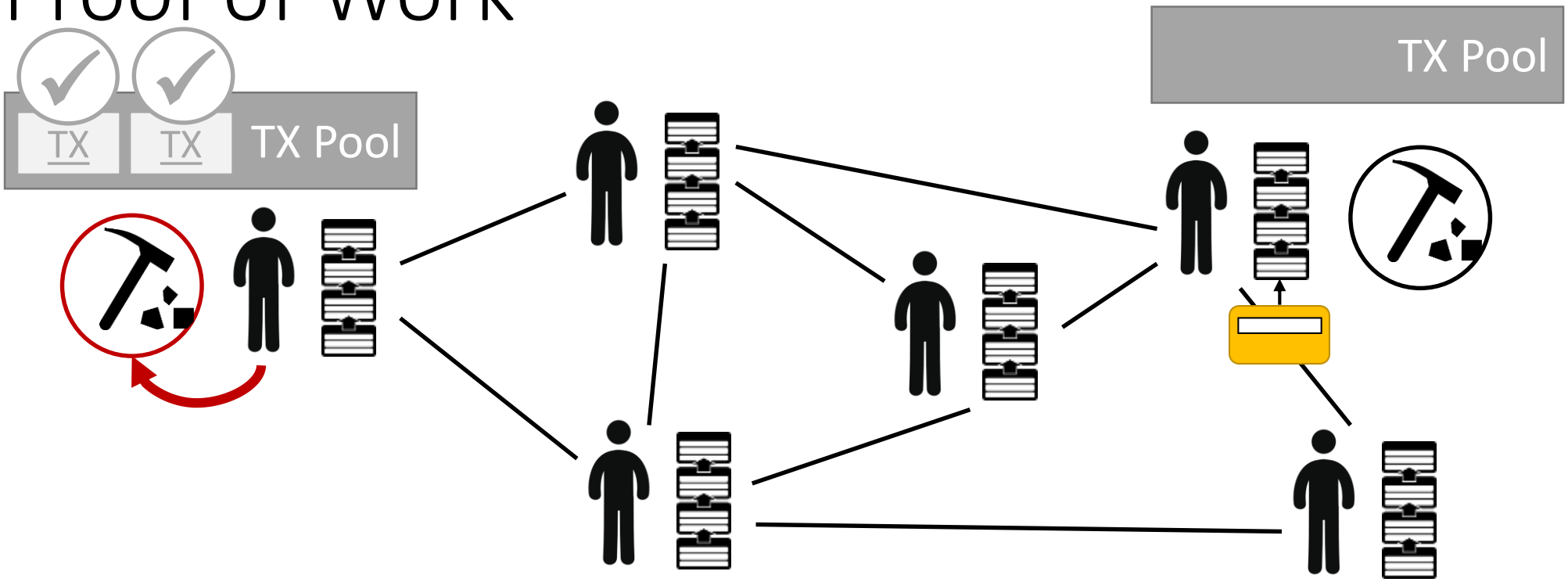
Proof of Work



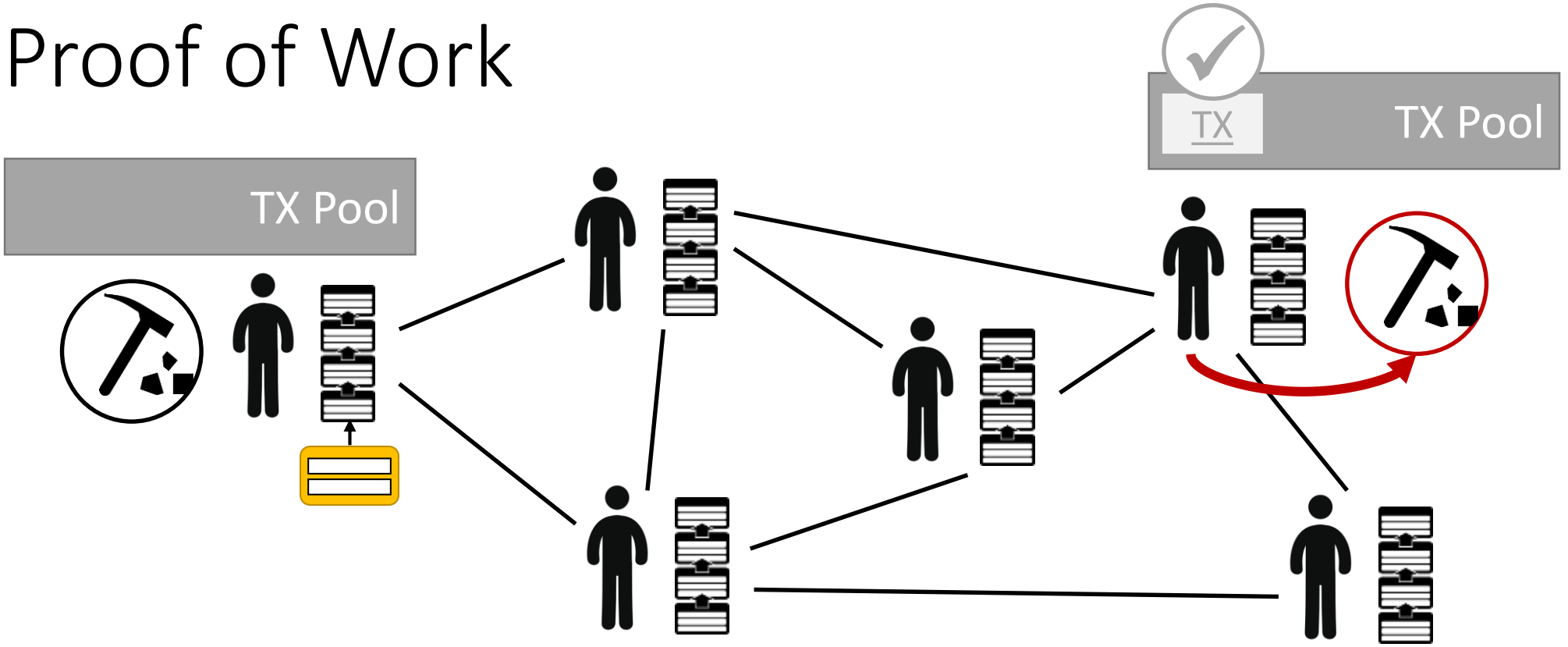
Proof of Work



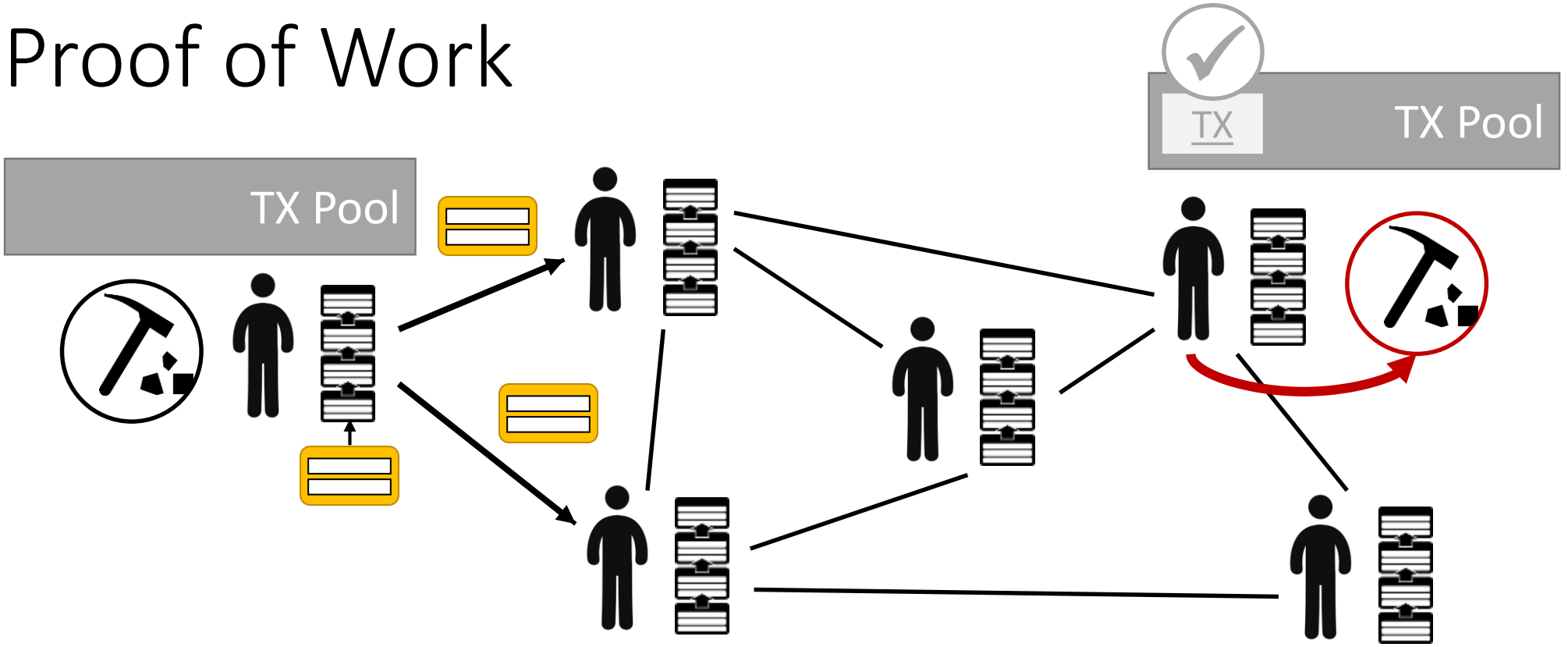
Proof of Work



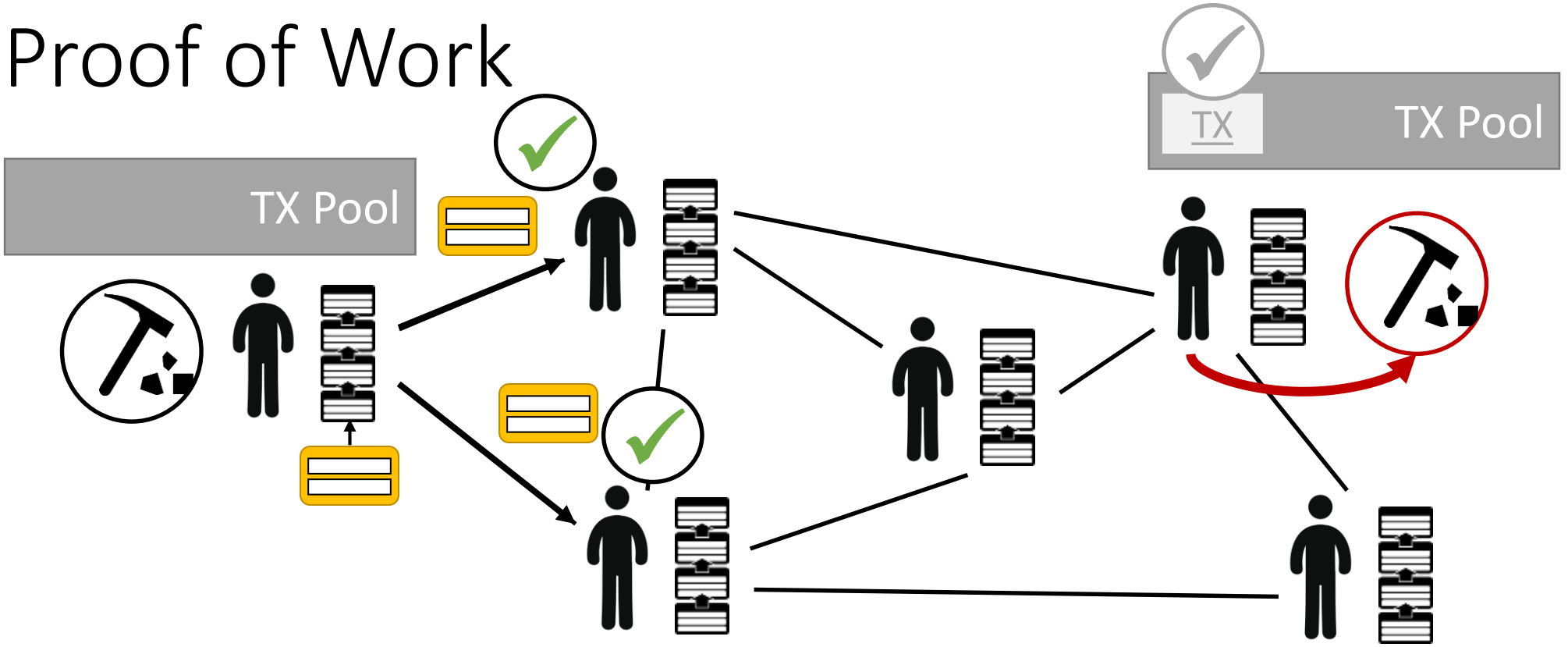
Proof of Work



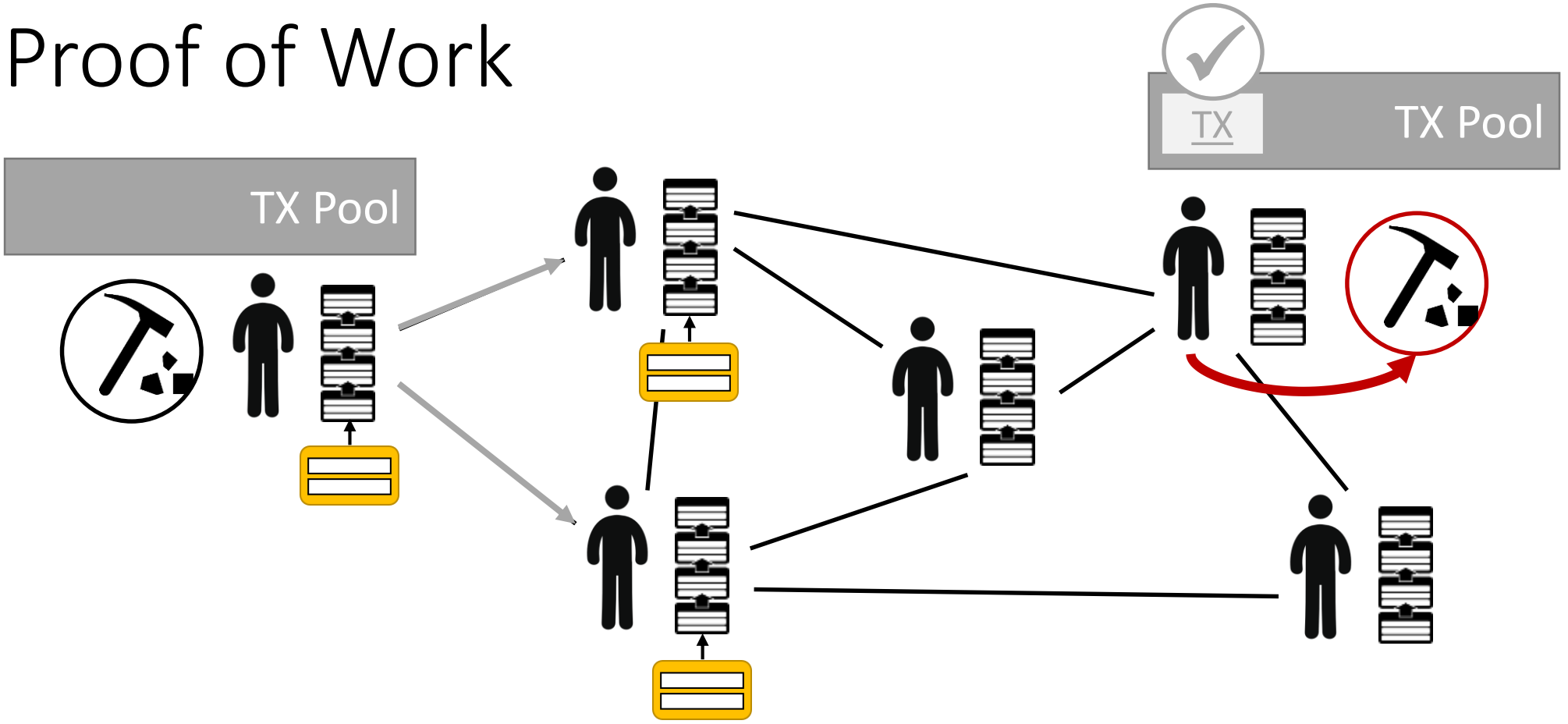
Proof of Work



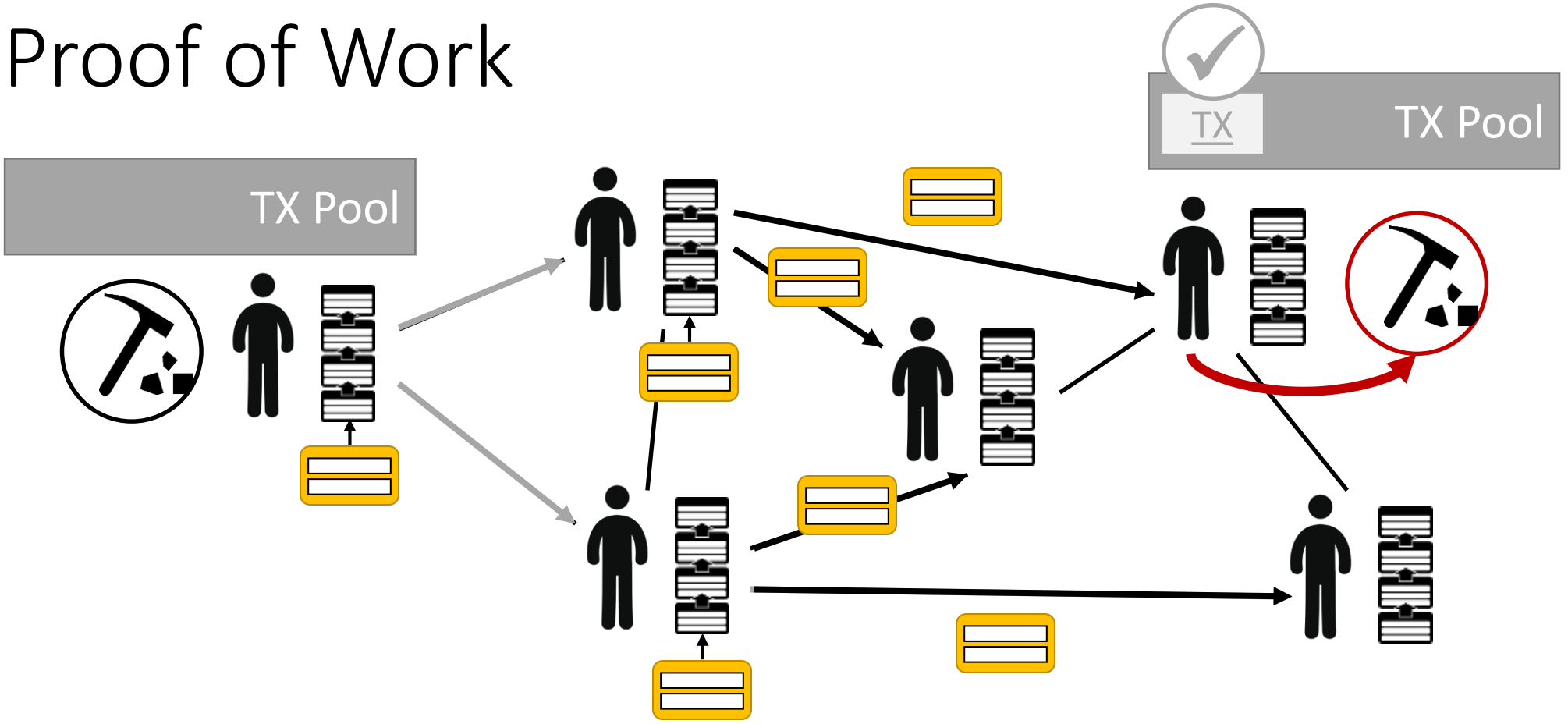
Proof of Work



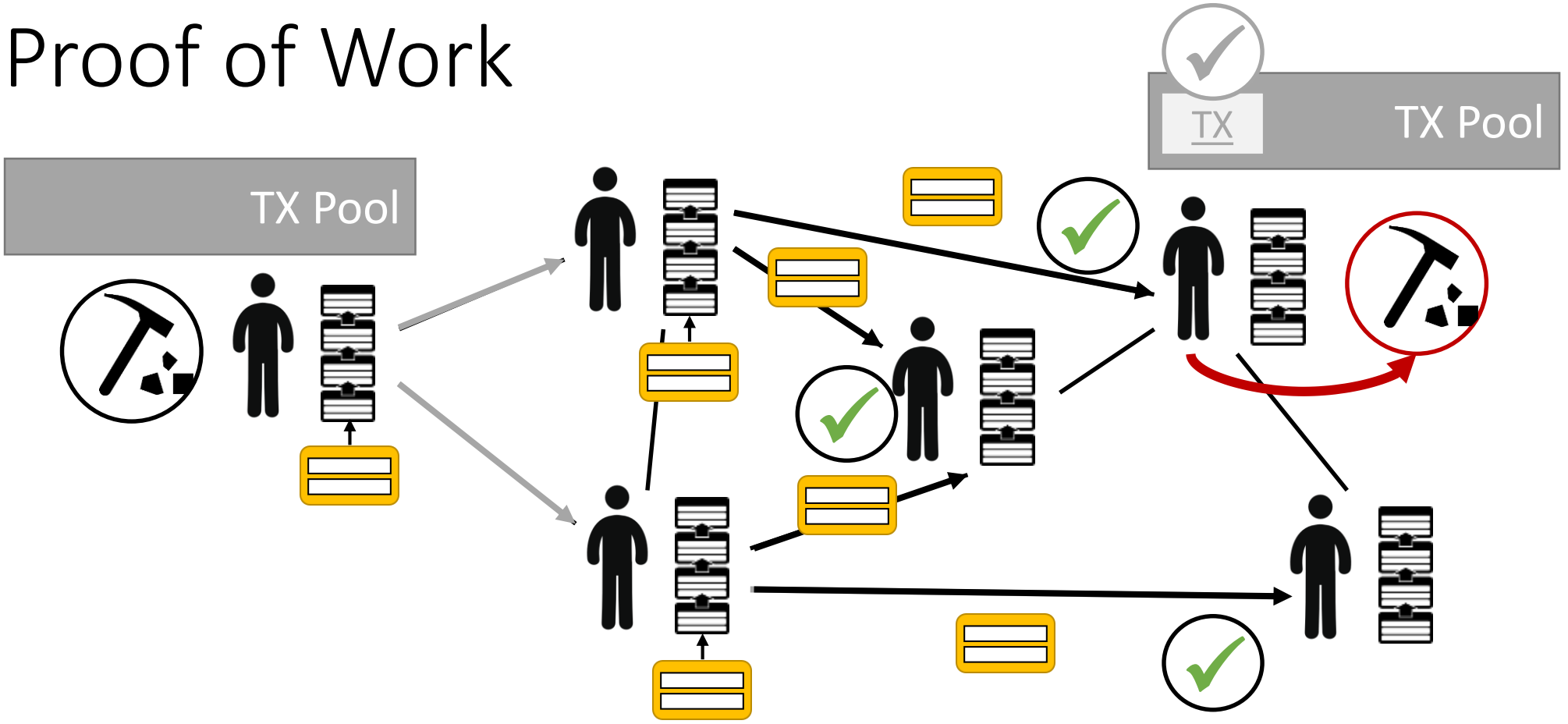
Proof of Work



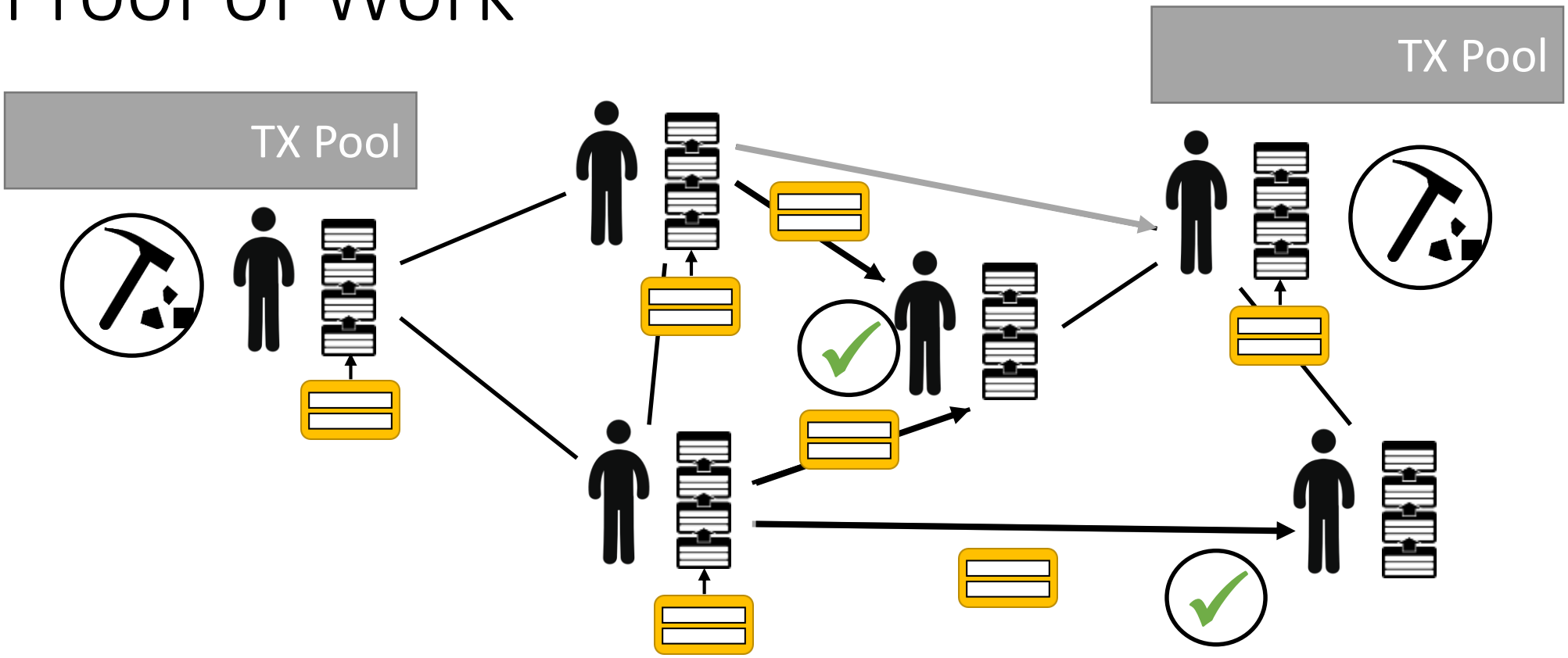
Proof of Work



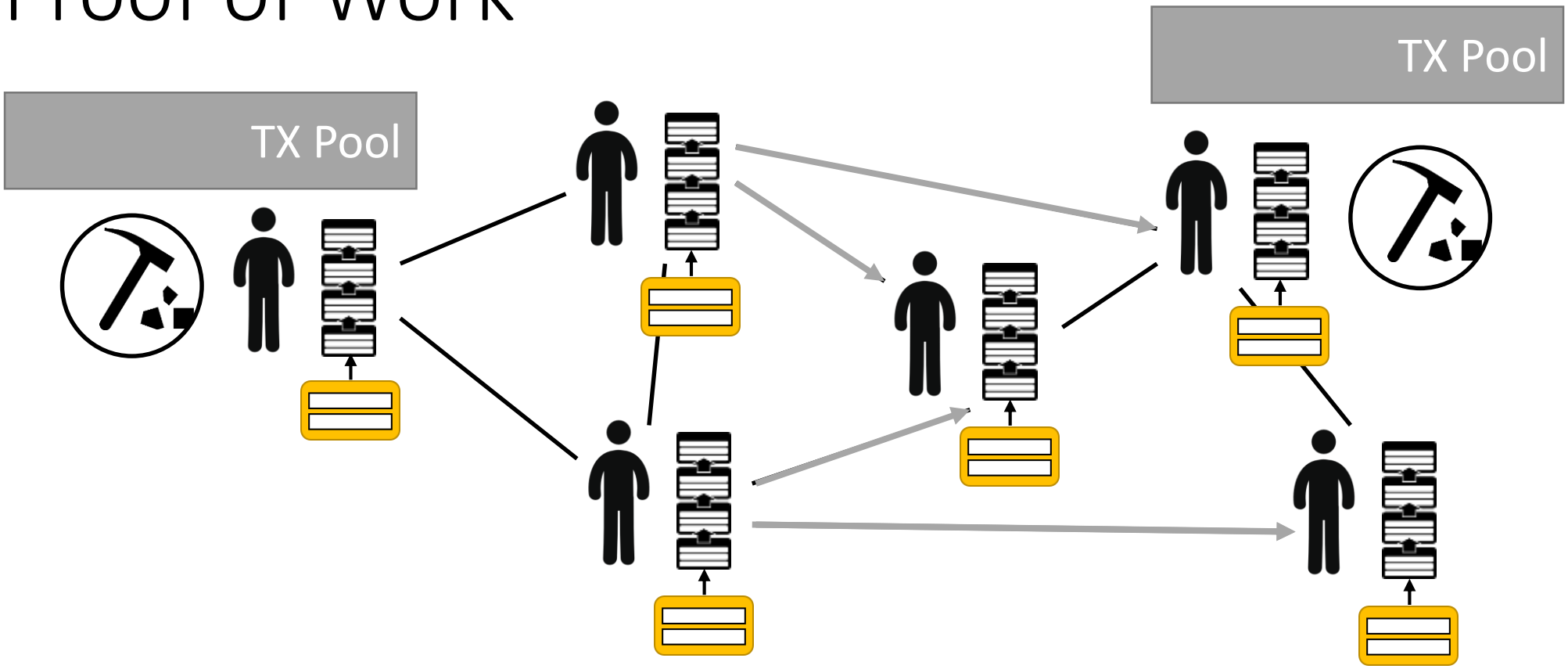
Proof of Work



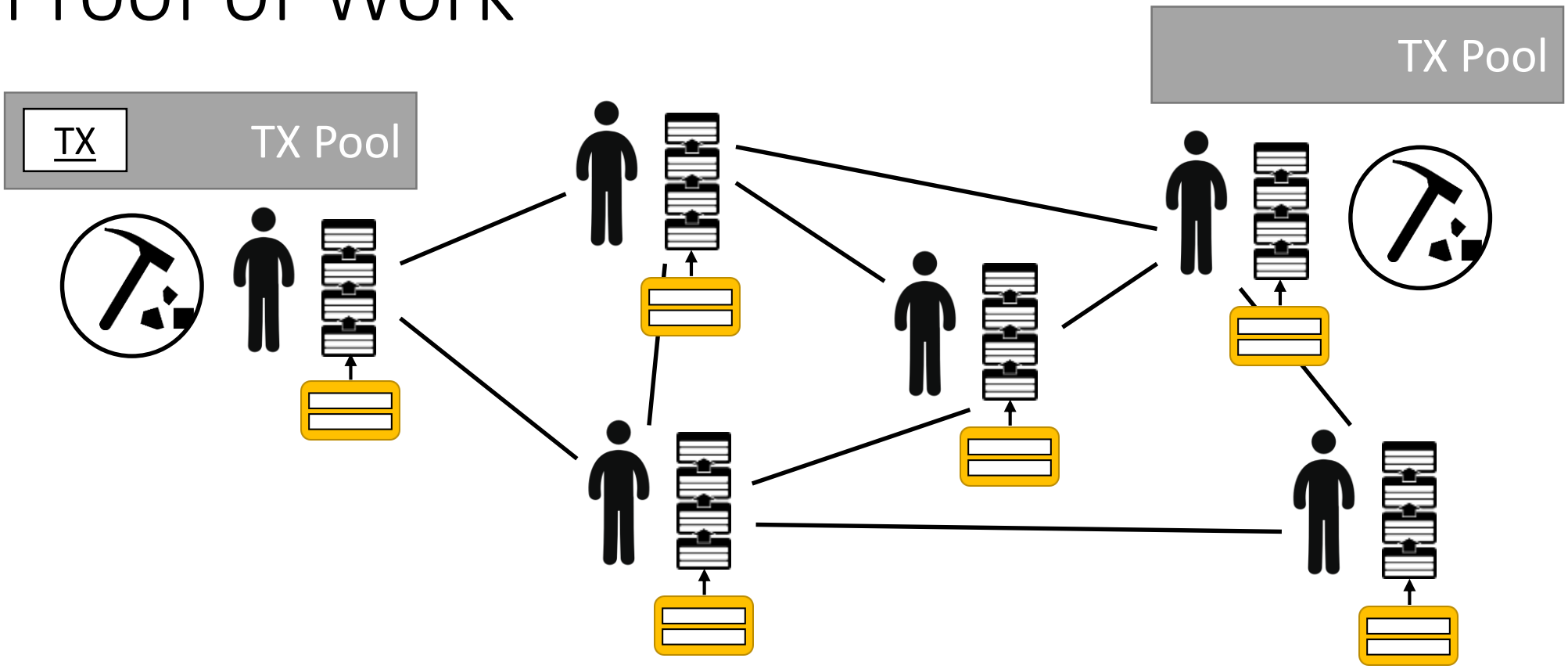
Proof of Work



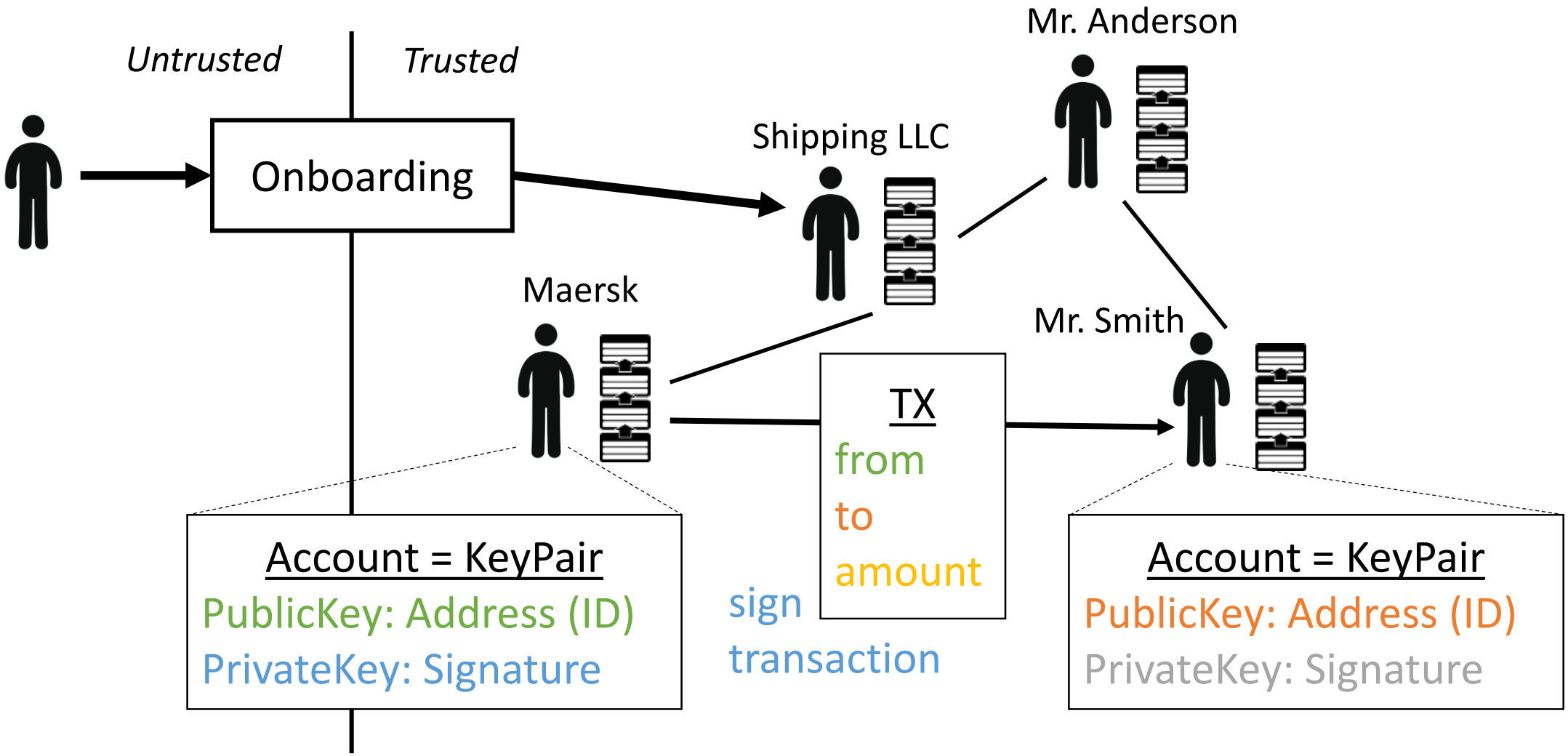
Proof of Work



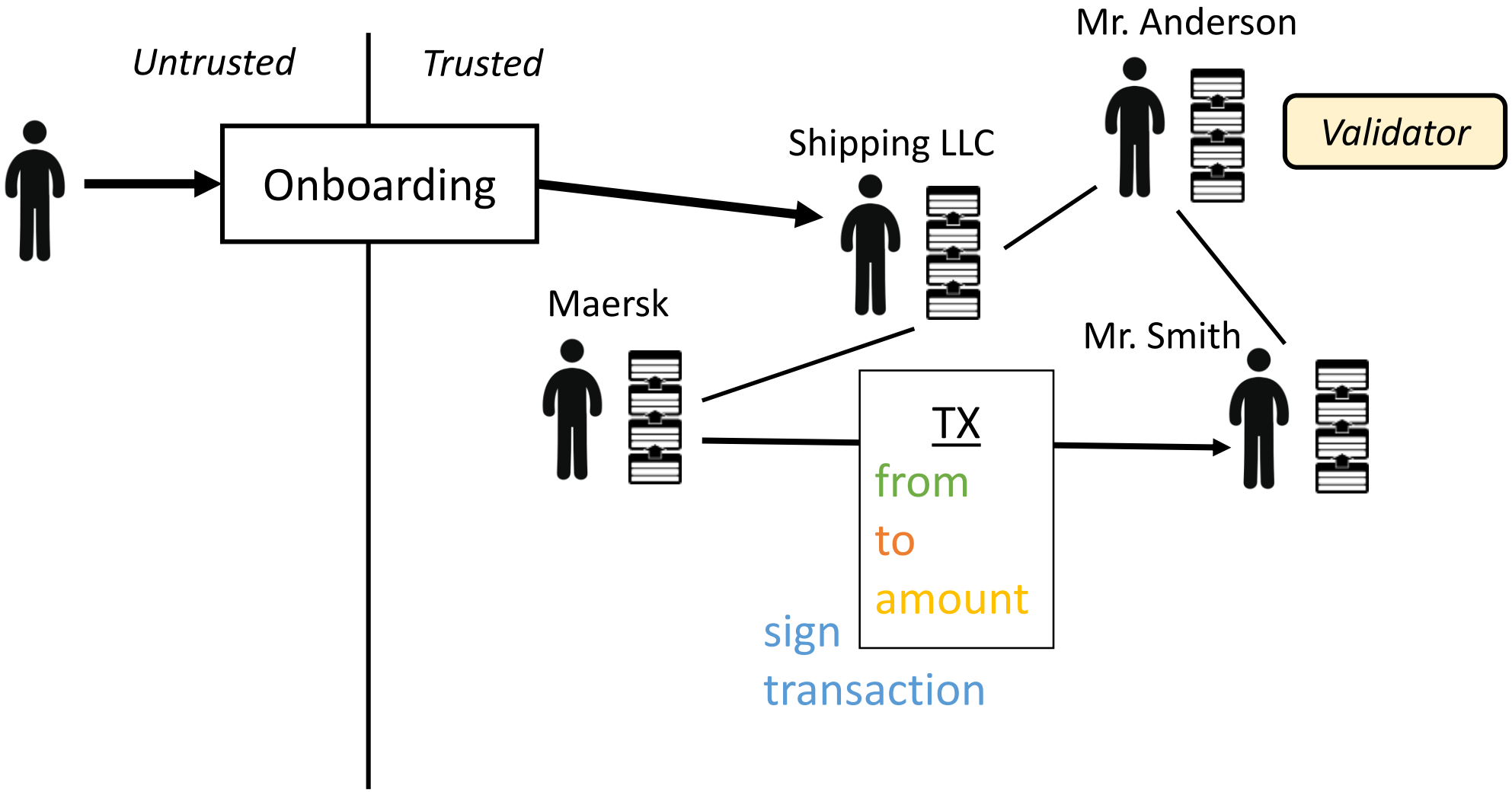
Proof of Work



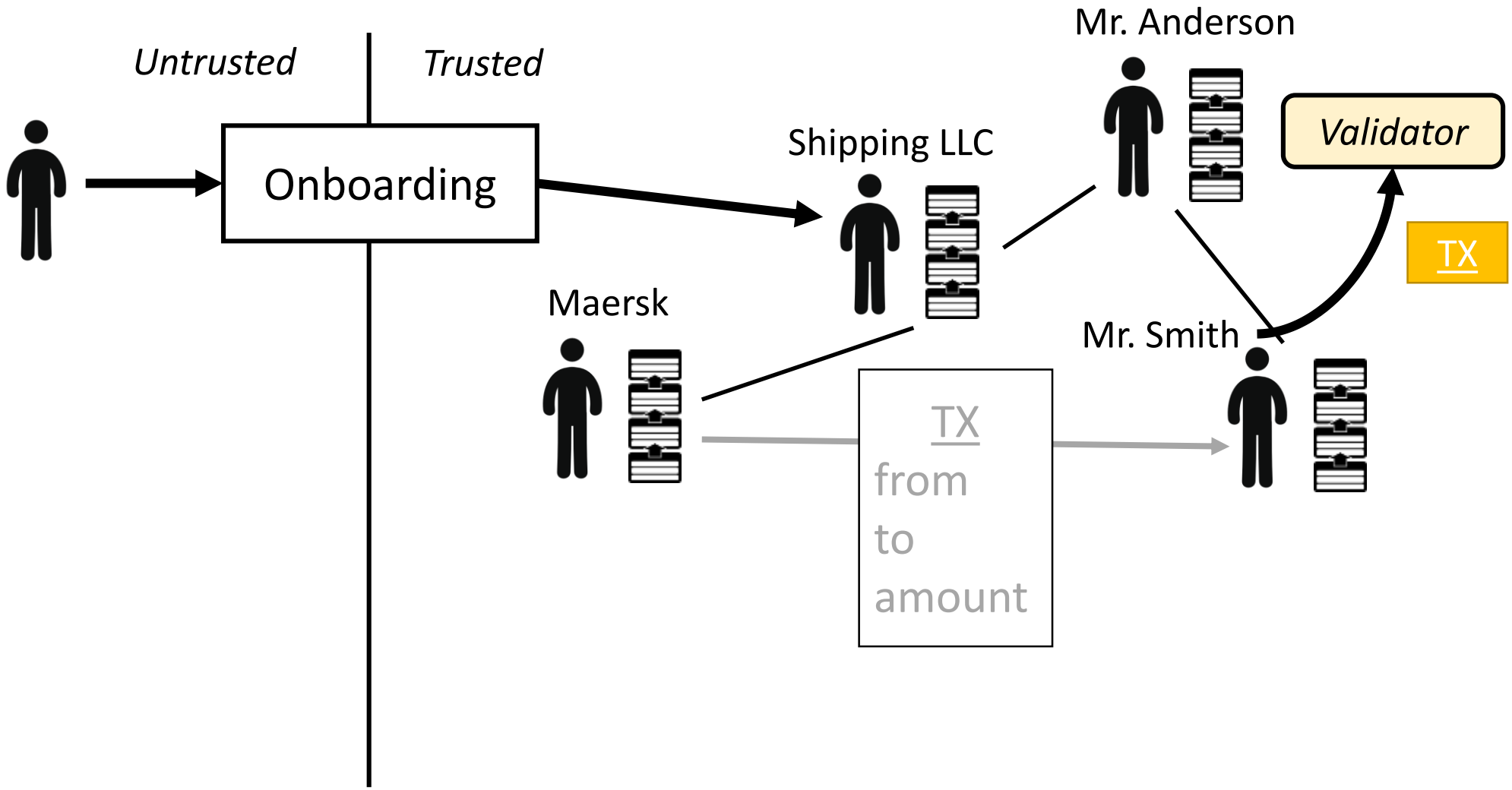
Identity in permissioned networks



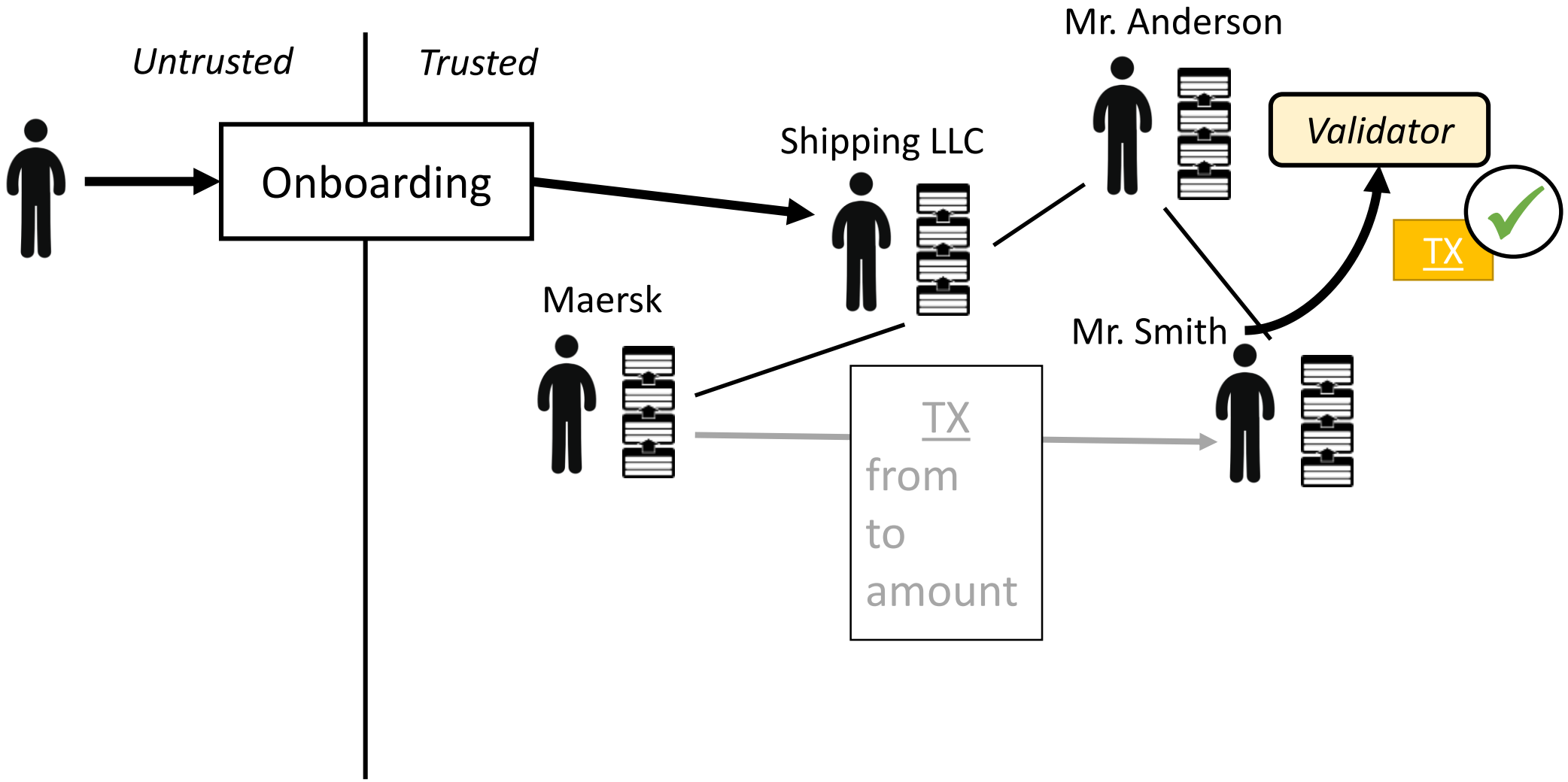
Proof of Authority



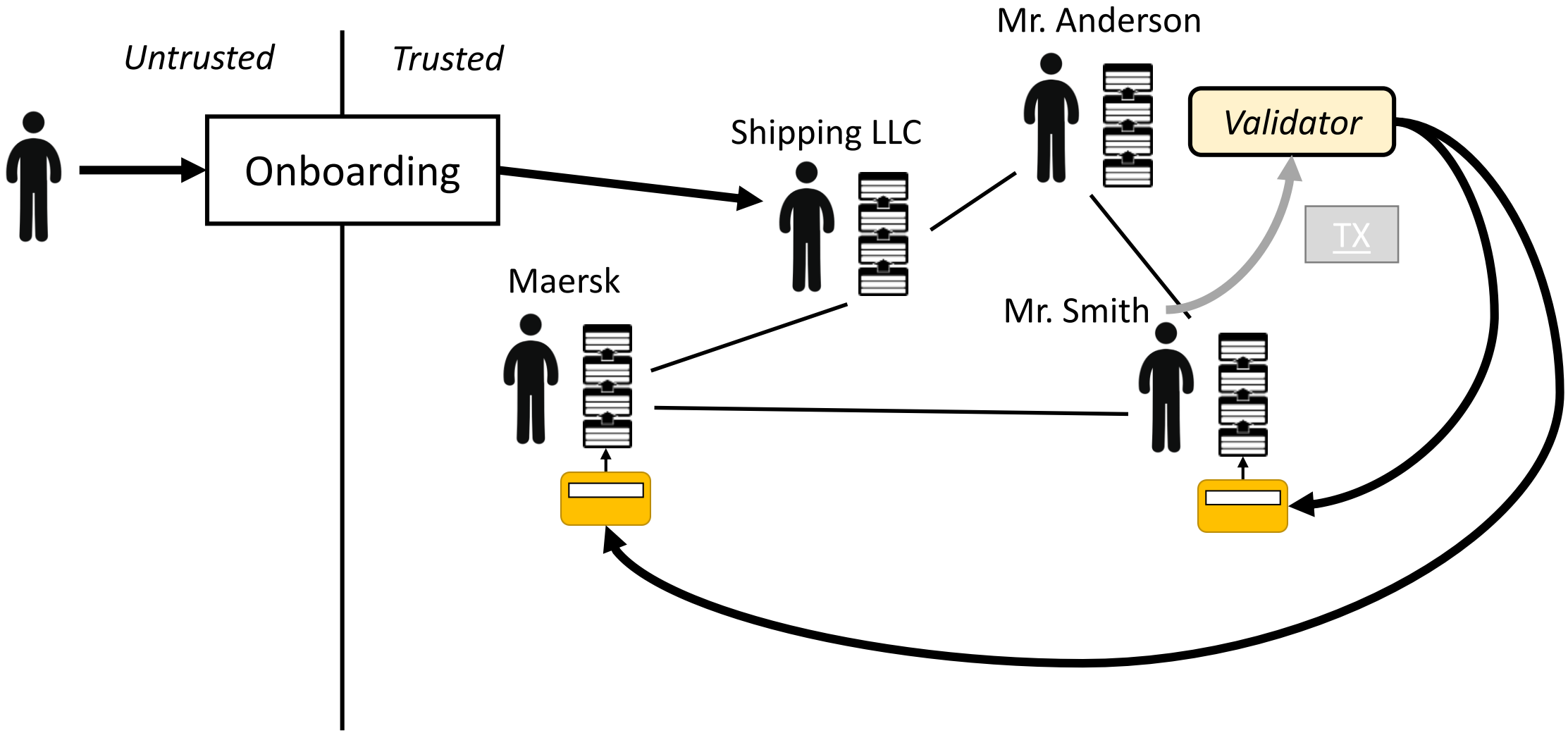
Proof of Authority



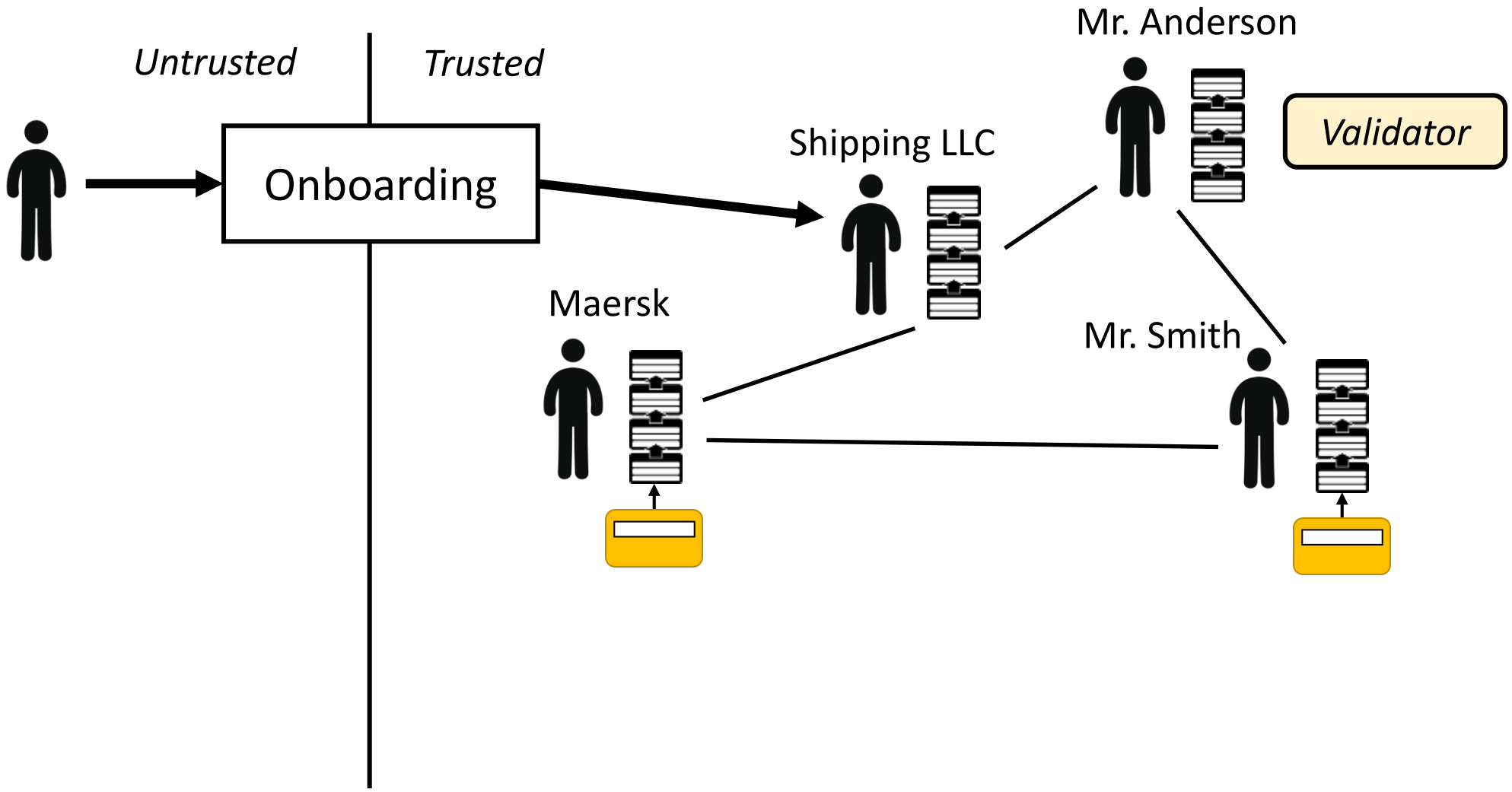
Proof of Authority



Proof of Authority



Proof of Authority



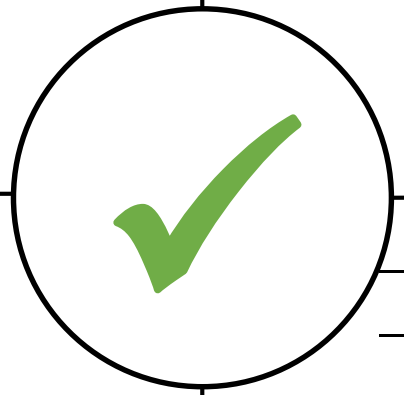
Proof of…

Proof of Work

- Solve a “cryptographic riddle” brute-force
- Difficult to solve – easy to validate (you can imagine a Sudoku)
- Solving takes time, recalculation is virtually impossible

Proof of Stake

- Choose a “truth giver” according to his “stake”
  - e.g. amount of cryptocurrency
  - Democratic …?



Proof of Elapsed Time

- Proof through special hardware
- Certification process for hardware owners
- Some selection process

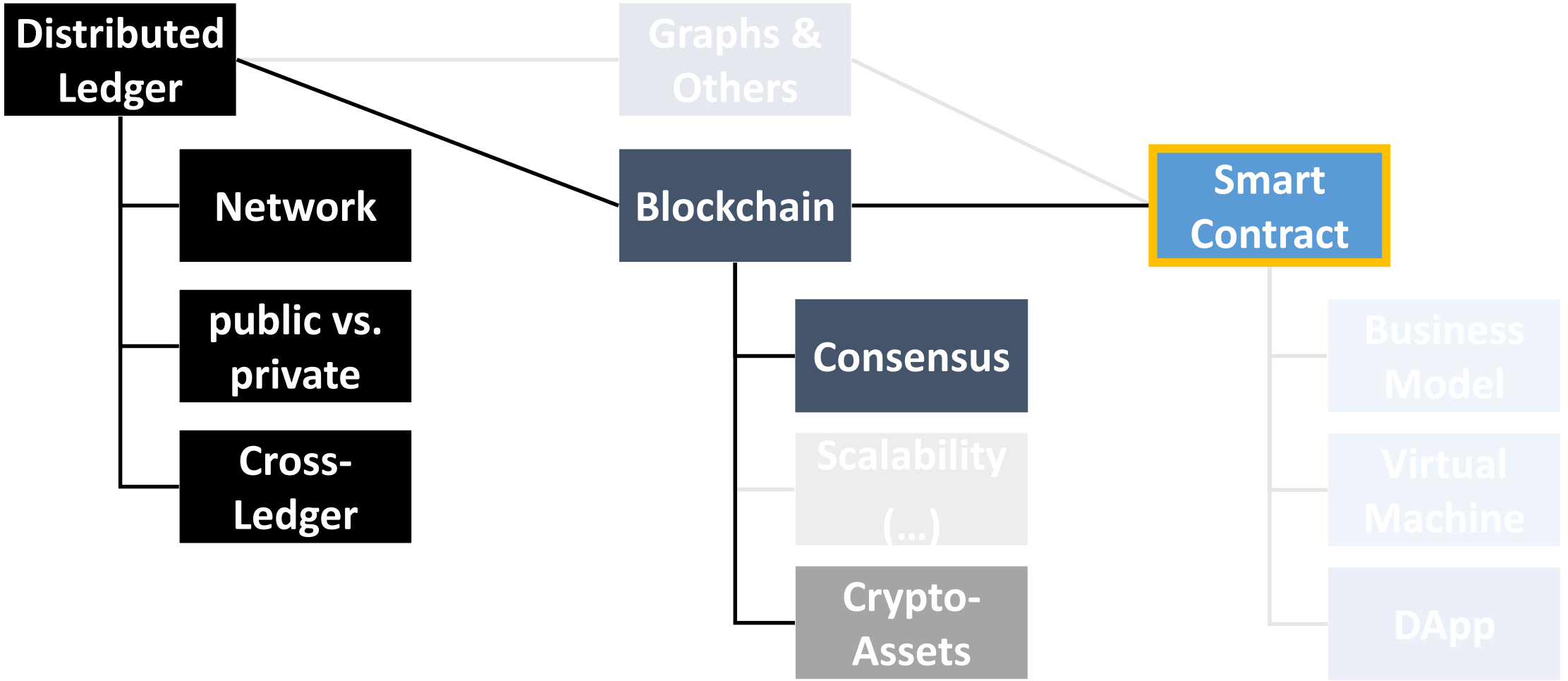
Proof of Authority

- Only certain nodes have assets
- They serve as “coin faucets”
- To get coins one has to reveal identity
- Used to secure test-networks

Smart Contracts

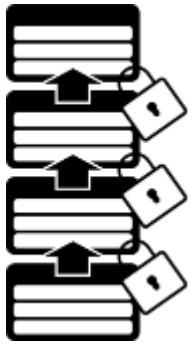
Smart Contract Overview (focus on Ethereum)

Let‘s focus on…



From Blockchain to Smart Contract Platform

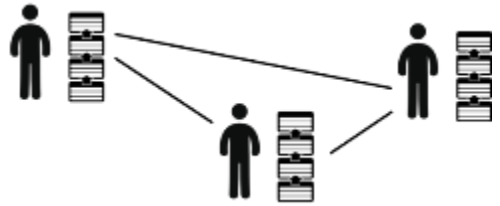
Cryptographic TRX list

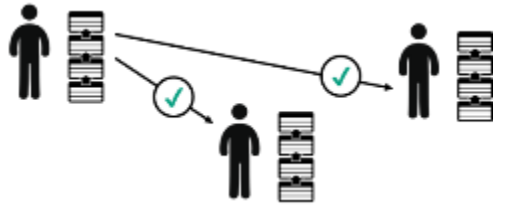


– Cryptographically secured ledger for the management of transactions and accounts

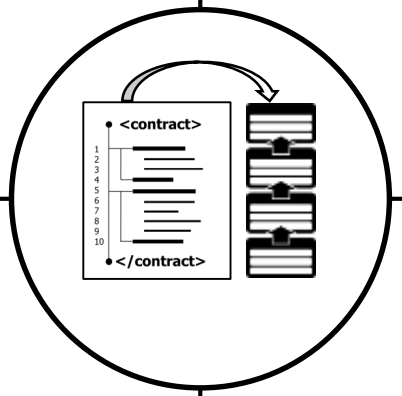
Peer-to-peer architecture

– Decentralized network of (equal) nodes





– Mechanism to agree on current state of system based on PO(…)

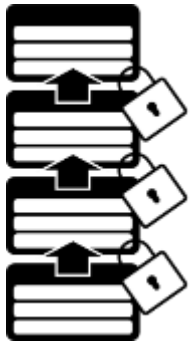


?

Consensus

From Blockchain to Smart Contract Platform

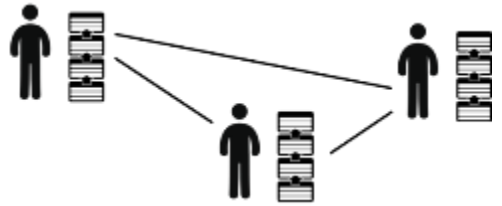
Cryptographic TRX list

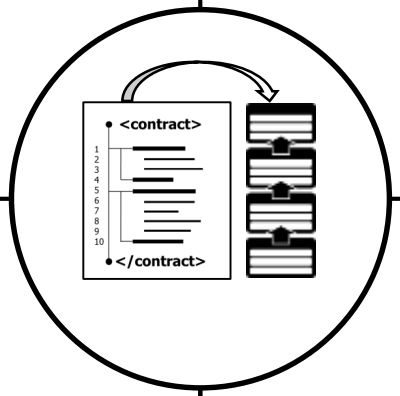


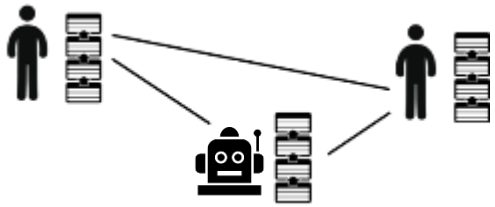
- Cryptographically secured ledger for the management of transactions and accounts

Peer-to-peer architecture

- Decentralized network of (equal) nodes

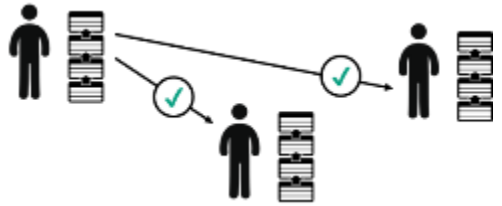






- Execute Smart Contract Bytecode
- Bytecode stored on Blockchain

Virtual Machine



- Mechanism to agree on current state of system based on PO(…)

Consensus

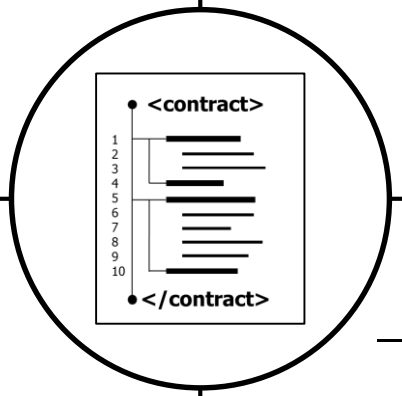
Smart Contracts in a Nutshell (Ethereum)

“Transaction Service-Interface”

- Put “data” on the “blockchain”
  State change through interface
- Interface: Methods & Parameters

Fairness and Transparency

- Contract Design → Fairness
- Bytecode openly available
- Every state change (data change) openly available



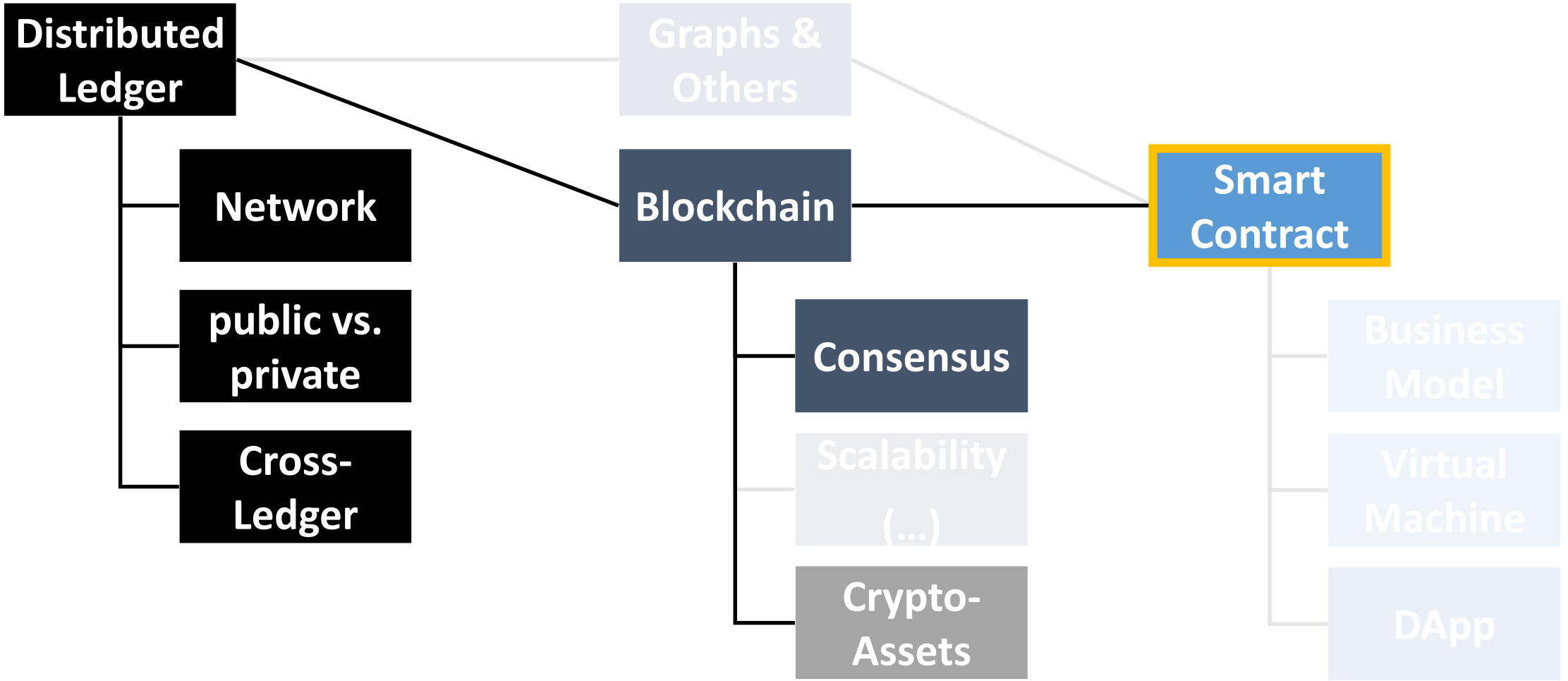
Contract Structure

- Definition of the contract
- Functionality of the contract
- Compare to: Class
- Bytecode on chain: Contract Creation
- No changes after creation

Contract State

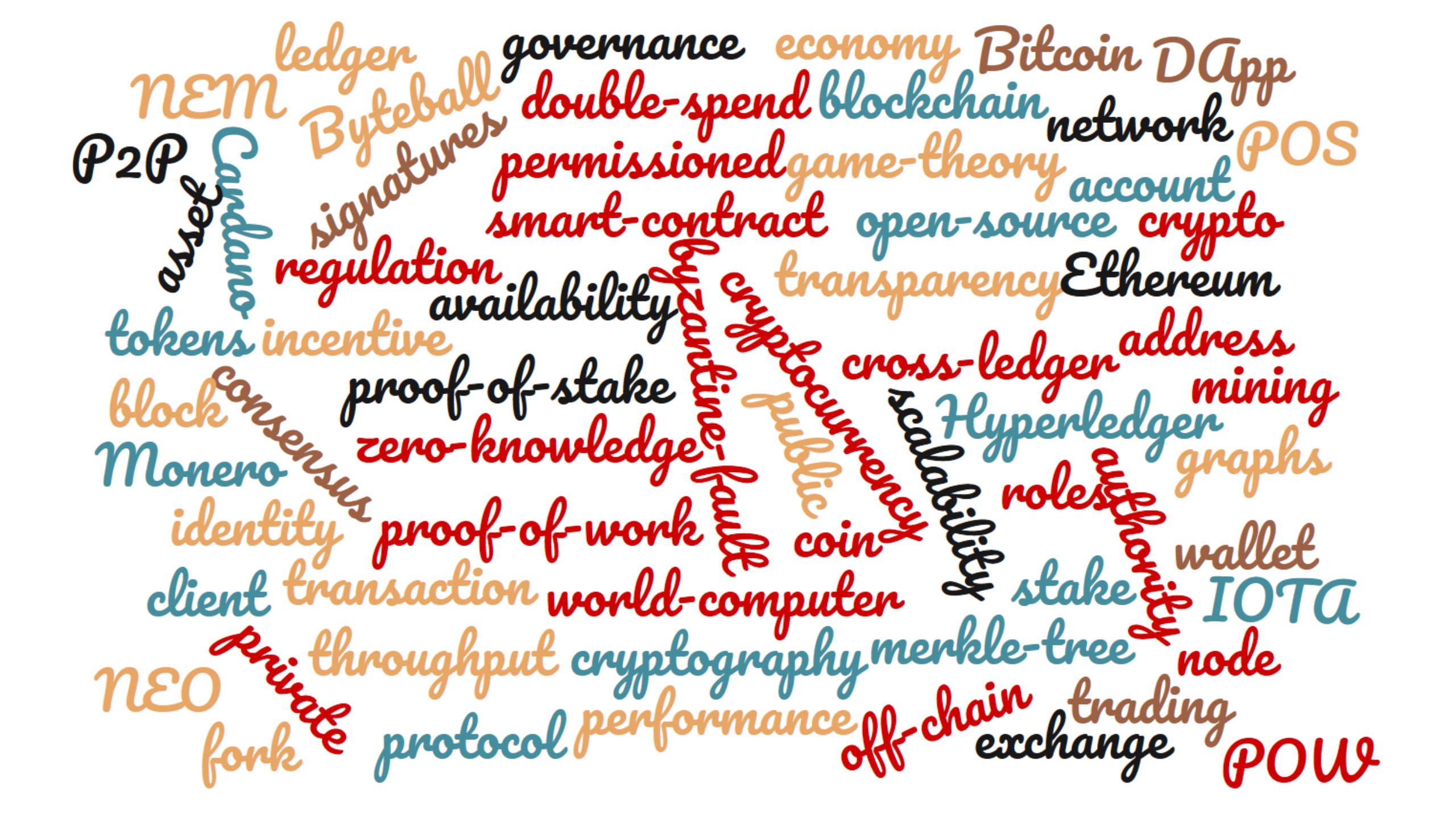
- Alter variable values within the contract through transactions
- After contract creation: Send TX to method at contract address

Let‘s focus on…



Didn‘t get Blockchain cards? Contact: eventmanagement@senacor.com

Just contact us via email or on our hompage www.senacor.com


governance
economy
Bitcoin
DApp
ledger
NEM
Byteball
double-spend
blockchain
network
POS
signatures
P2P
permissioned
game-theory
account
asset
Cardano
smart-contract
open-source
crypto
regulation
transparency
Ethereum
availability
byzantine-fault
cryptocurrency
tokens
incentive
address
cross-ledger
proof-of-stake
mining
block
consensus
public
scalability
Hyperledger
zero-knowledge
graphs
Monero
roles
authority
identity
proof-of-work
coin
wallet
client
transaction
world-computer
stake
IOTA
throughput
cryptography
merkle-tree
node
private
NEO
fork
protocol
performance
off-chain
trading
exchange
POW