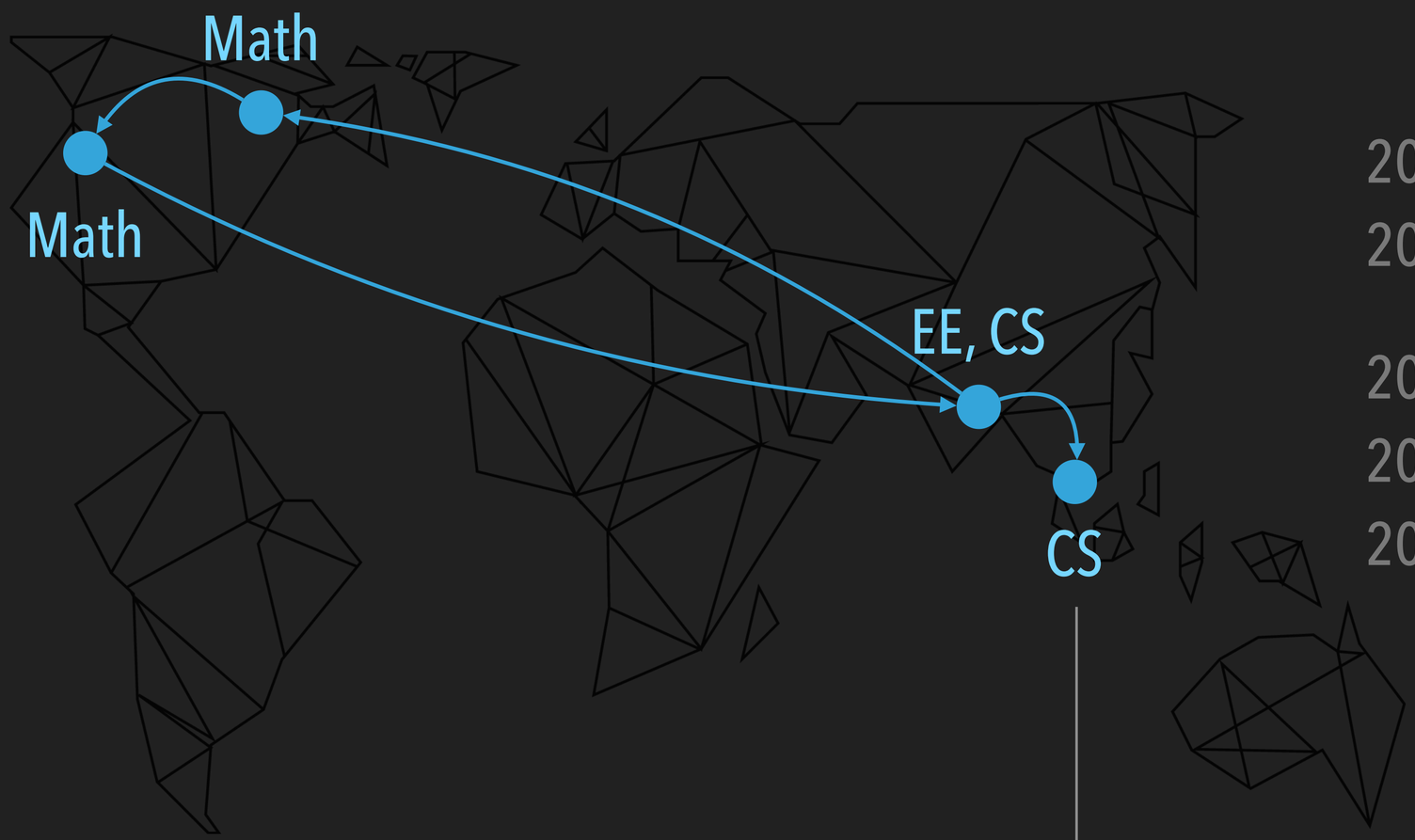
Bitcoin and Beyond

The World of Crypto–Currencies



2018 to date	Lecturer, NTU, Singapore
2014 - 2017	Lecturer, ISI Kolkata, India
2010 - 2014	PhD, Computer Science
2006 - 2008	MMath, Pure Mathematics
2002 - 2006	BTech, Electronics Engg.

I teach Data Science and Machine Learning
My research interests are in Cybersecurity
I study all technical aspects of Blockchain

Sourav Sen Gupta

Lecturer, SCSE, NTU Singapore

sg.sourav@ntu.edu.sg


24 HOUR LOW
$11,774.17
24 HOUR HIGH
$11,939.43
ALL TIME HIGH
$19,665.39
CIRCULATING SUPPLY
18.46M
AVERAGE TRANSACTION FEE (24H)
$2.52
VALUE TRANSACTED (24H)
$1.88B
$15000
$10000
$5000
2014
2016
2018
2020
coindesk

Silk Road

anonymous marketplace

Welcome **OzFreelancer**!

messages(0) | orders(0) | account(฿0.00) | settings | log out

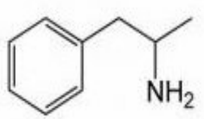
search | (0)

Shop by category:

- Drugs(1582)
  - Cannabis(271)
  - Dissociatives(33)
  - Ecstasy(217)
  - Opioids(106)
  - Other(65)
  - Prescription(274)
  - Psychedelics(306)
  - Stimulants(190)
- Apparel(37)
- Art(1)
- Books(300)
- Computer equipment(9)
- Digital goods(218)
- Drug paraphernalia(33)
- Electronics(13)
- Erotica(165)
- Fireworks(1)
- Food(1)
- Forgeries(34)
- Hardware(1)
- Home & Garden(5)
- Lab Supplies(5)
- Medical(3)
- Money(89)
- Musical

10 Grams high grade MDMA 80+%

฿61.17



Amphetamines sulfate / Speed freebase...

฿28.59

2g Jack Frost (weed) *420 SALE****

฿8.54

CENTRINO LABS Test Enanthate 250mg/ml - 10ml

$203.94

30x (VIAGRA) Sildenafil SOFT CAPSULES

$103.81

1 x Blue Rockstar

$7.61

G-13 Potpourri - 10g - 5FPB22 - Ships Free!

$50.01

5 Grams of pure MDMA crystals

฿42.04

100 red Y tablets 111mg (lab tested)...

฿97.77

Michael Jackson Discography 1971-2009...

฿2.52

[1] Expertly Handrolled MASSIVE AAA Organic

$25.00

Generic Cialis 20mg (Tadalafil) 100mg

$86.06

DMT (NN-DMT) 10.0g

$1,437.50

20G B Grade Afghan Heroin (Brown Powder)#2 Quality

$850.61

3.5g Albino Rhino (weed)

฿12.37

10mg Flexeril (muscle relaxant)...

฿3.22

***10gr. Amphetamine Sulphate...

฿33.19

1 gram ✖ Moroccan Hash ✖ DUTCH QUALITY

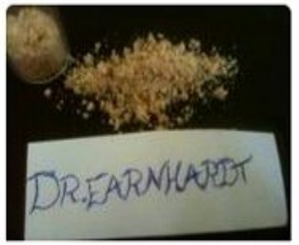
$7.47

2C-E 25g (powder)

$849.57

50G Pure Indian Ketamine Crystal | UK | BULK

$868.23



(' white/gold DMT 100 mg HQ

$13.50

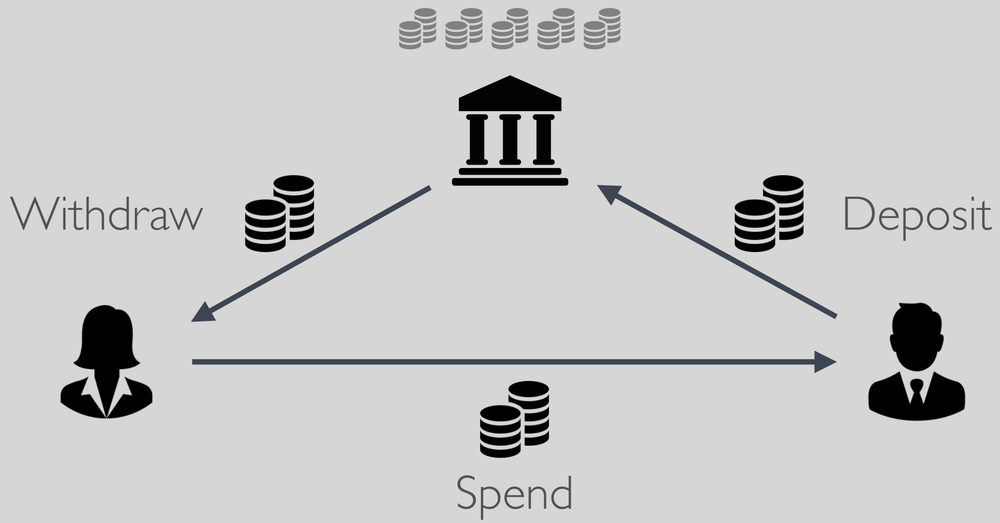
Arise, you have nothing to lose

but your barbed wire fences!

Currency

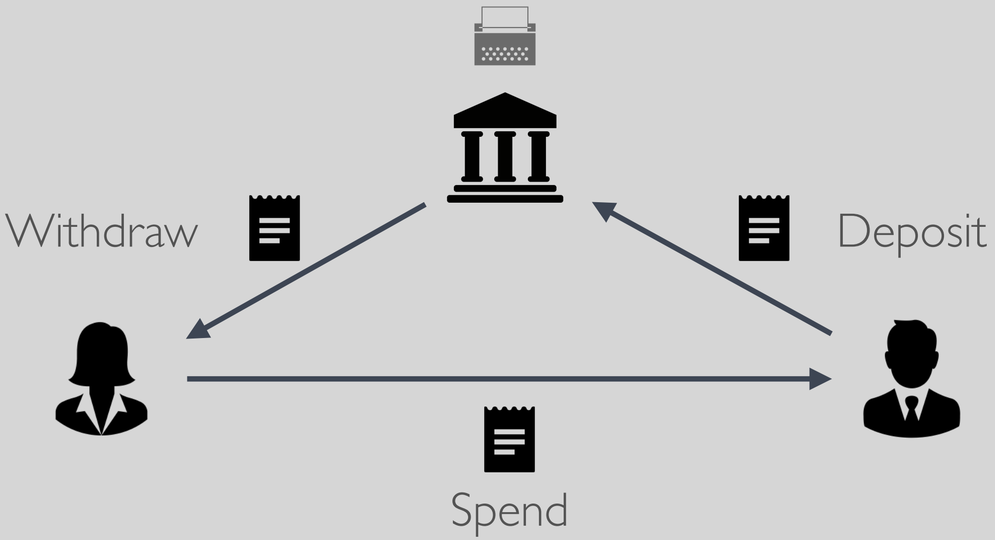
cur·ren·cy *noun*

Medium of Exchange



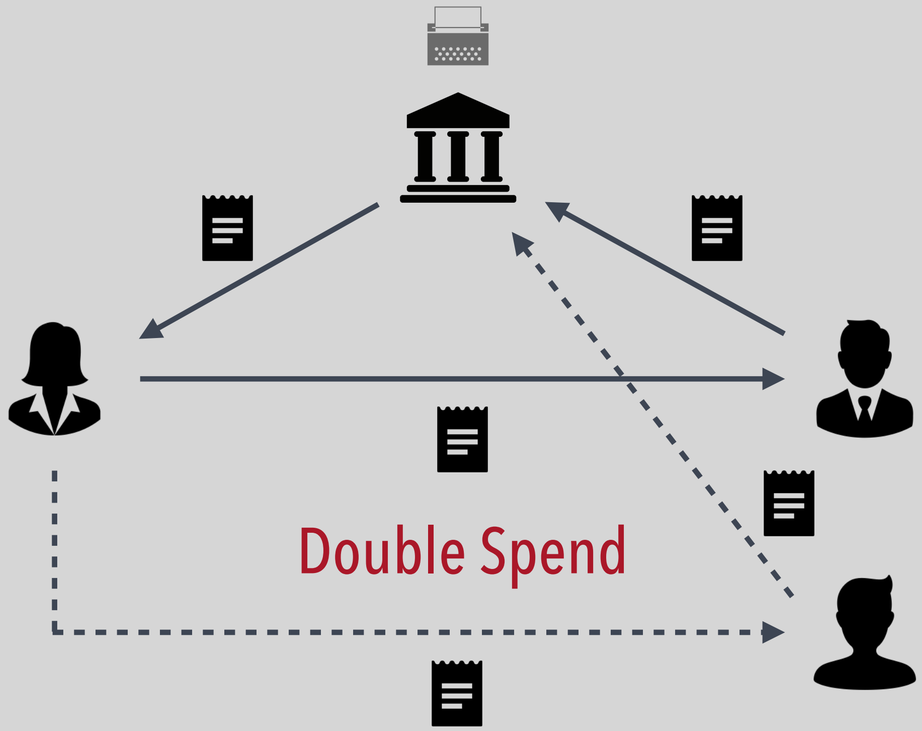
Centralized Accounting for some Two-Party Transaction

cur·ren·cy *noun*



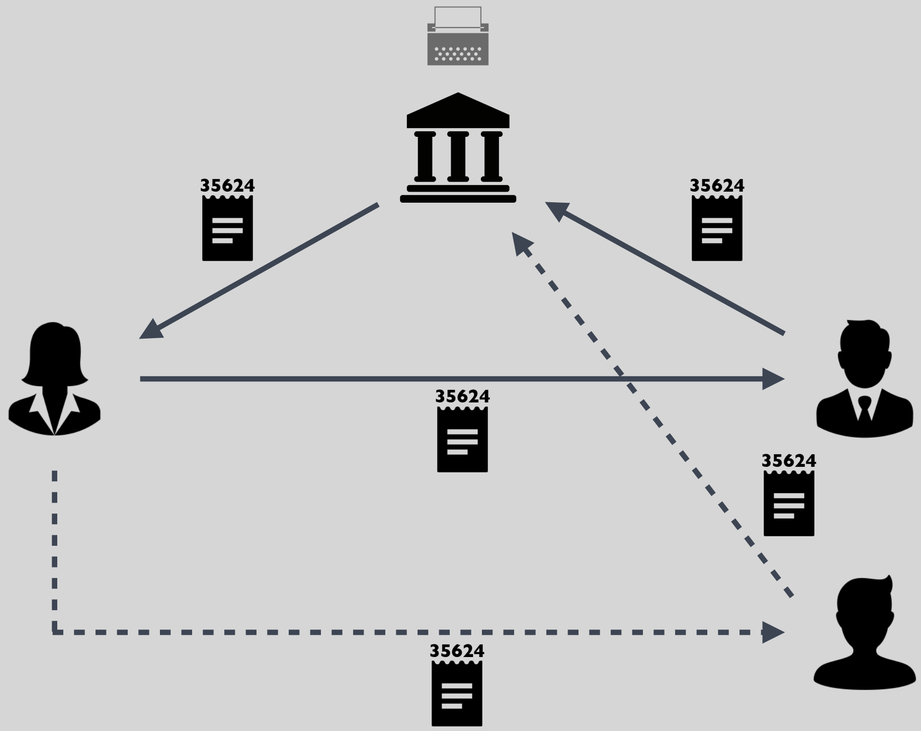
Digital Representation of
the Two-Party Transaction

digital currency



digital currency

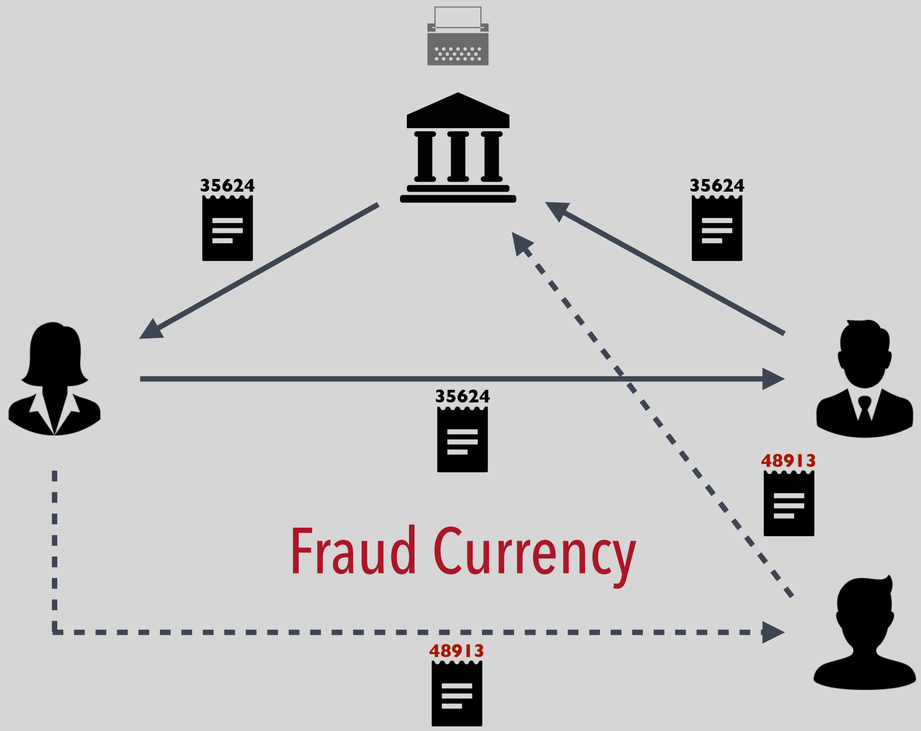
Digital Representation of money can be Duplicated



digital currency

Digital Representation with

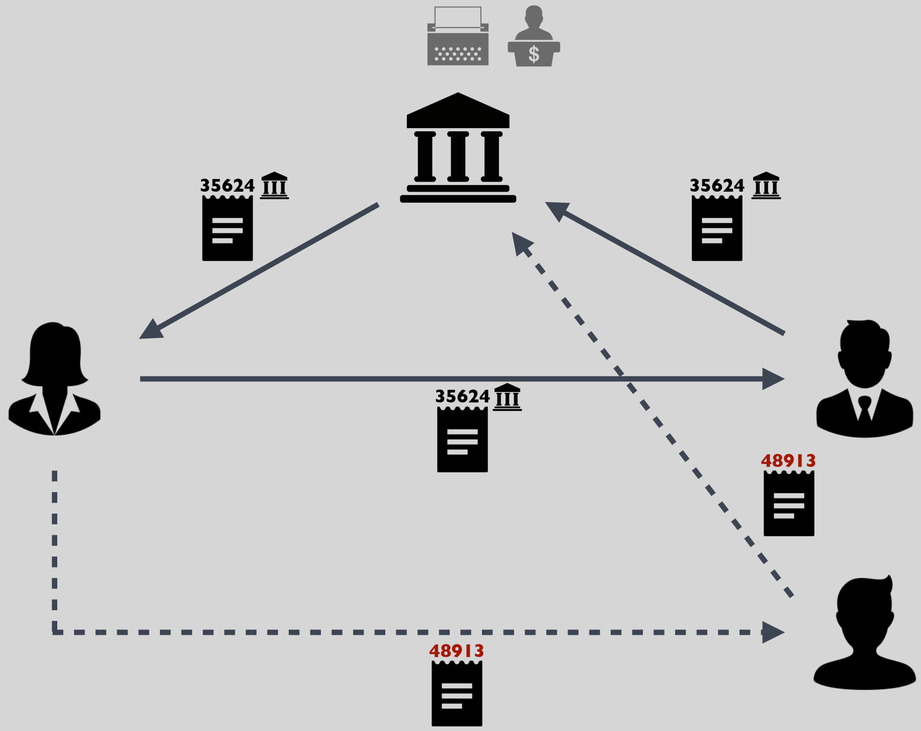
Unique Identifier for safety



digital currency

Digital Representation with

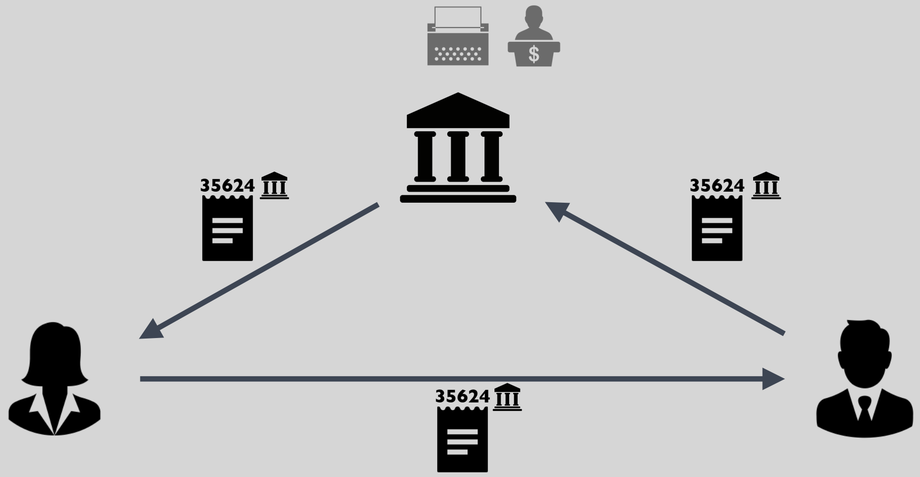
Fraudulent Identifier



digital currency

Digital Representation with

Authenticated Identifier



Digital Representation of
the no Individual Privacy

digital currency

Blind Signature

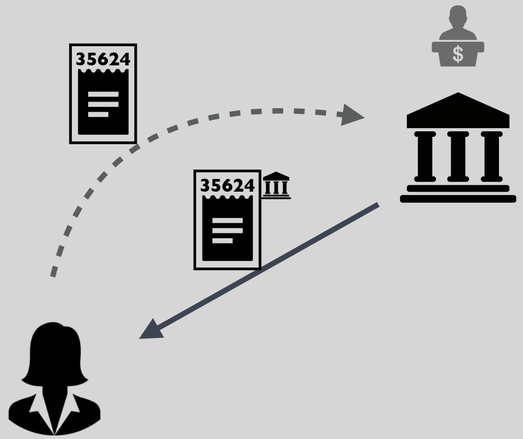
David Schaum, 1984

On the one hand, knowledge by a third party of the payee, amount, and time of payment for every transaction made by an individual can reveal a great deal about the individual's whereabouts, associations and lifestyle. For example, consider payments for such things as transportation, hotels, restaurants, movies, theater, lectures, food, pharmaceuticals, alcohol, books, periodicals, dues, religious and political contributions.

On the other hand, an anonymous payments systems like bank notes and coins suffers from lack of controls and security. For example, consider problems such as lack of proof of payment, theft of payments media, and black payments for bribes, tax evasion, and black markets.

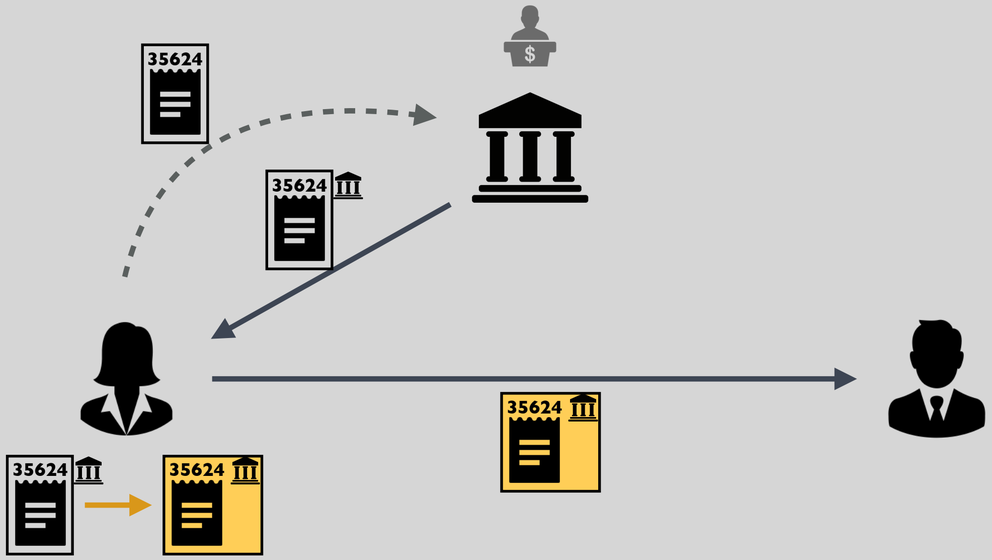
The concept of Untraceable
e-Payments and e-Cash

anonymous digital currency



Commitment for e-Cash
authorized by Blind Sign

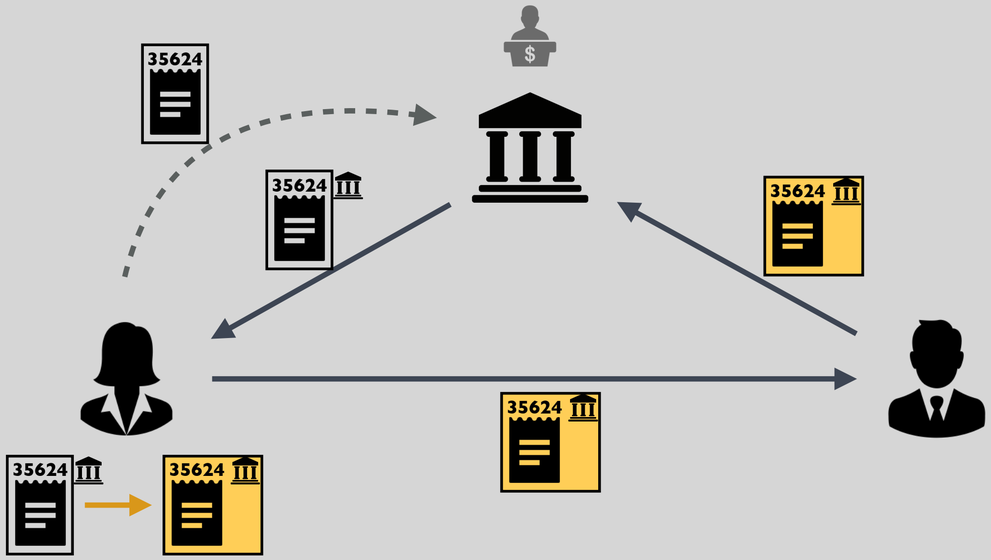
anonymous digital currency



Commitment verified by

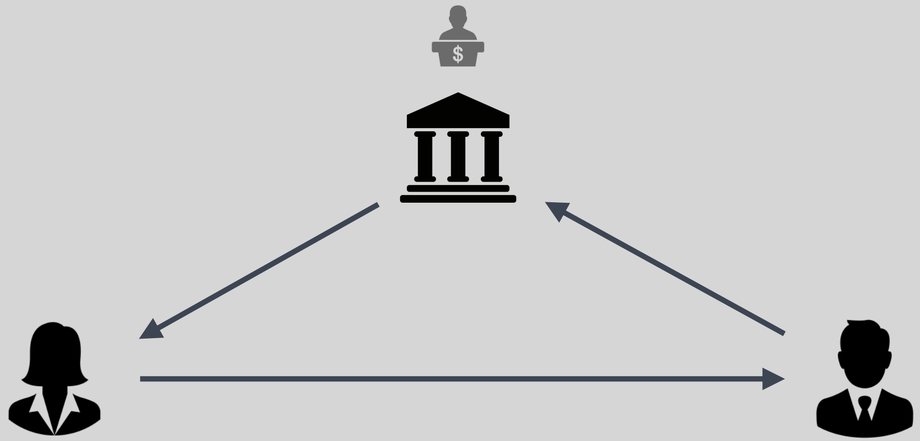
Zero-Knowledge Proof

anonymous digital currency



Blind Signature and
Zero-Knowledge Proof

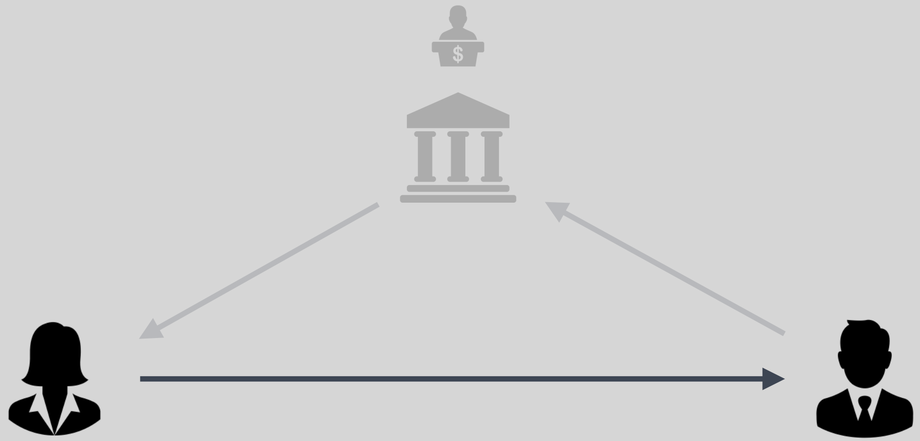
anonymous digital currency



Commitment + Encryption
+ Blind Signature

connected by Zero-Knowledge Proof

anonymous digital currency



anyone?

What if anonymity is not enough, and you want to Decentralize the Currency?

decentralized digital currency

CypherPunks

Phil Zimmermann

PGP

1991

Adam Back

HashCash

1997

Wei Dai

B-Money

1998

Nick Szabo

BitGold

1998

Hal Finney

RPoW

2004

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

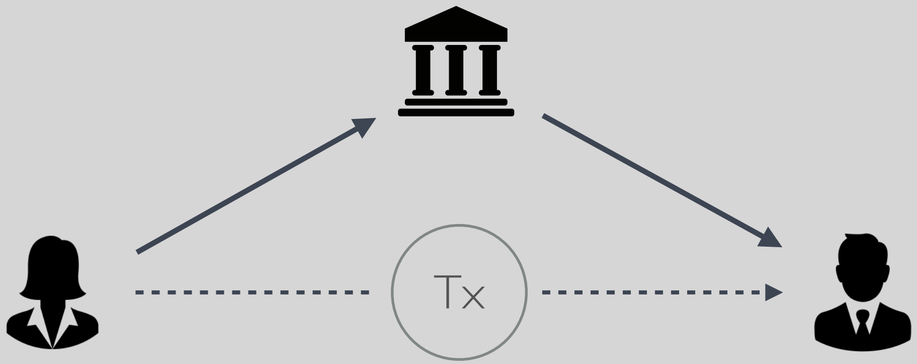
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Bitcoin

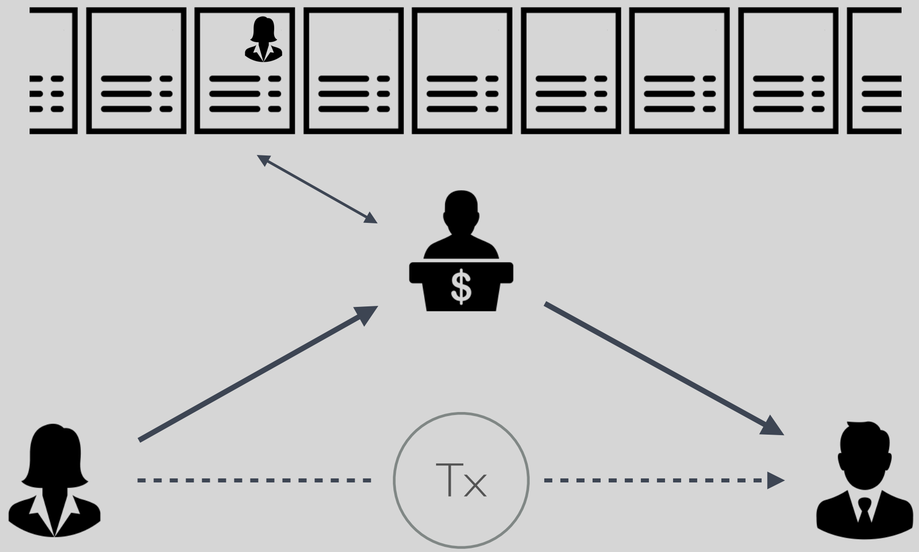
Satoshi Nakamoto

31 October 2008



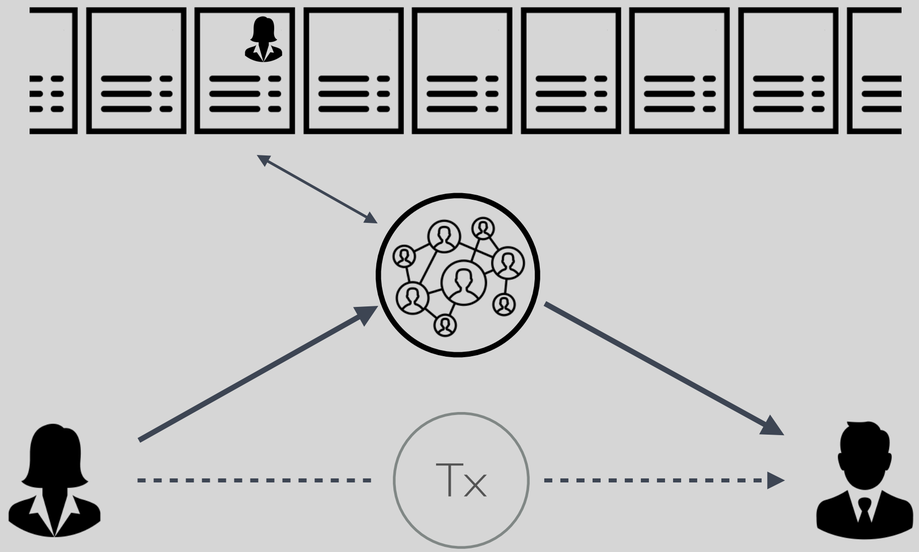
Centralized Transaction as
we are all familiar with

not Bitcoin



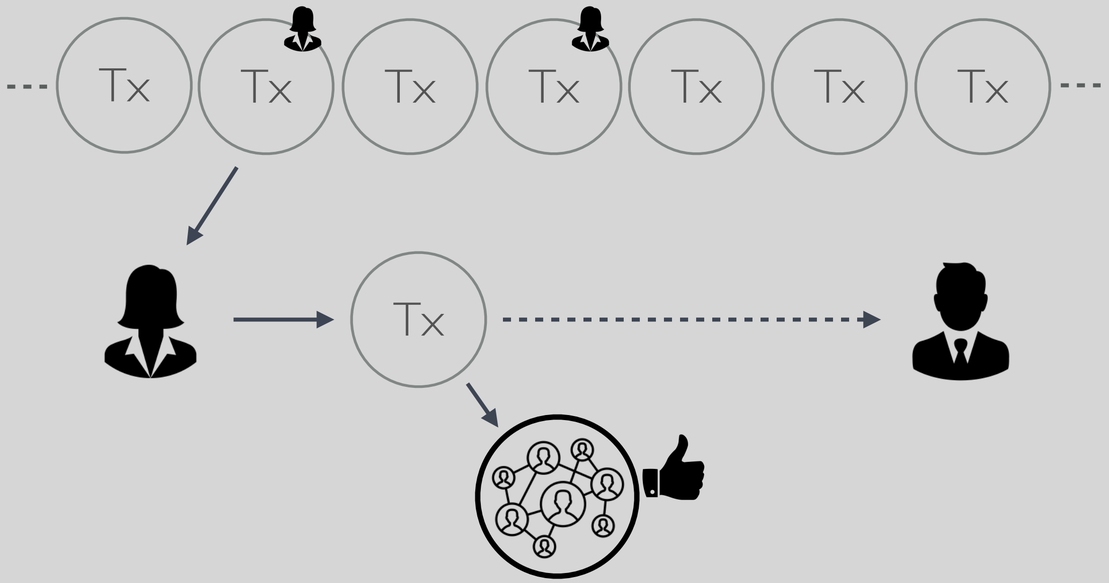
Centralized Transaction based on a Centralized Account-based Ledger

not Bitcoin



Decentralized Transaction based on a Decentralized Account-based Ledger

not Bitcoin yet

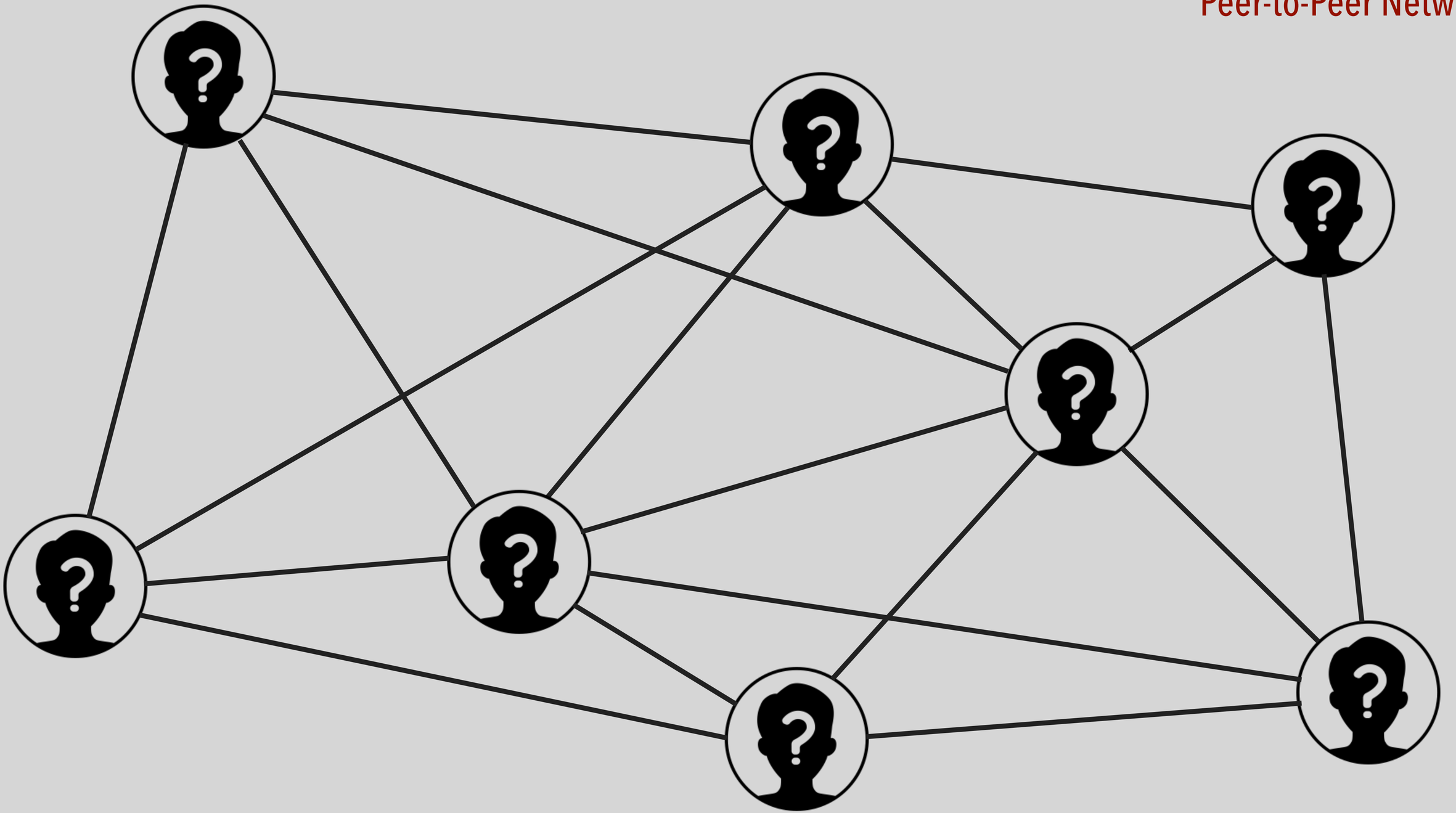


almost there …

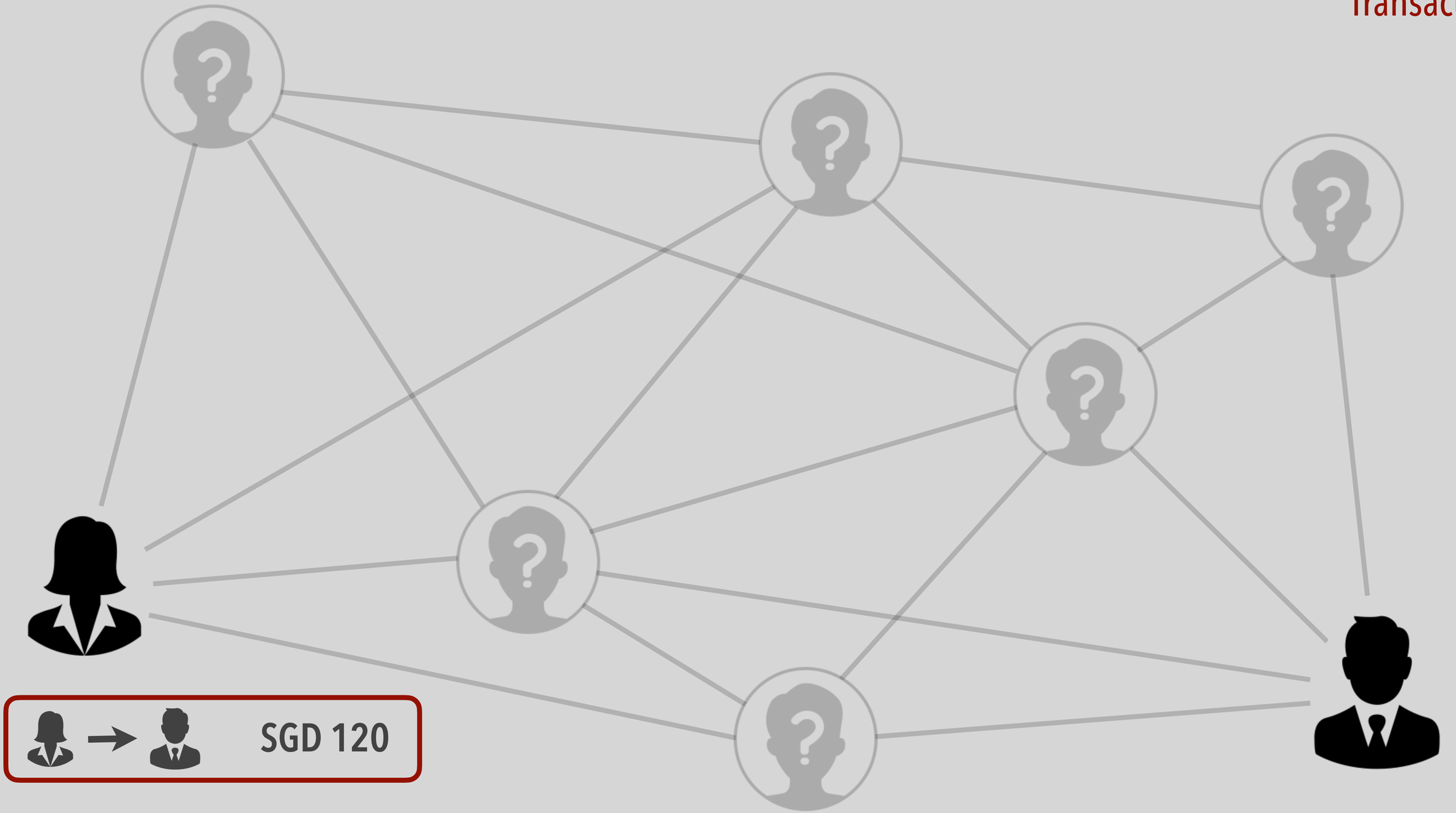
Decentralized Transaction based on a Decentralized Transaction-based Ledger

Transaction

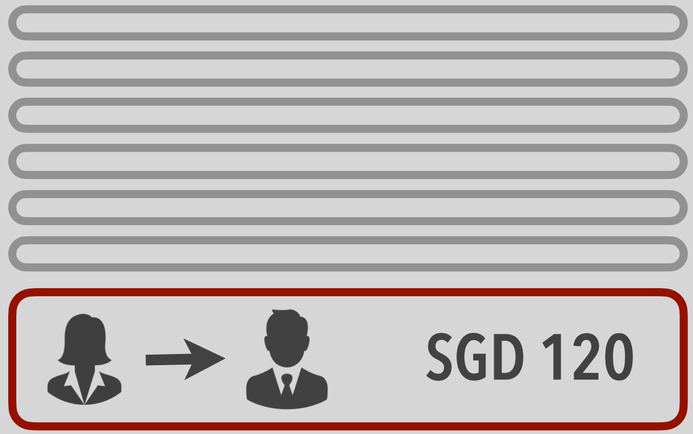
Peer-to-Peer Network

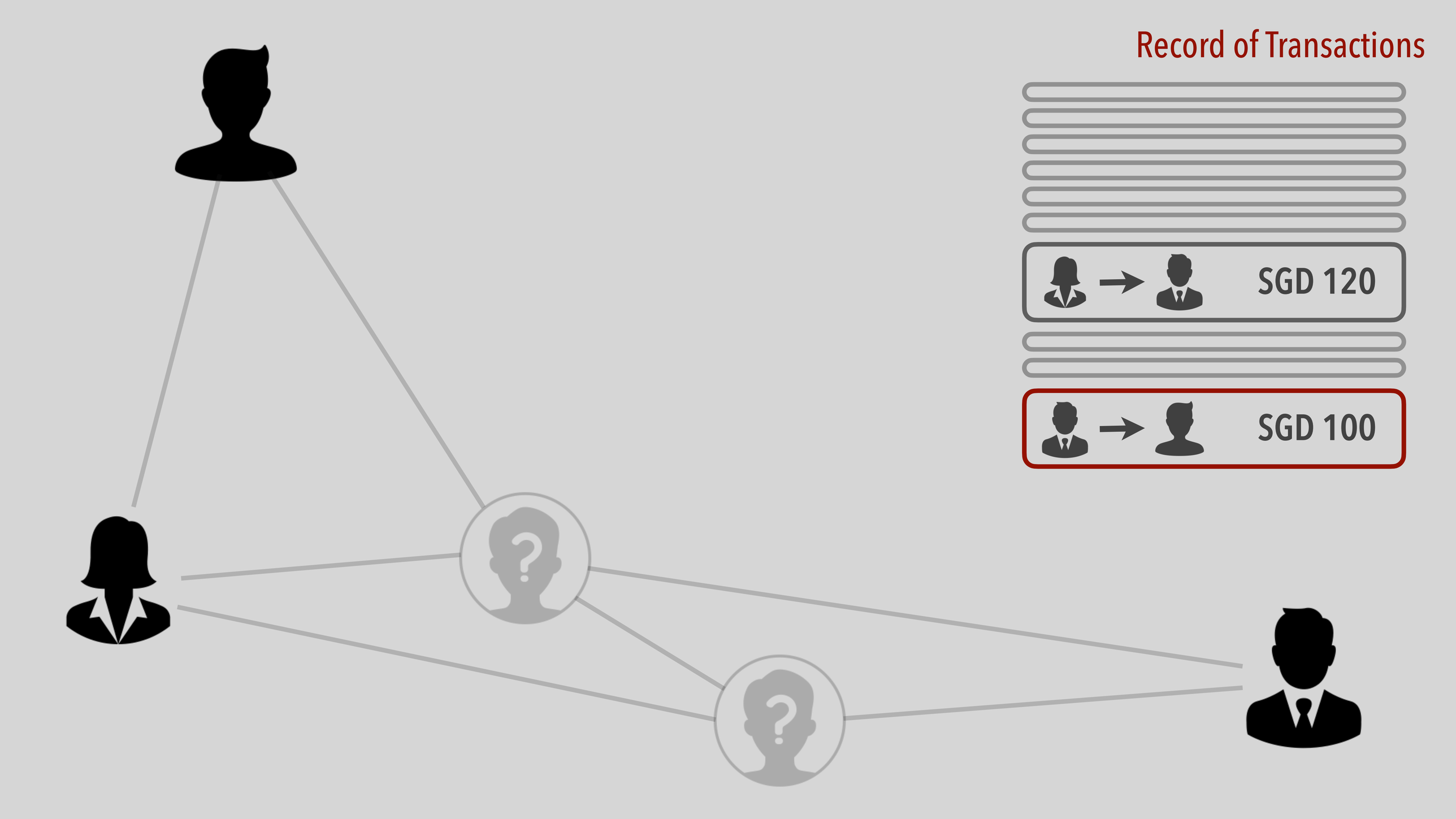


Transaction

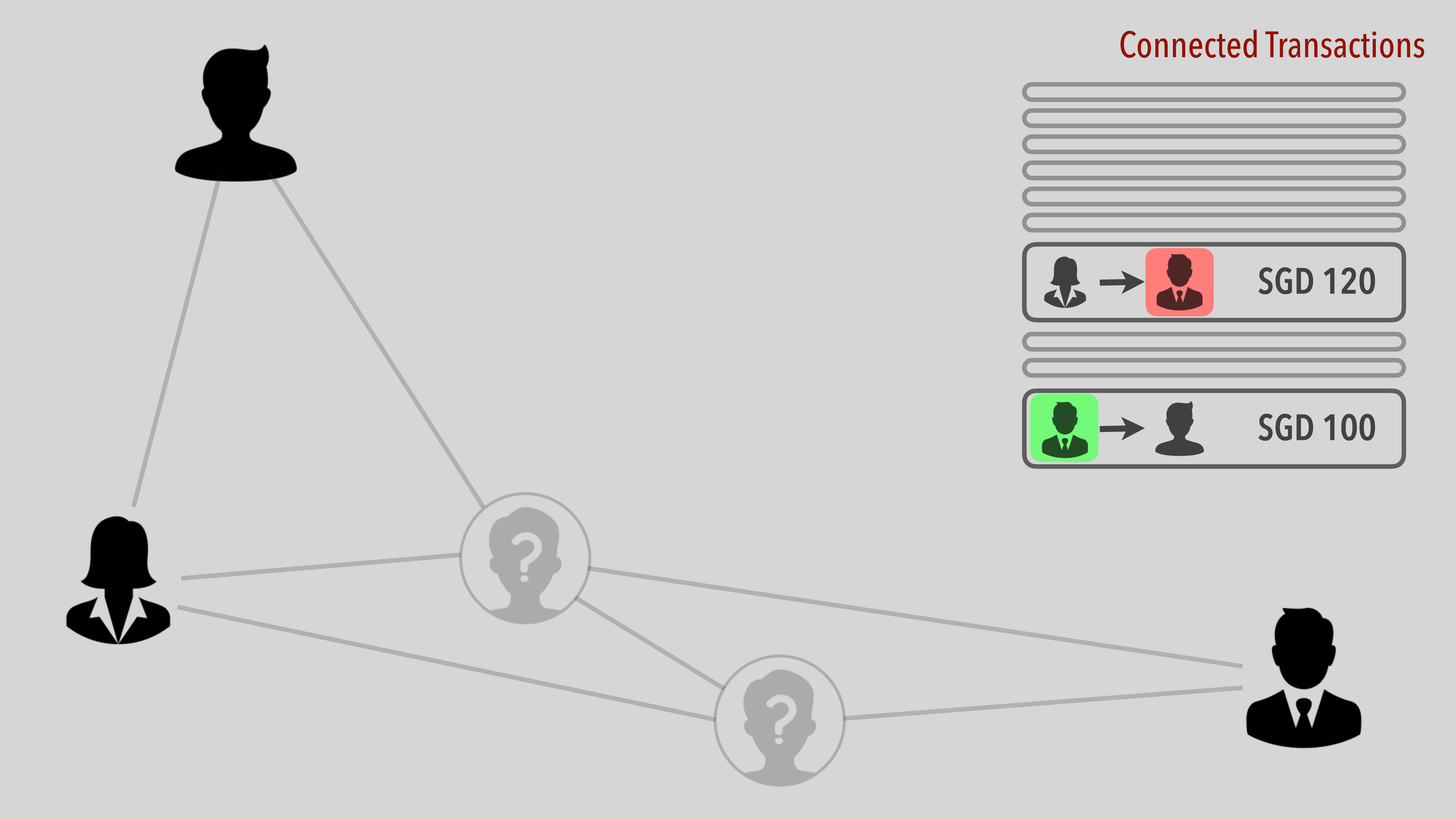


Record of Transactions

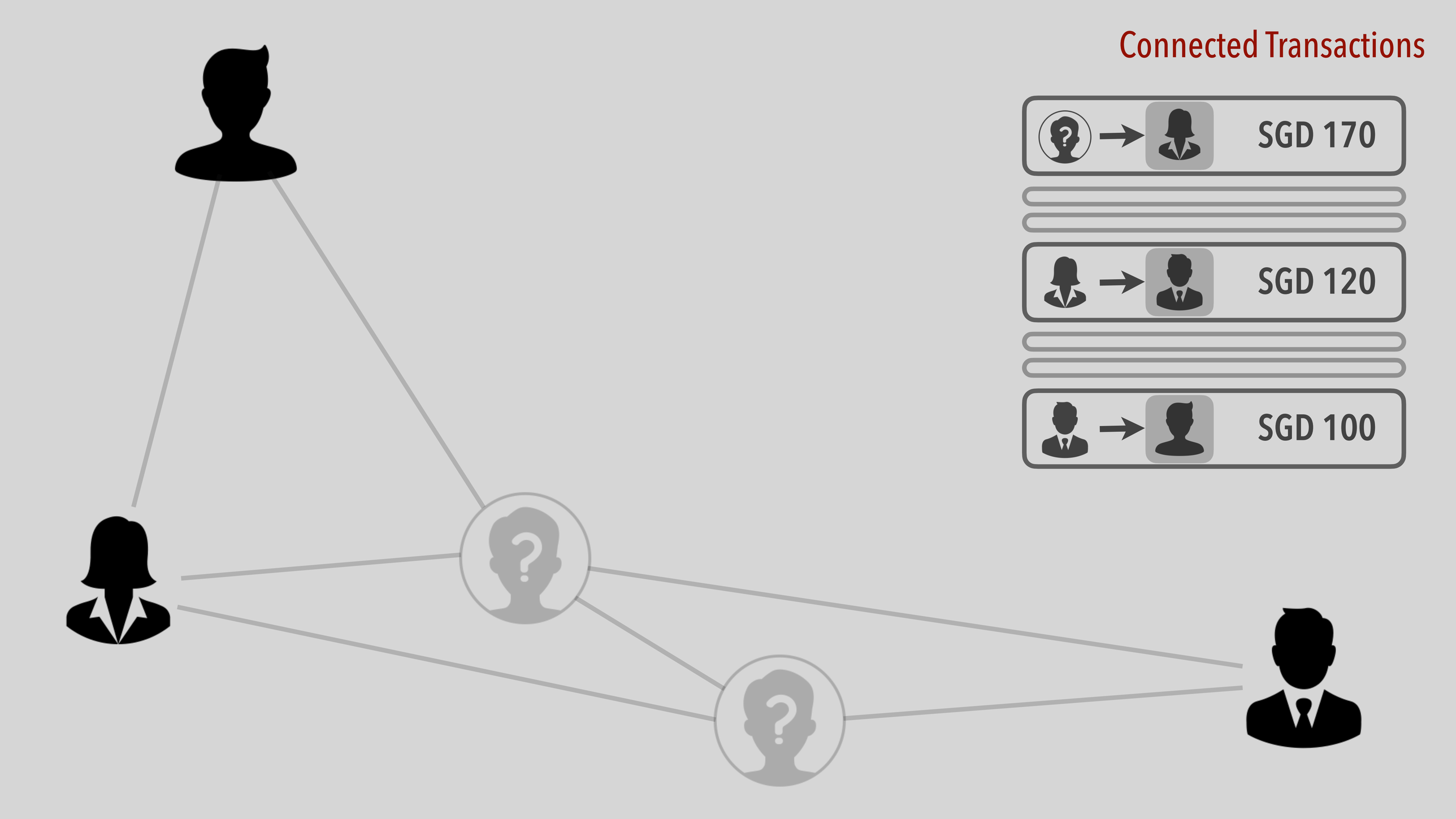



Record of Transactions
SGD 120
SGD 100

Connected Transactions



Connected Transactions



Digital Signature

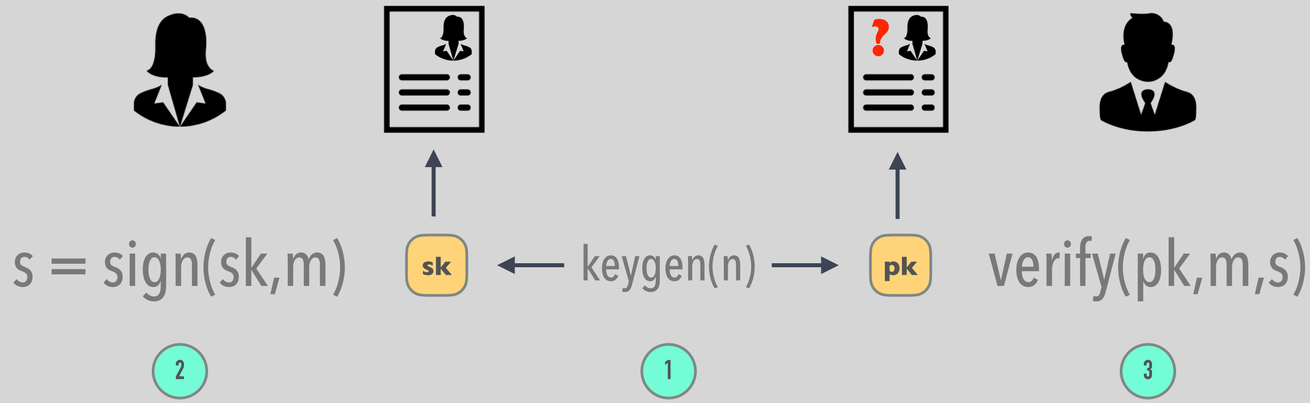
Authentic Proof of Ownership

Three algorithms

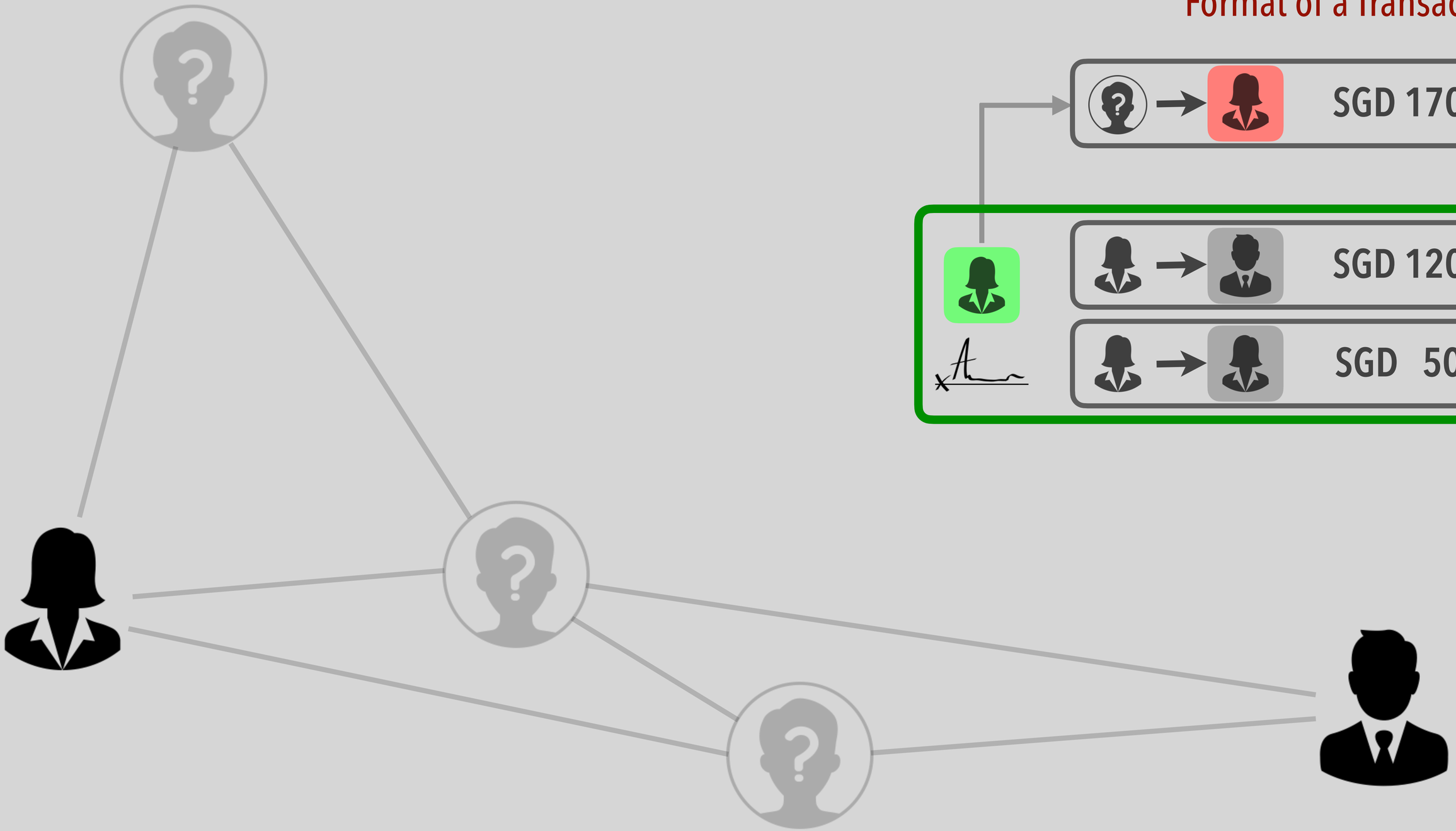
sk, pk = keygen(n)

s = sign(sk, m)

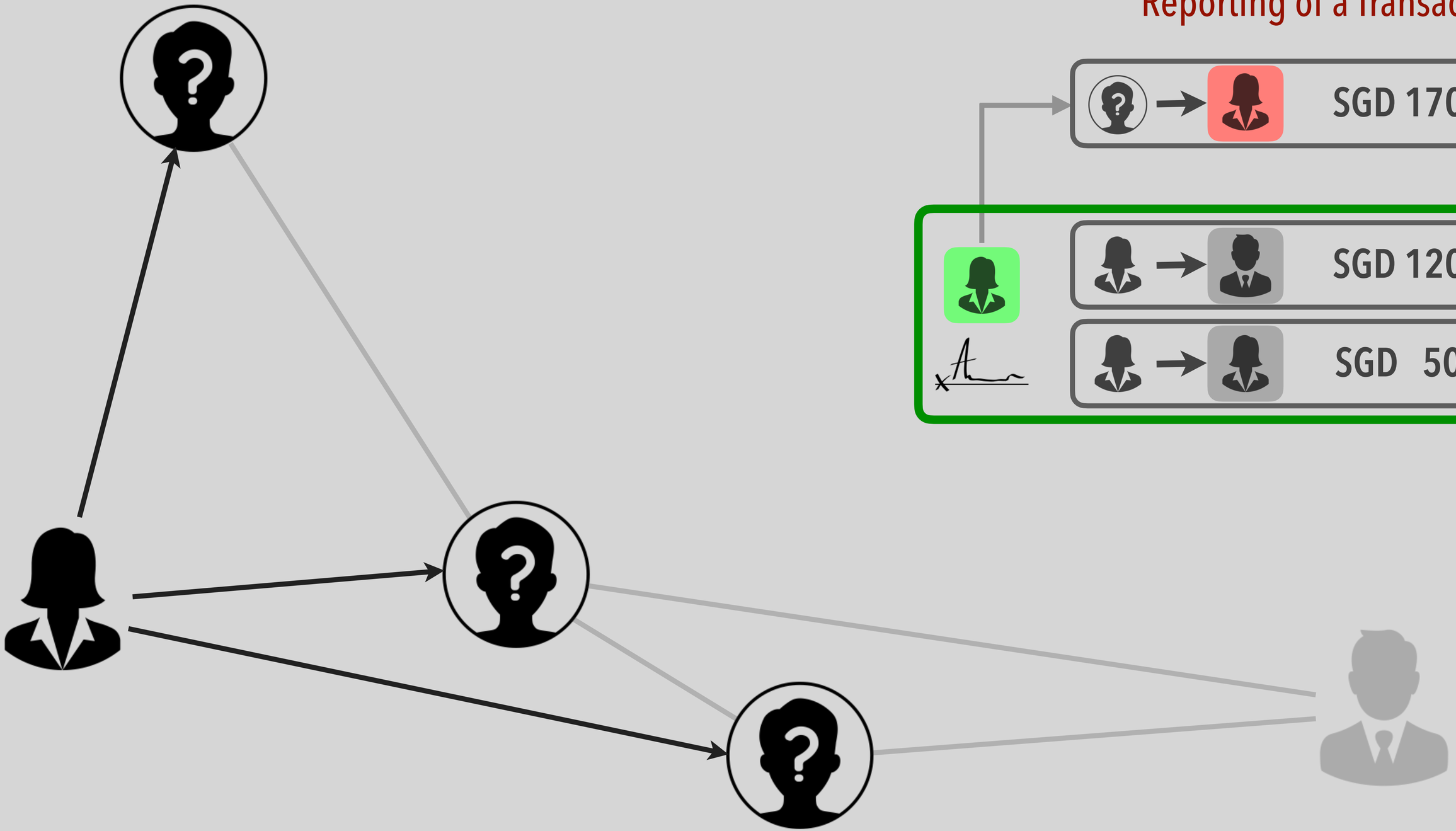
verify(pk, m, s)



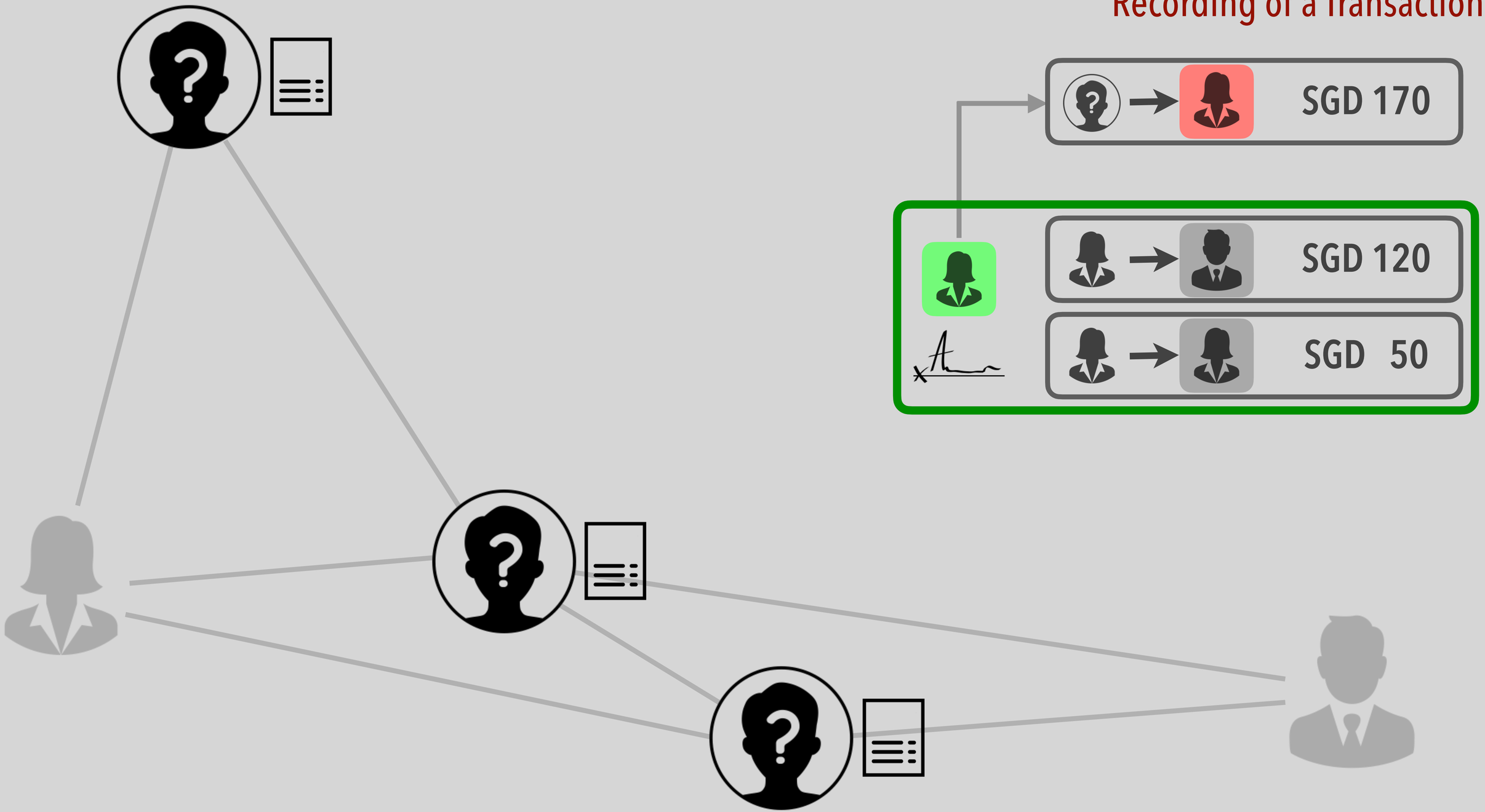
Format of a Transaction



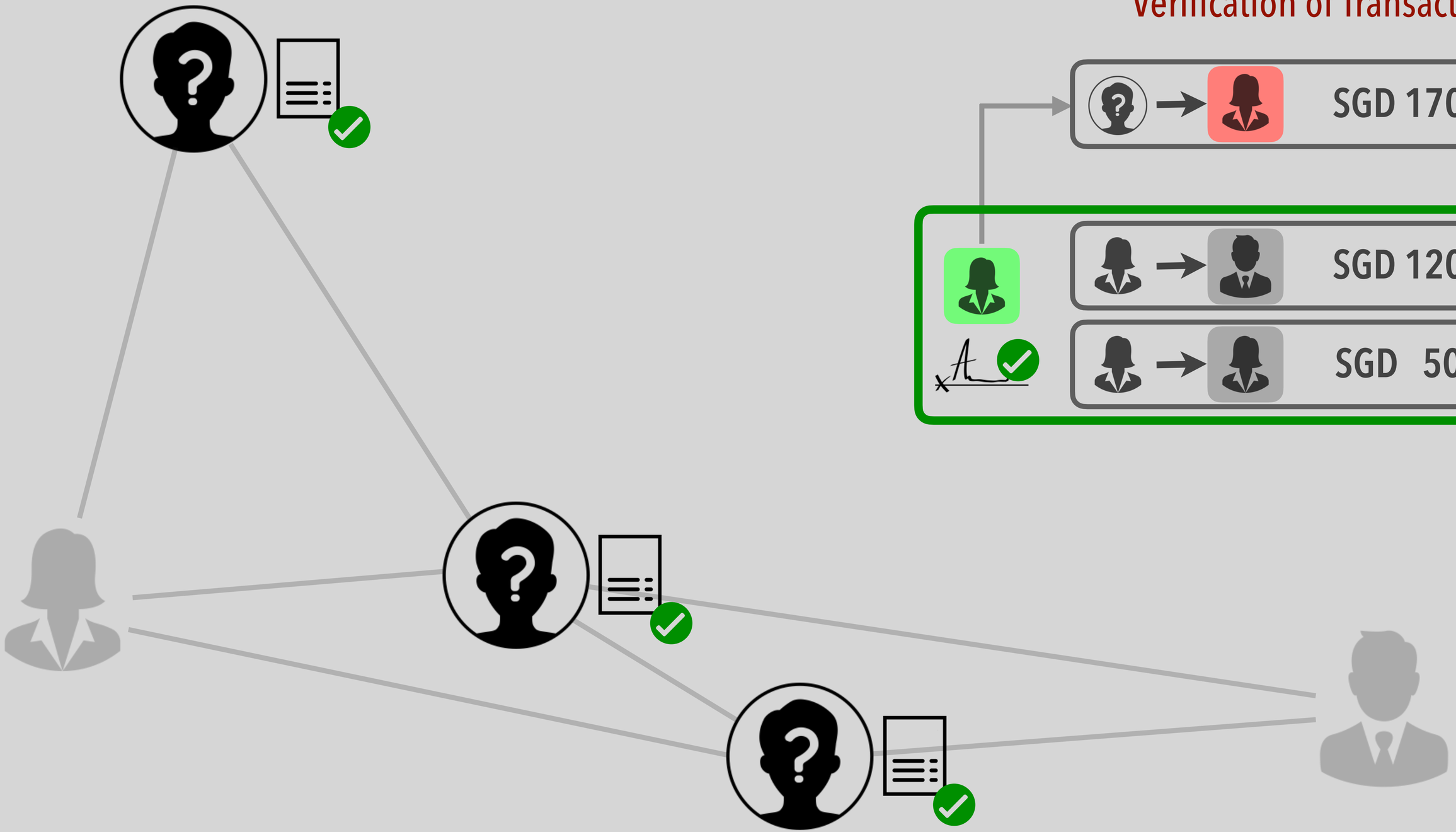
Reporting of a Transaction

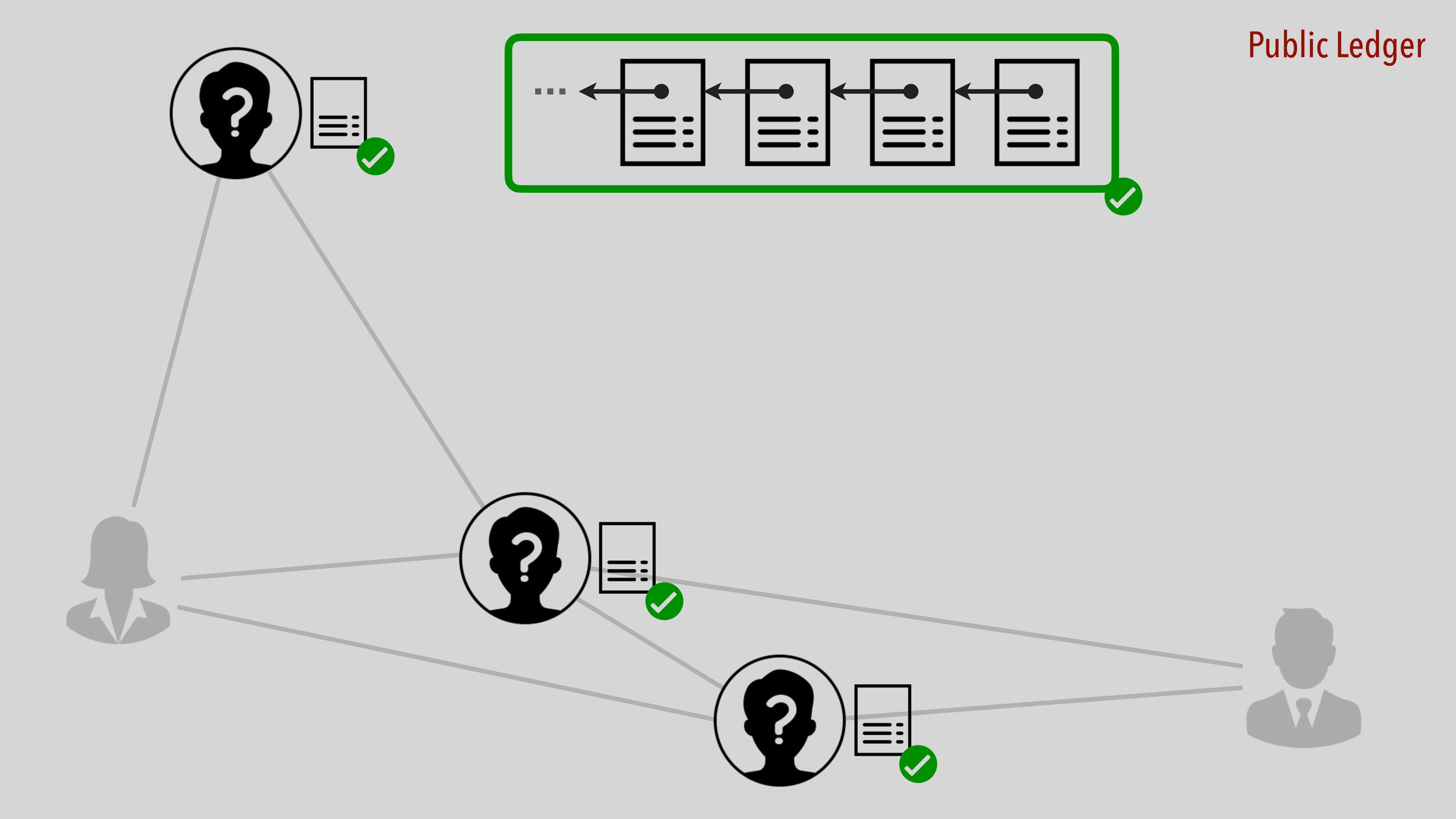


Recording of a Transaction

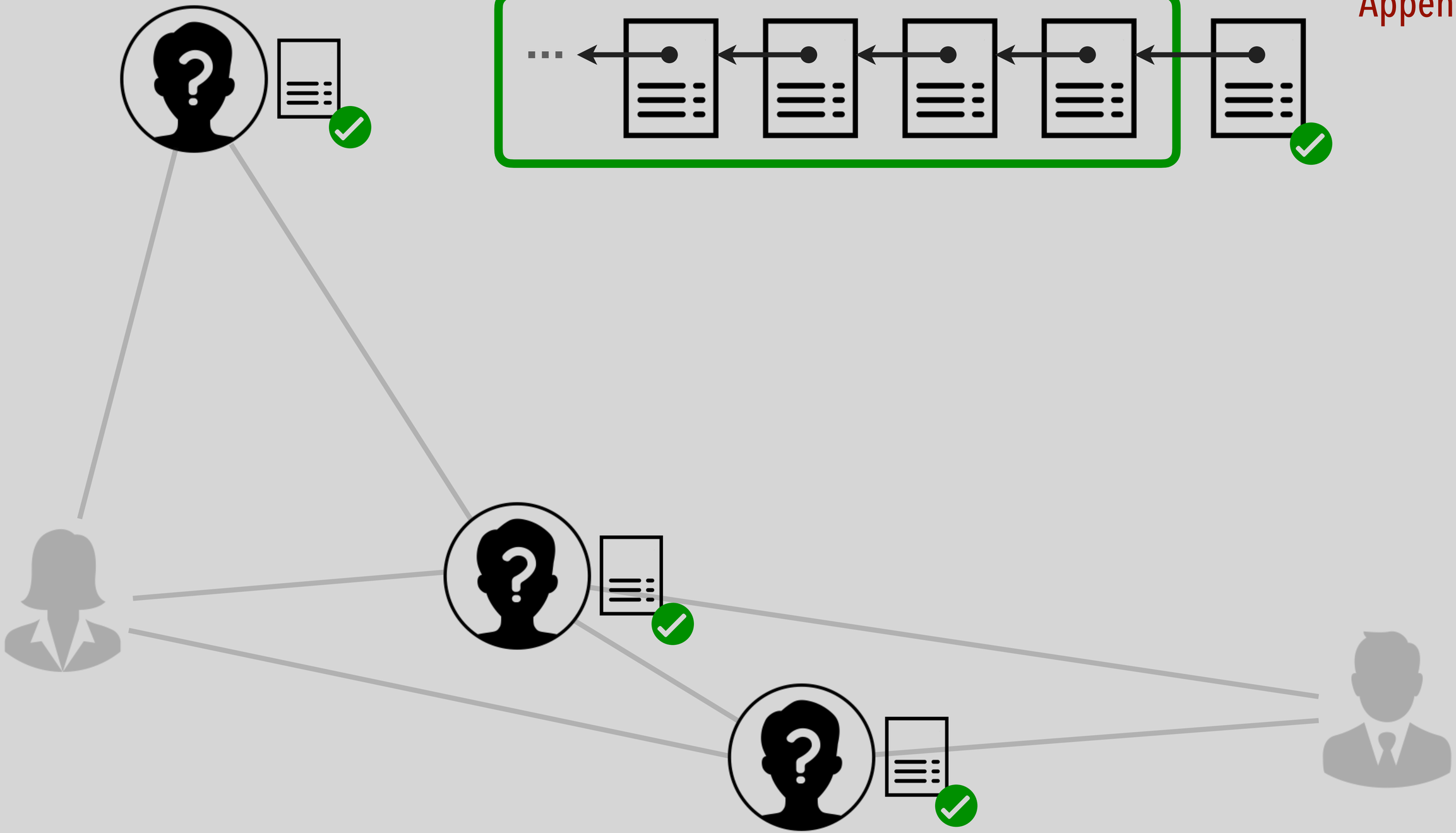


Verification of Transactions

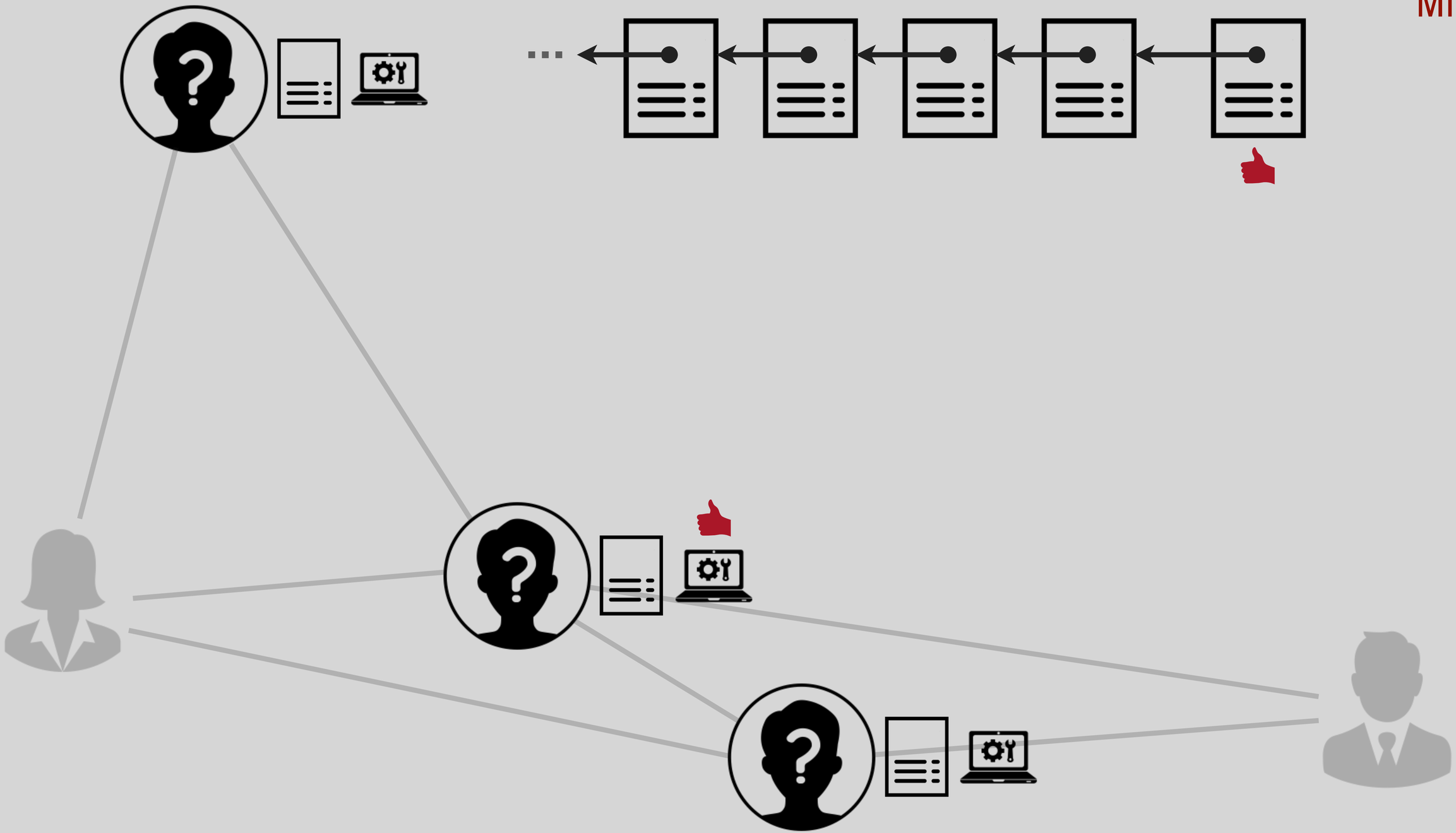


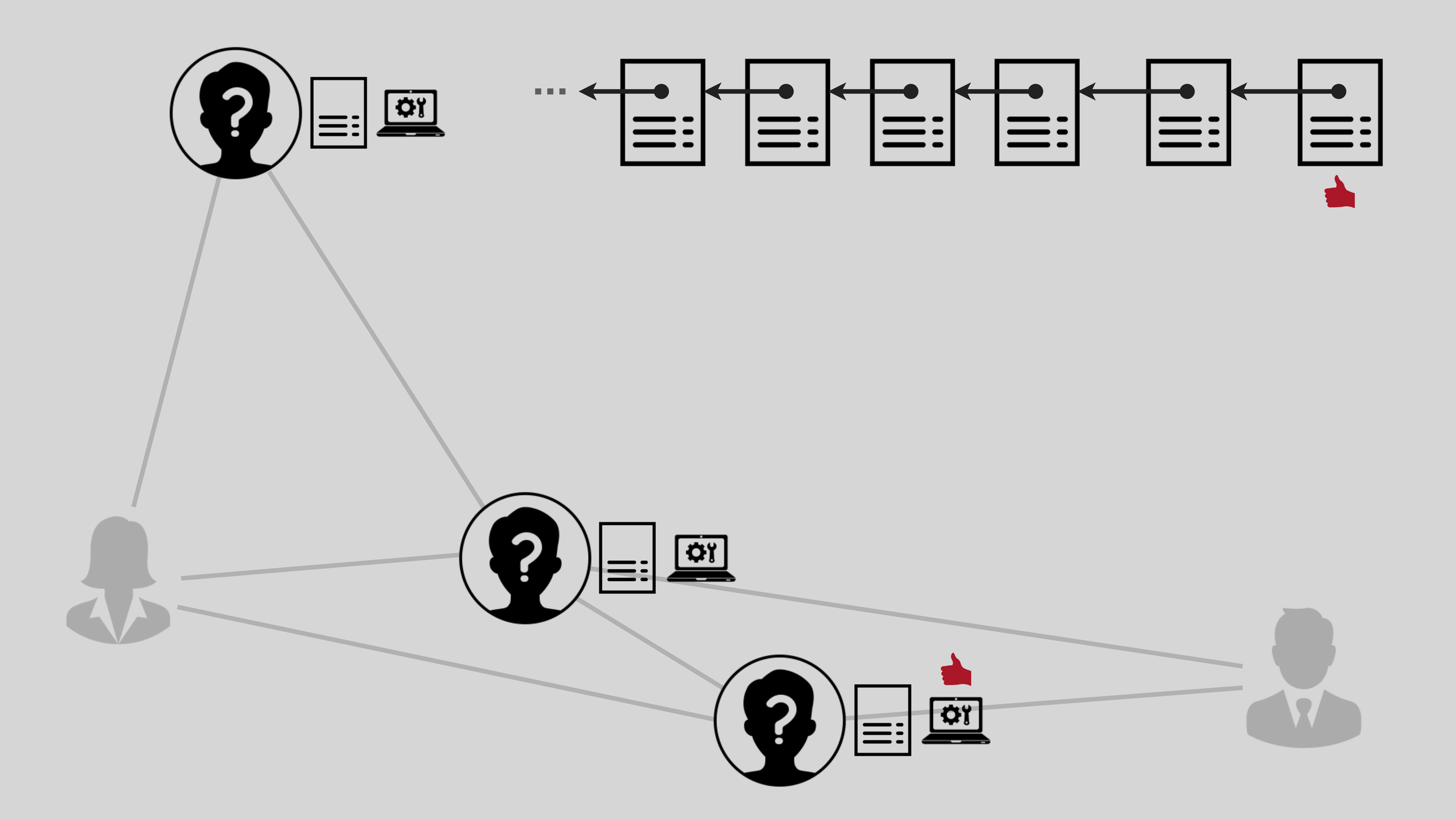

Public Ledger

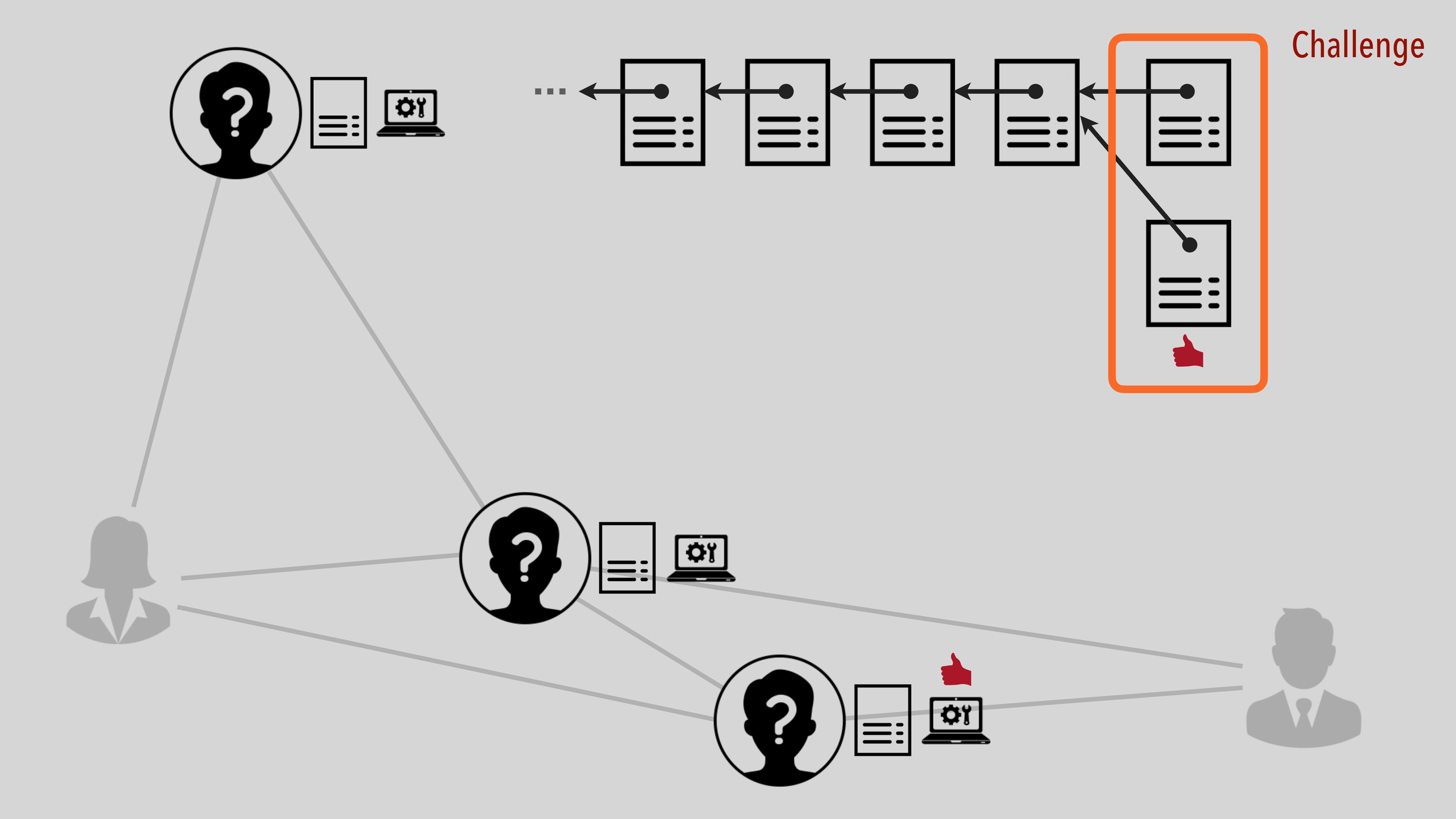
Appending



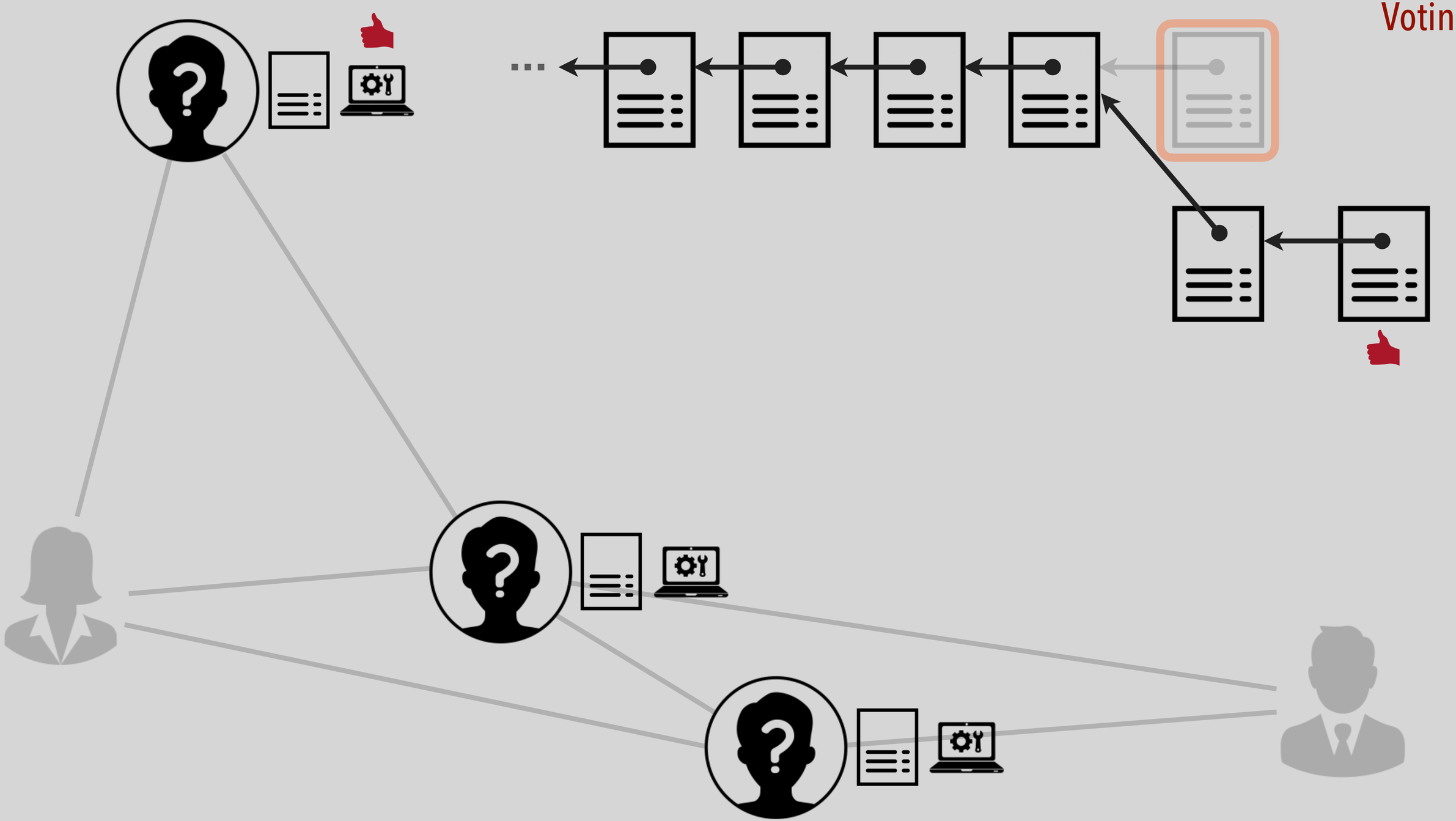
Mining

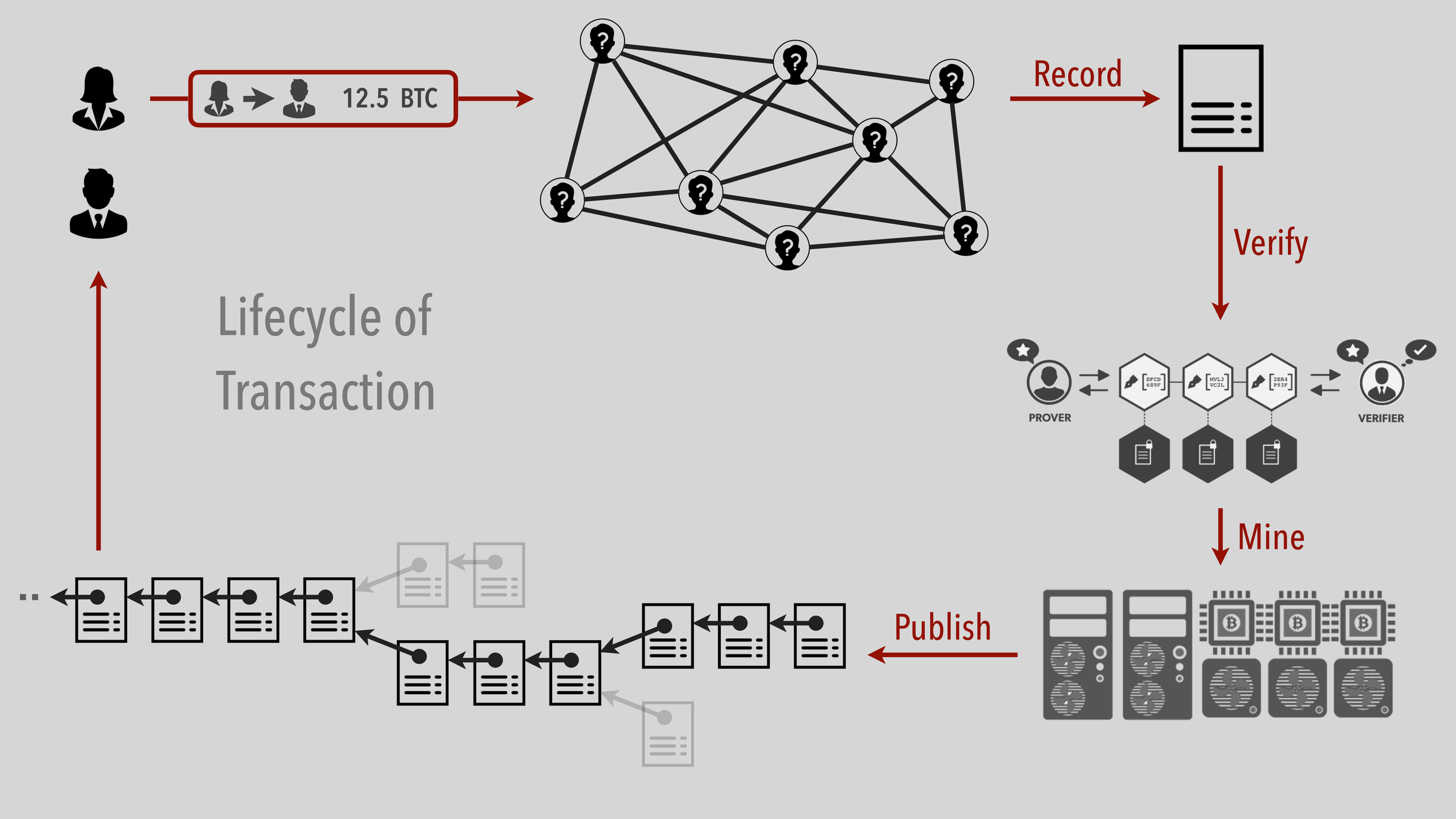





Challenge

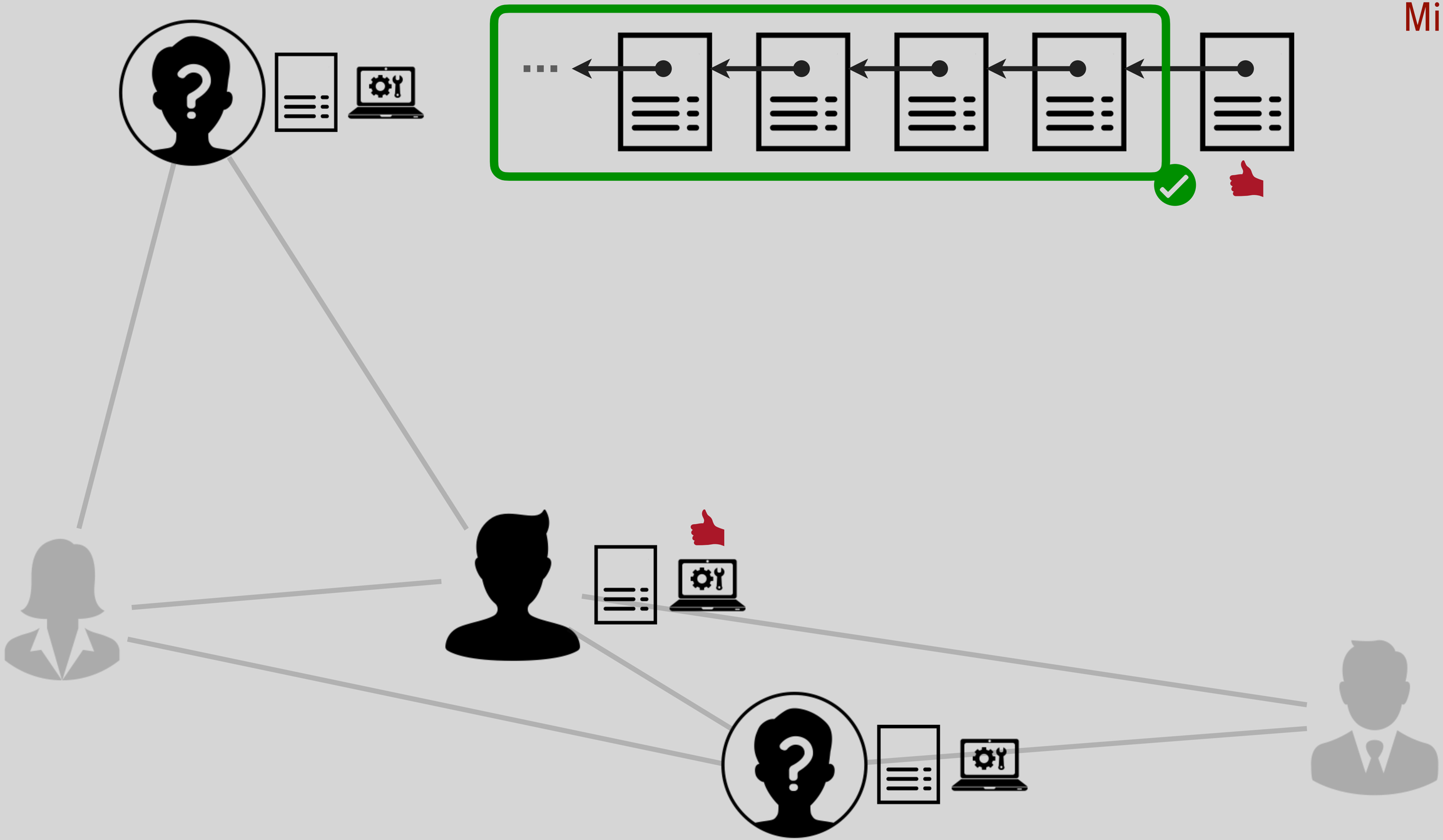
Voting

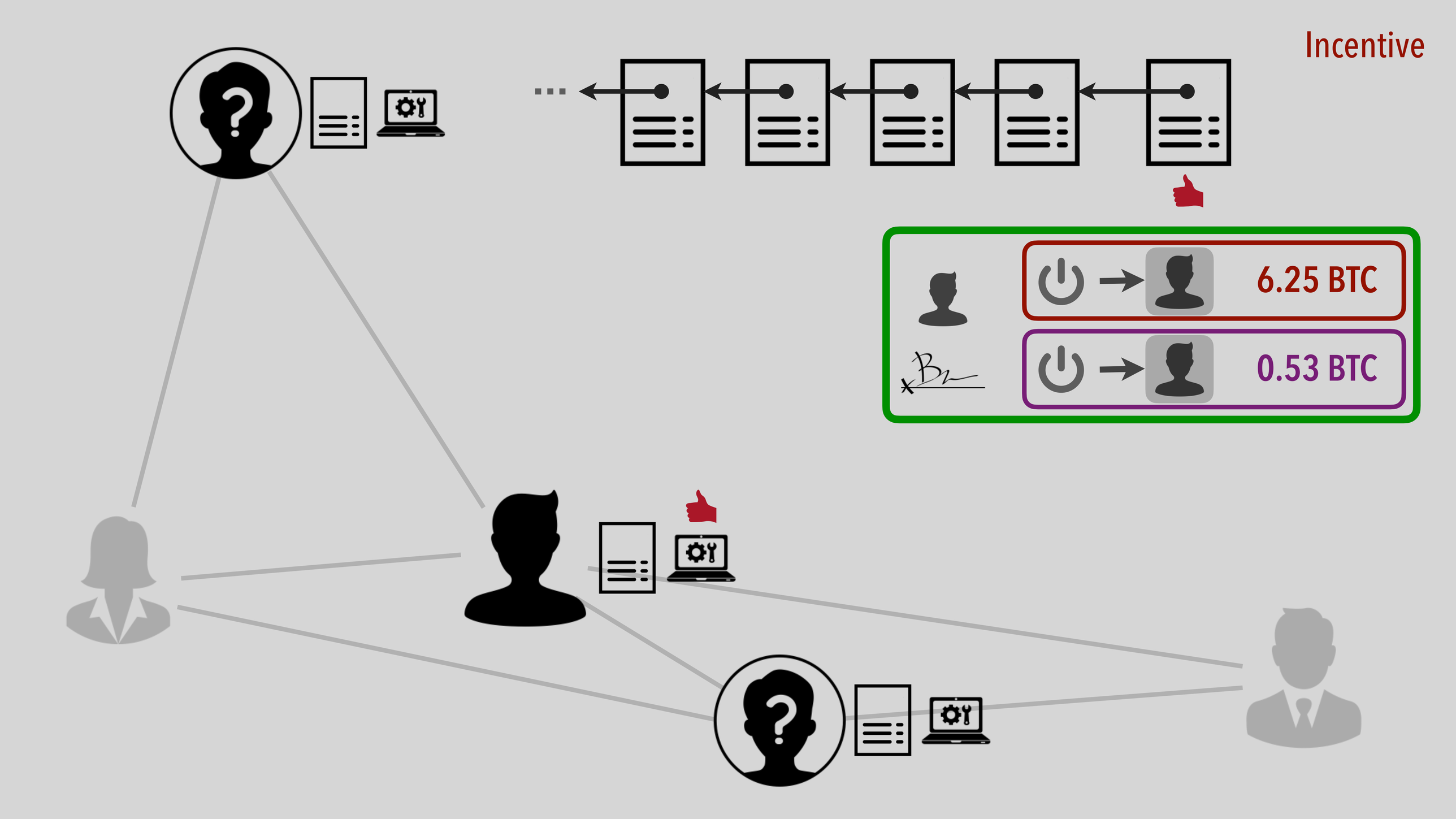



12.5 BTC
Record
Verify
Mine
Publish
PROVER
VERIFIER
Lifecycle of
Transaction

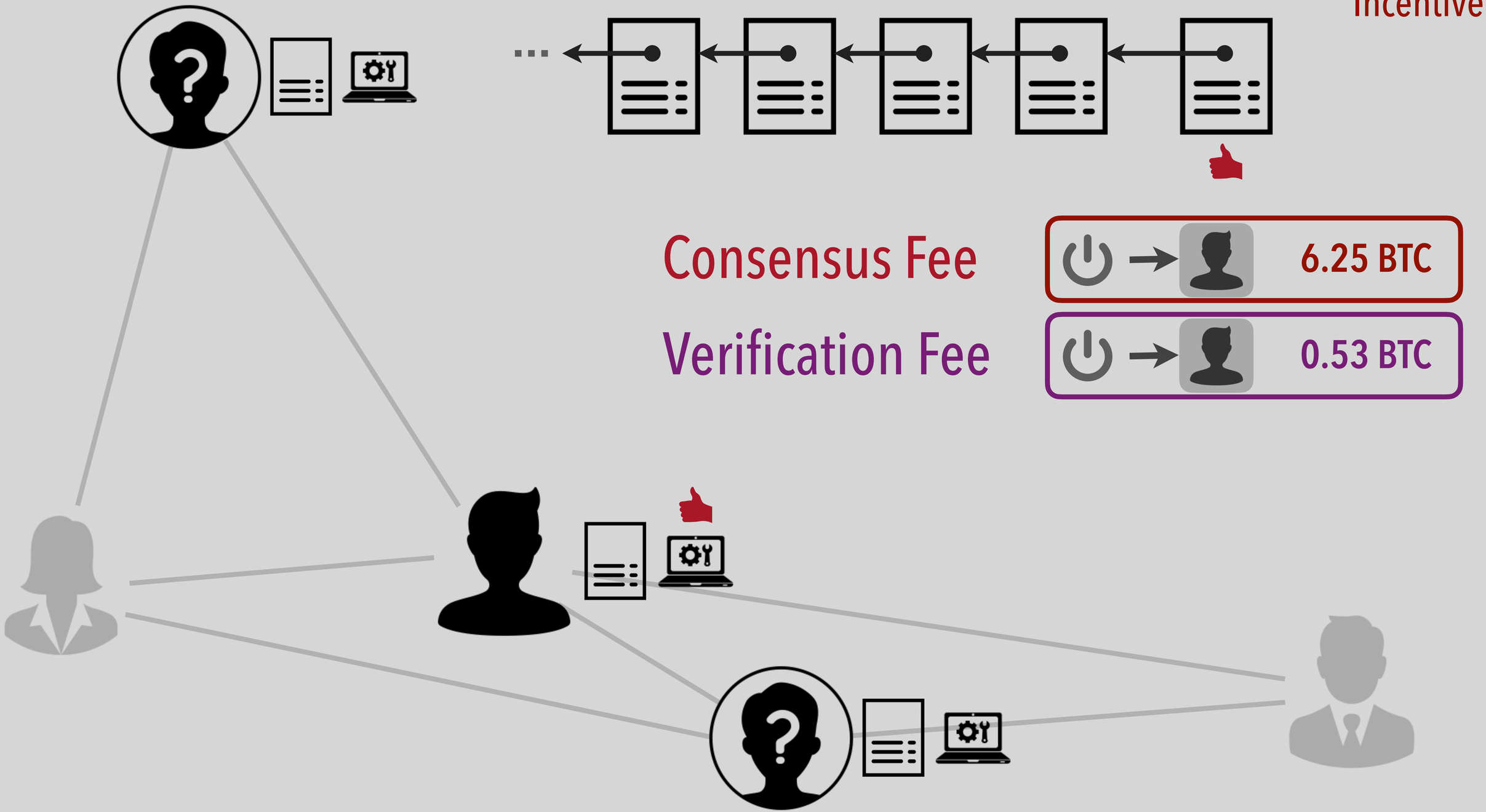
Consensus

Mining




Incentive
6.25 BTC
0.53 BTC

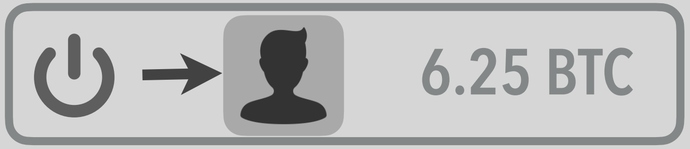
Incentive



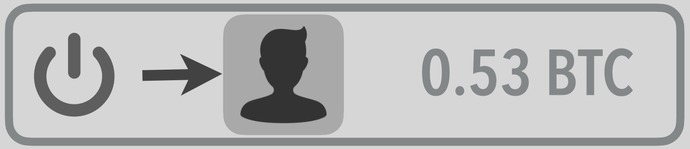
Blockchain

… from its two sides

Consensus Fee



Verification Fee



Goal of the System

Creating a verifiable tamper-resilient ledger.
Active network for End-Users to utilize reliably.

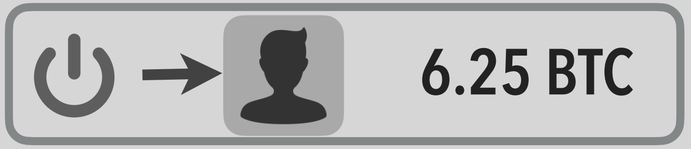
Demand of End-Users

Inclusion of records in the distributed ledger.
Value of records greater than verification cost.

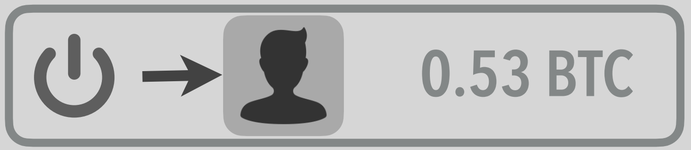
Consensus

Who pays the Fee?

Consensus Fee



Verification Fee



Economic Incentives

Built into the system/software to ensure that the Players of the “Blockchain Game” play honestly.

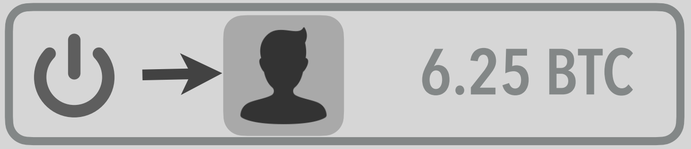
Design of Incentives

Incentives within the System to motivate honesty and Reward or Punishment to motivate Behavior.

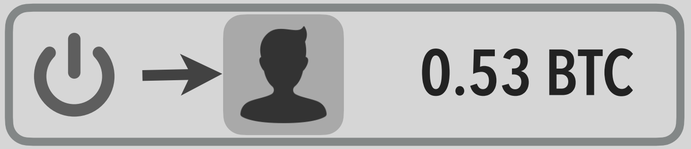
Verification

Who pays the Fee?

Consensus Fee



Verification Fee



Cost of Verification

Built into the system/software for End-Users to incentivize the miners for Inclusion of Records.

Penalizing Spams

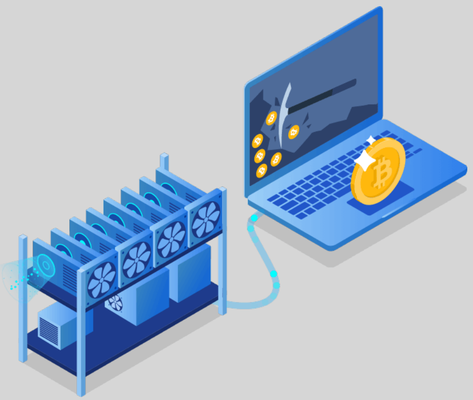
Set to a minimum to ensure less spamming by End-Users as well as an active Mining Network.

Bitcoin

Satoshi's Brilliance

hash(   )

= 0x 00…00 XX…XX

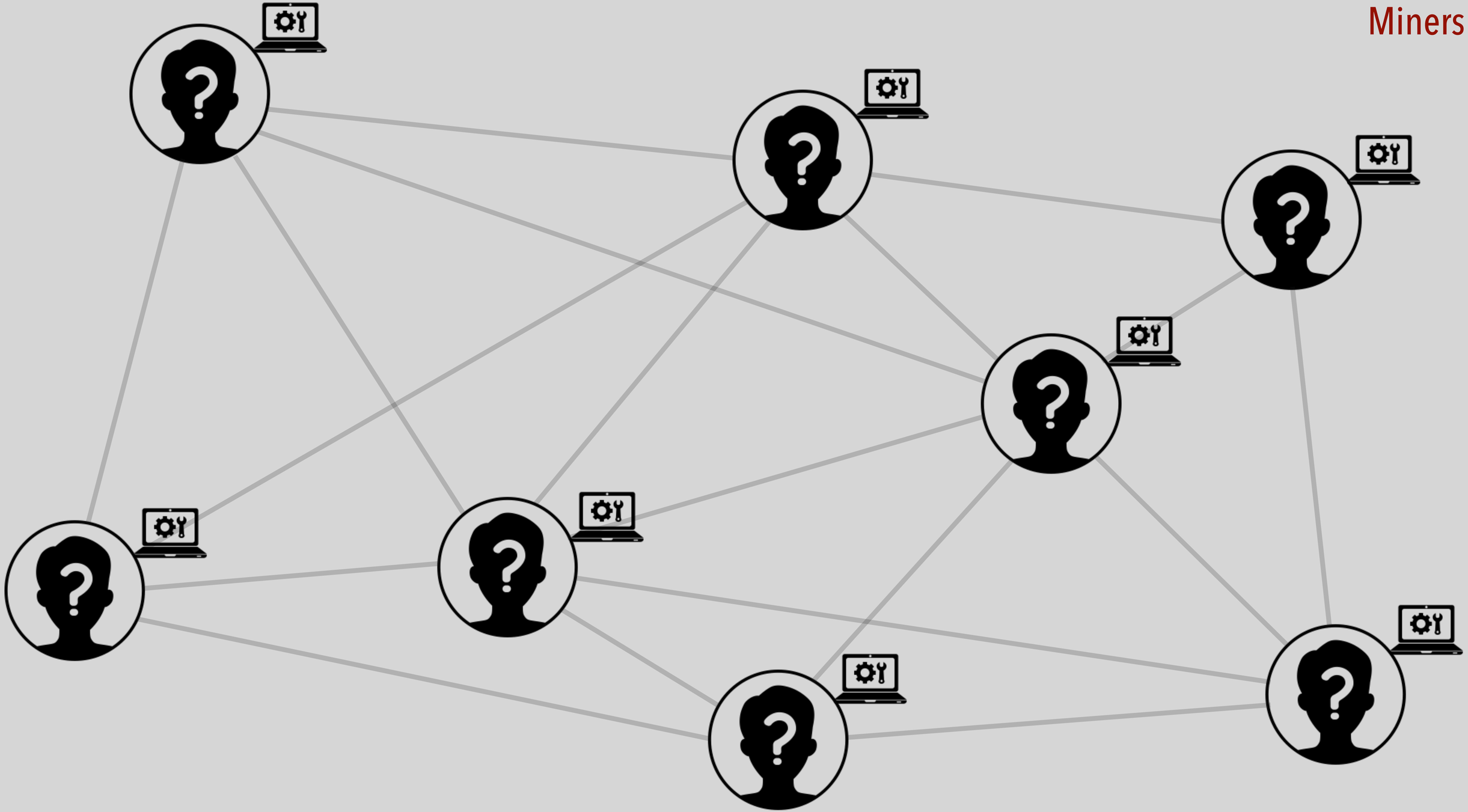


Economic Incentives

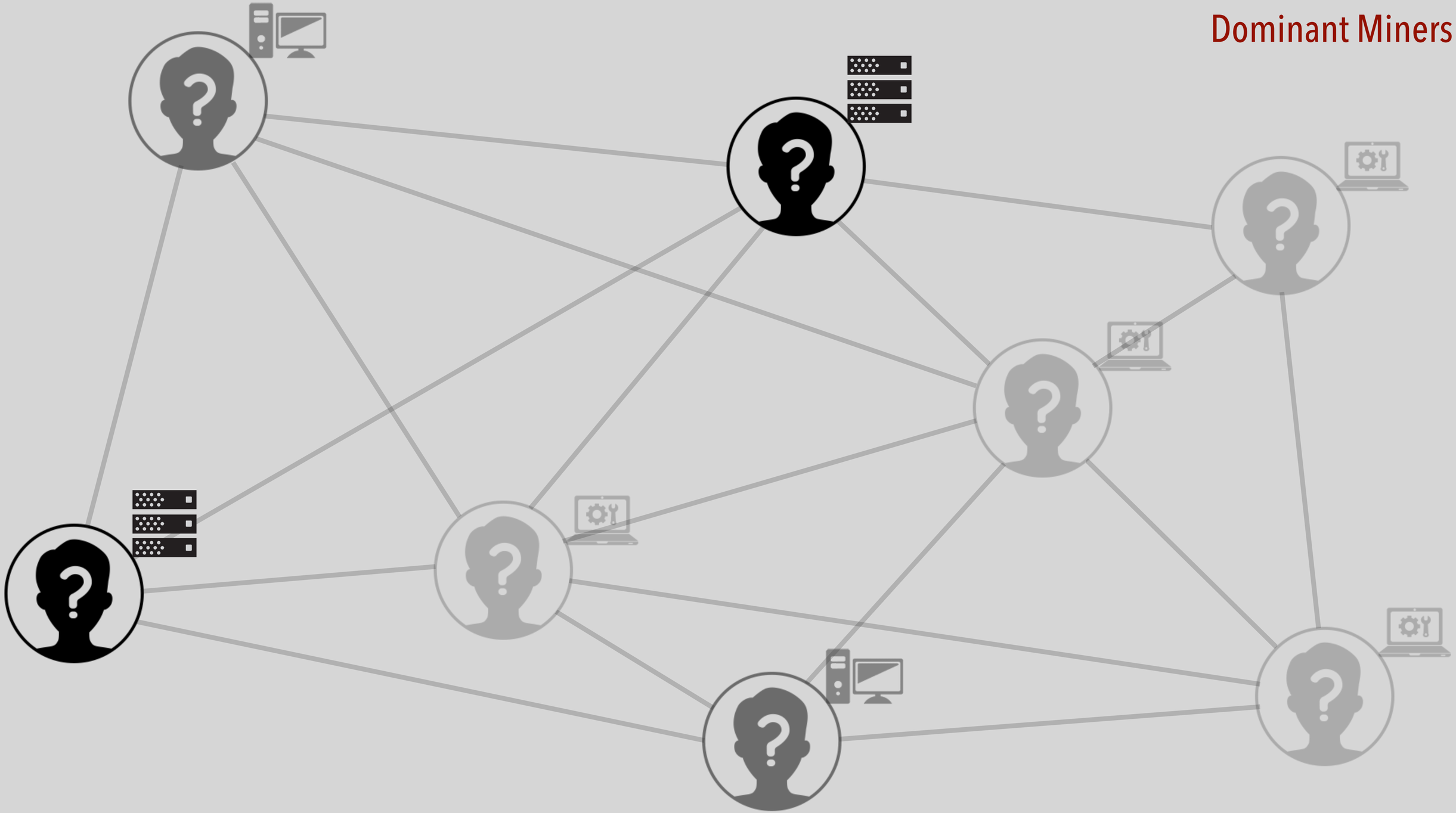
Built into the system/software to reward Miners with Bitcoin, as well as regulates Bitcoin creation.

Reusable Proof-of-Work

Built into the system/software to elect Miners for block creation, as well as to moderate Hardness.

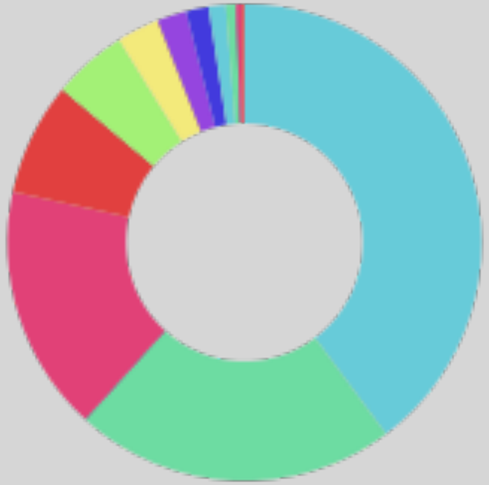

Miners

Dominant Miners



Consensus

Proof-of-Work



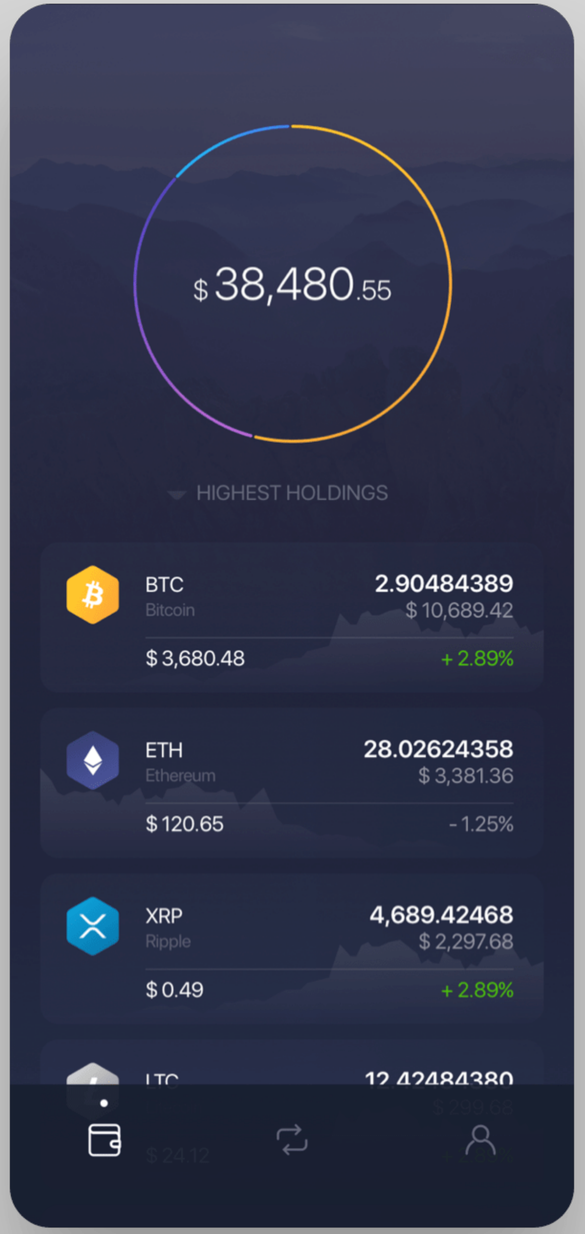
https://www.youtube.com/watch?v=J-He70rznIQ

Uneven Hash Power

Hashrate distribution of Proof-of-Work systems generally end up biased to a few Miners/Pools.

Severely non-Green

Proof-of-Work puzzles are extremely costly but otherwise completely useless computations.



Check Out

Bitcoin Demo

https://coindemo.io/

Bitcoin Blockchain

https://www.blockchain.com/explorer

Cryptocurrency Market

https://coinmarketcap.com/

Abstraction

Blockchain

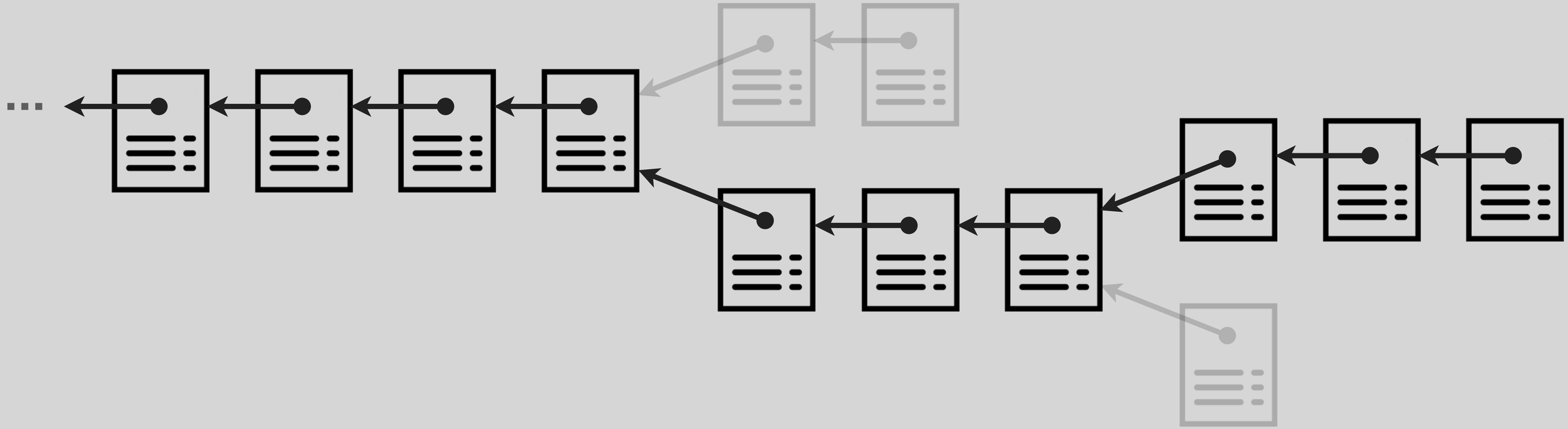
Distributed Ledger

Publicly Verifiable

Tamper Resilient

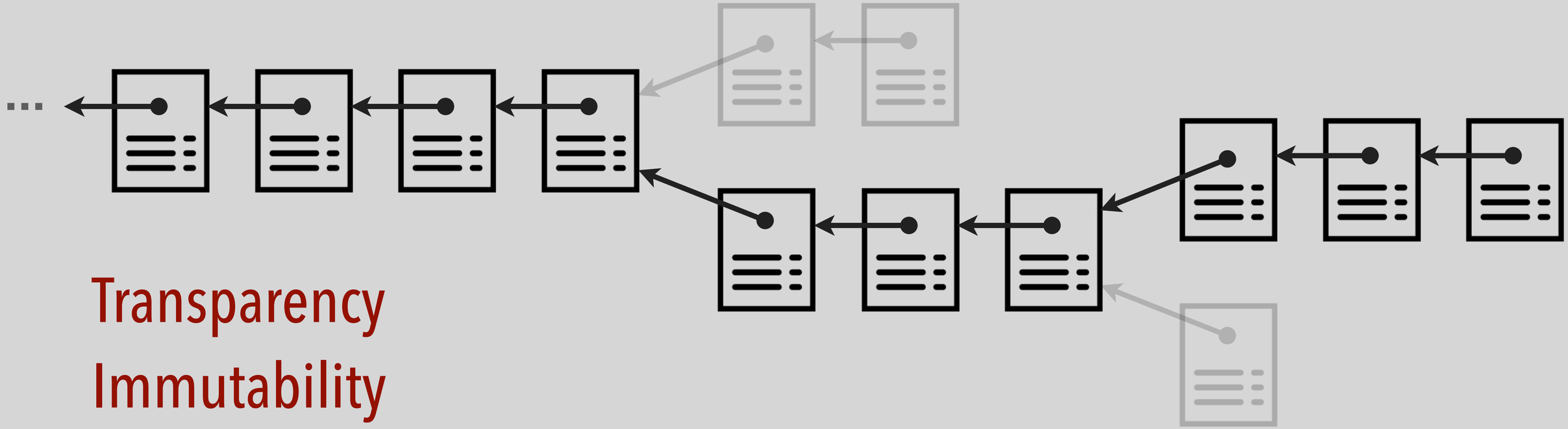
Eventually Consistent

Semi Decentralized



Shared State

Ledger of Records

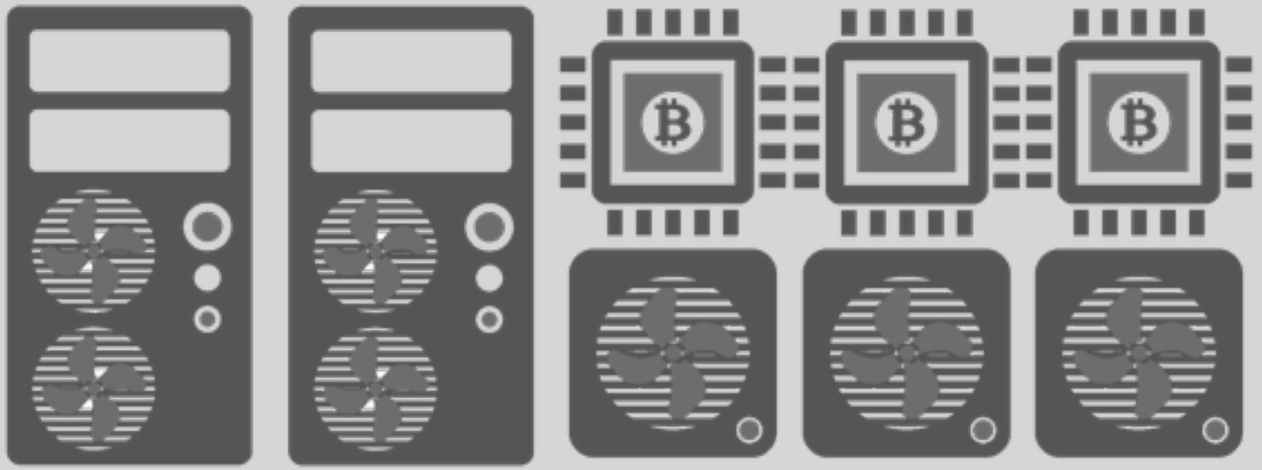


Transparency

Immutability

Consistency

Consensus Protocol

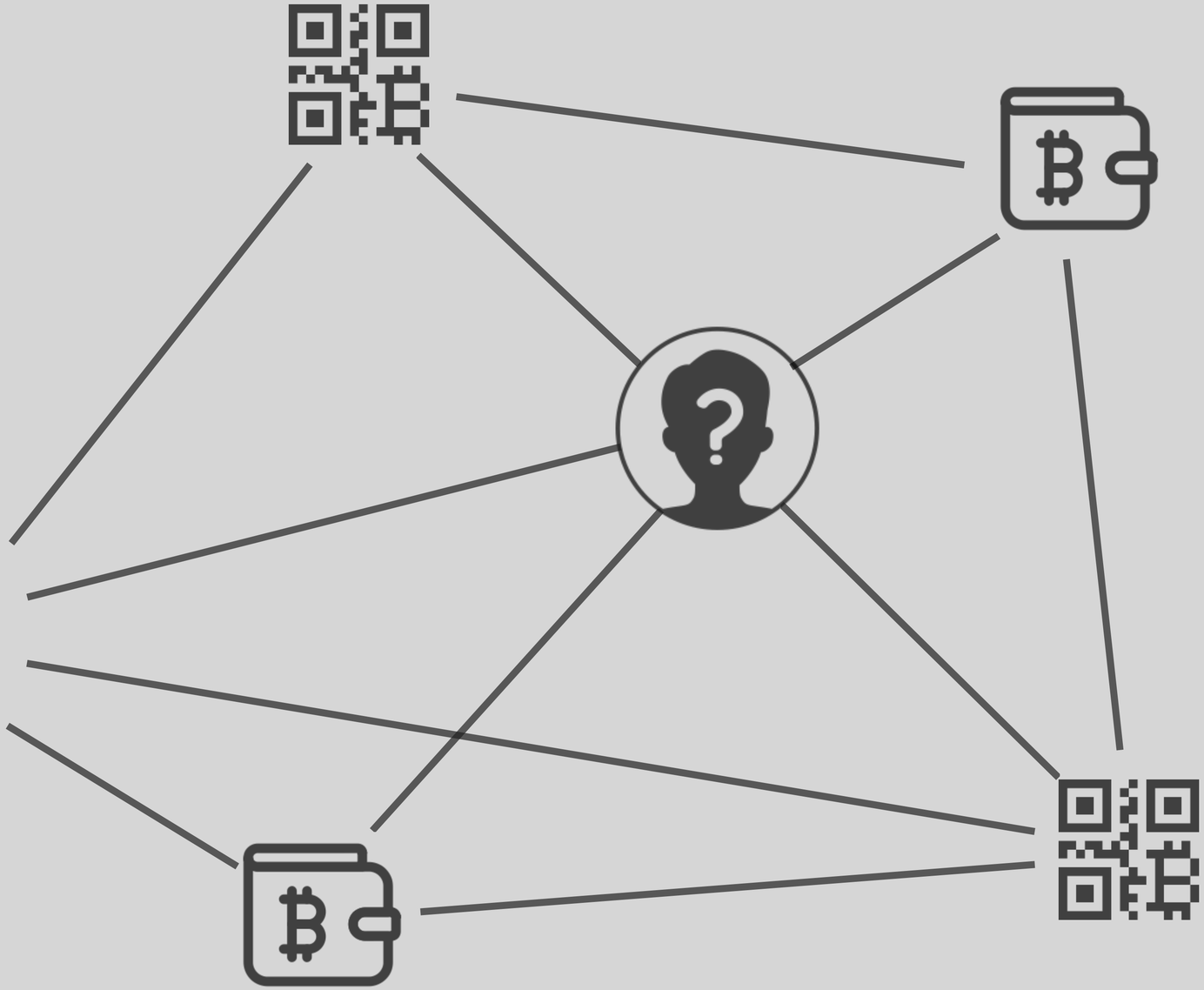


Immutability

Decentralization

Attribution

Digital Identity

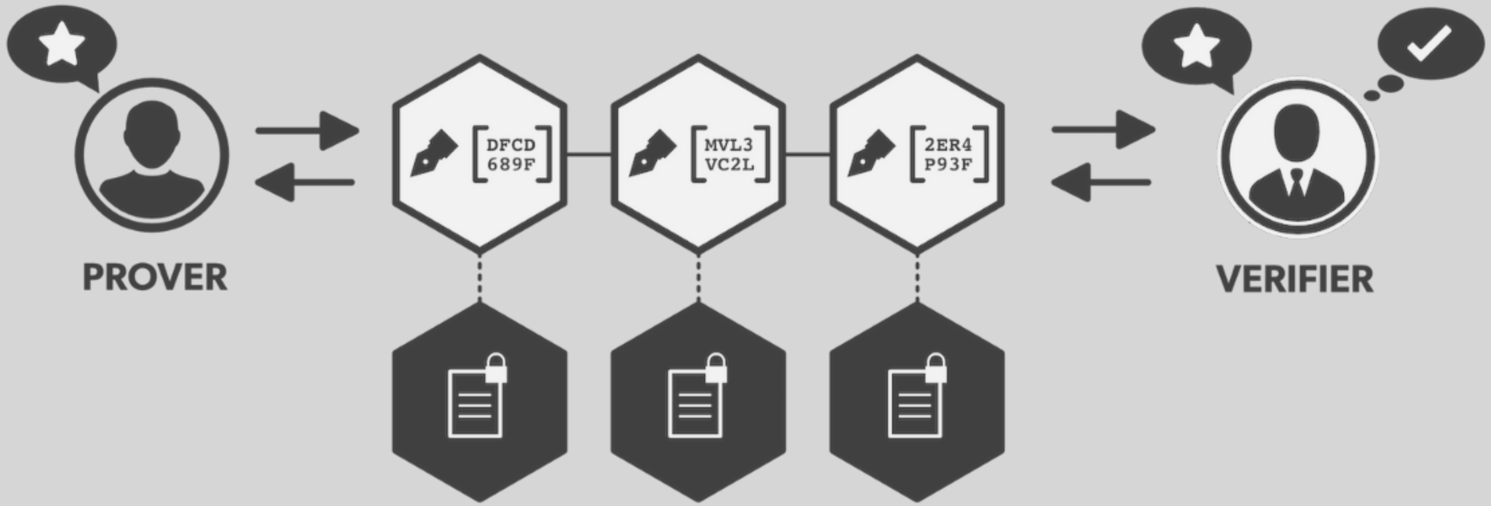


Decentralization

Provenance

Authenticity

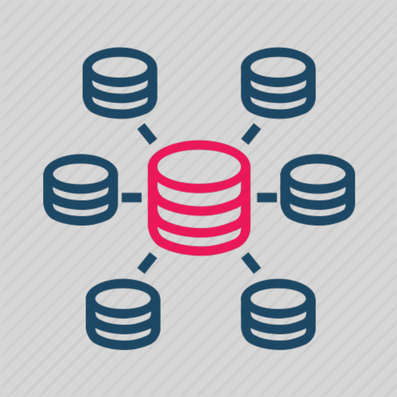
Challenge-Response



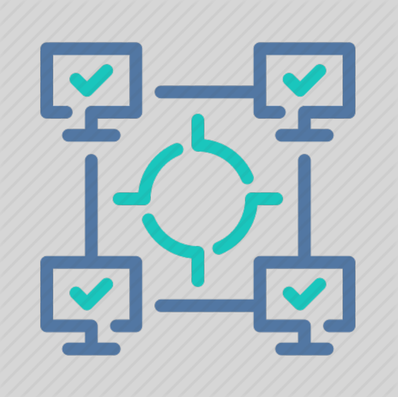
Provenance

Accountability

Cryptocurrencies

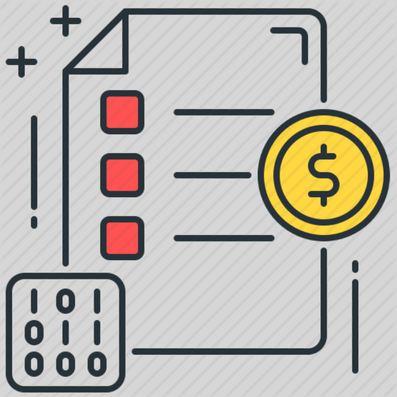


Blockchain



Consensus

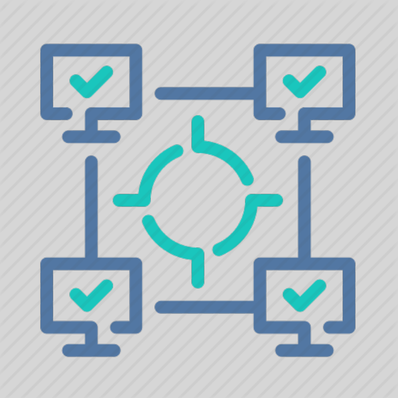
Digital Wallet



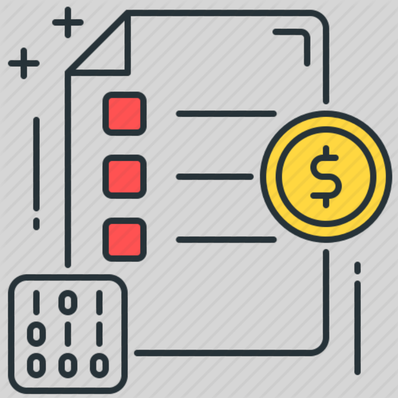
Signature

Bitcoin

Blockchain



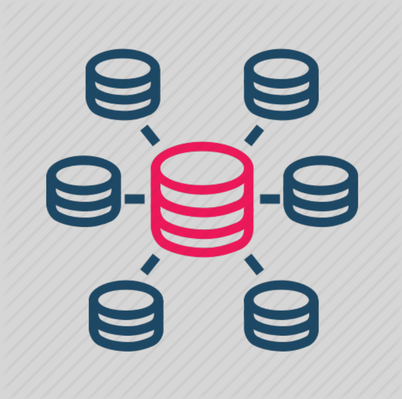
Proof-of-Work



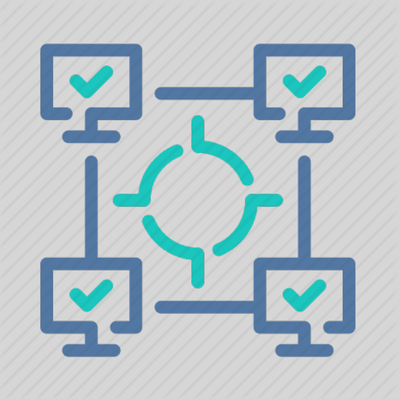
Signature

Pseudonymous

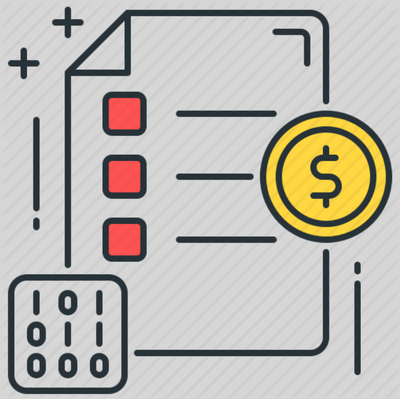
Bitcoin Cash



Blockchain*



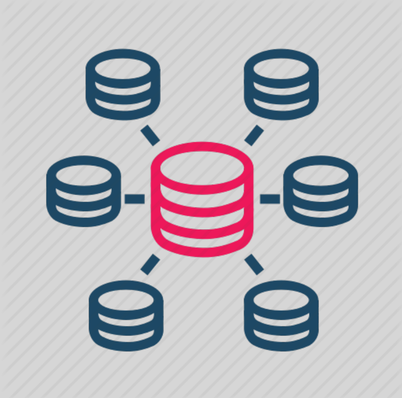
Proof-of-Work



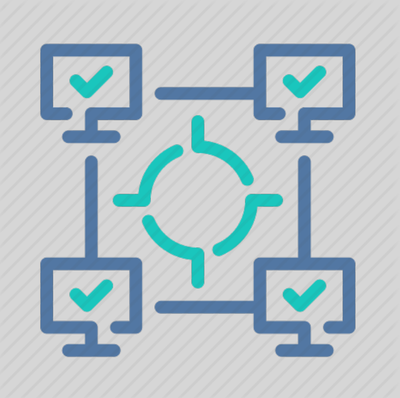
Signature

Pseudonymous

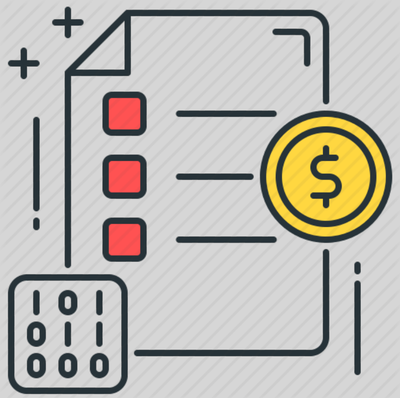
Litecoin



Blockchain*



Proof-of-Work*

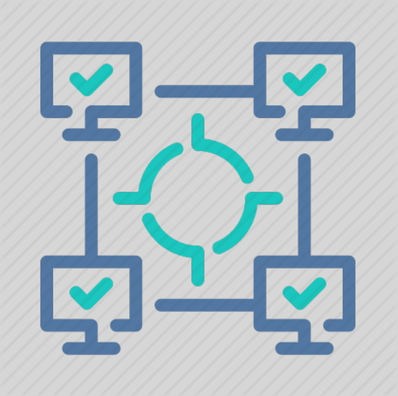


Signature

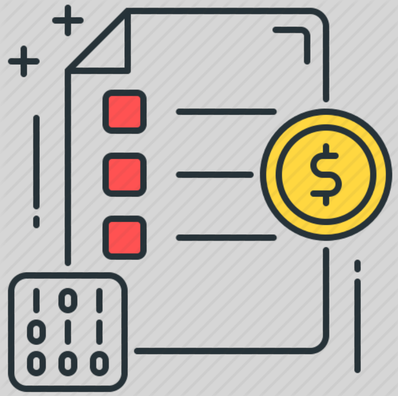
Pseudonymous

Monero

Blockchain*



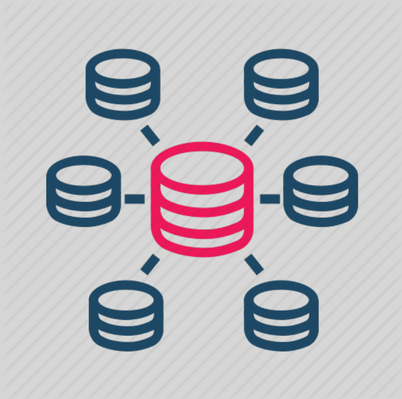
Proof-of-Work*



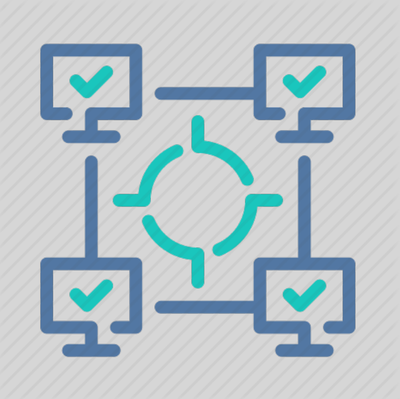
Ring-Signature

Un-Linkable

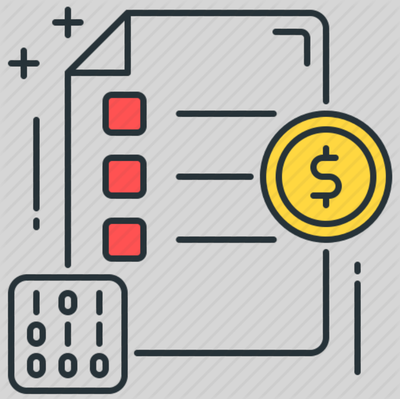
ZCash



Blockchain*



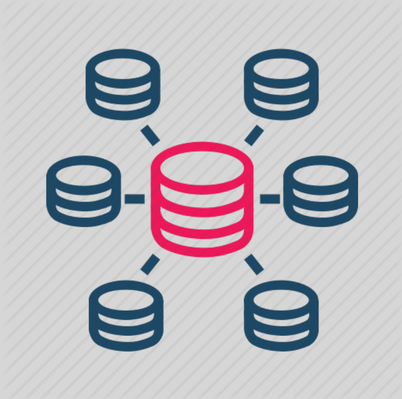
Proof-of-Work*



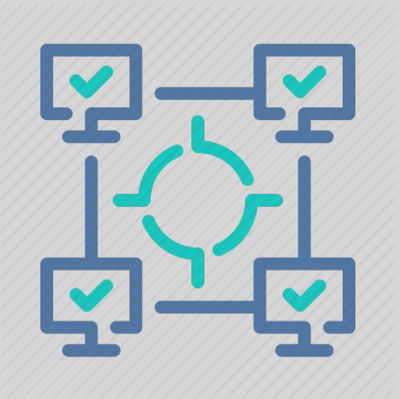
Zero-Knowledge

Anonymous

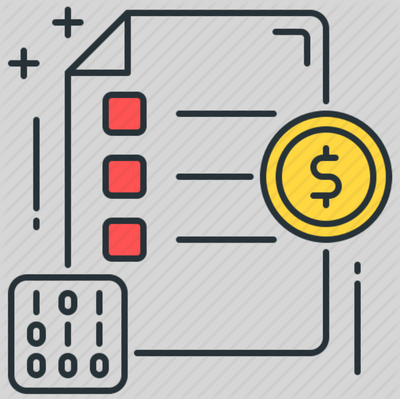
Ripple



Blockchain*



Ripple-Protocol



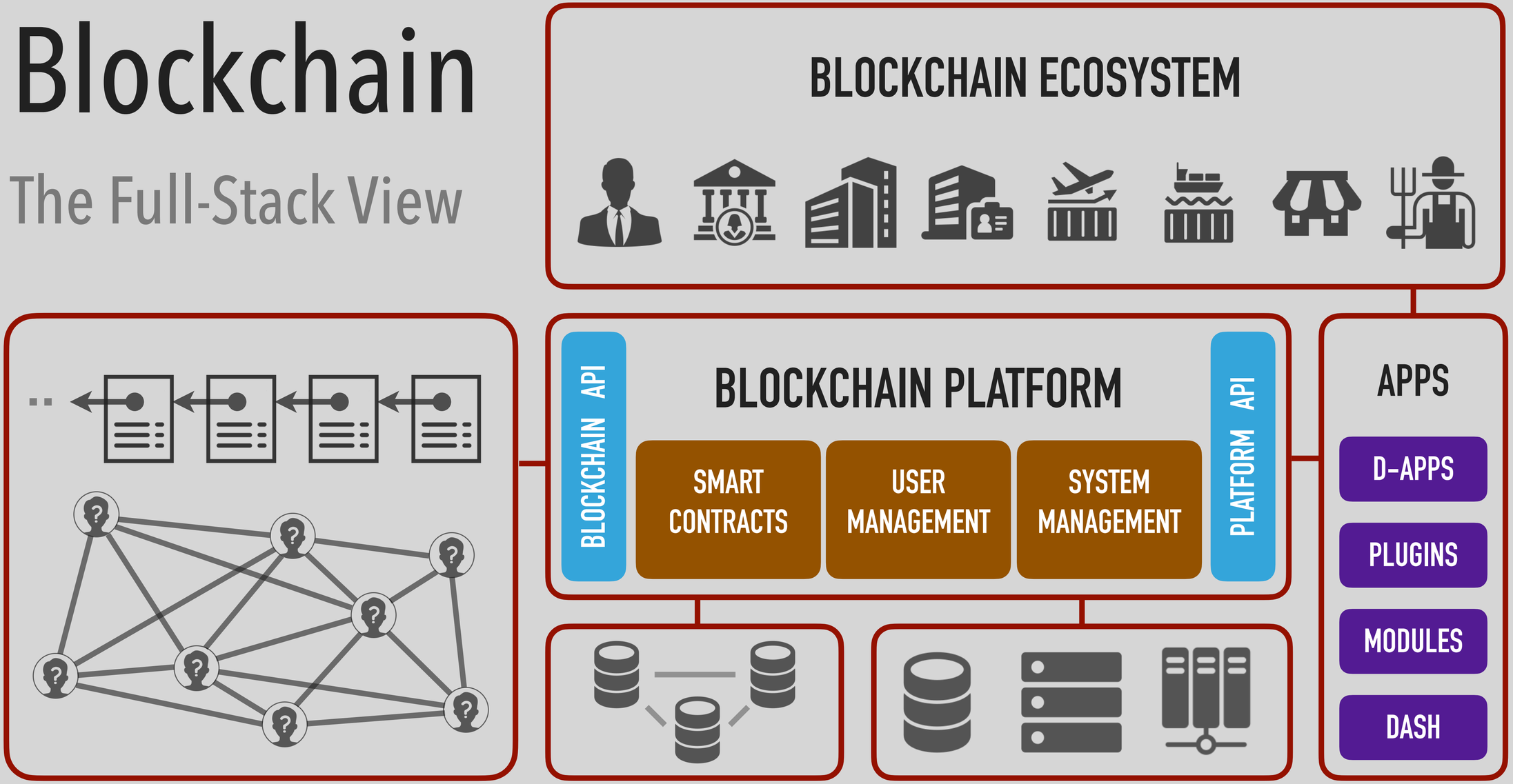
Payments

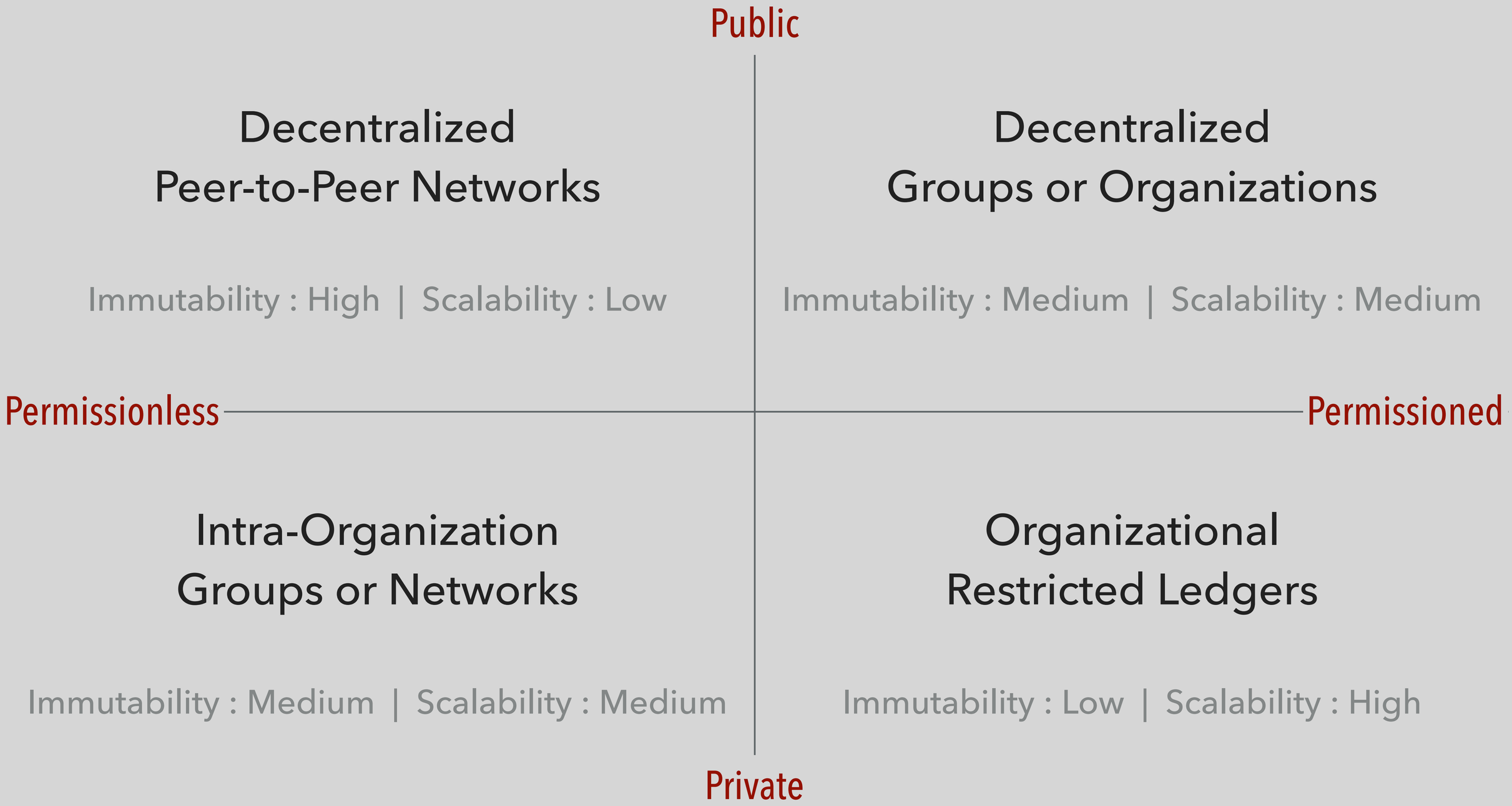
Registered

Blockchain

Blockchain

The Full-Stack View




Public
Decentralized
Peer-to-Peer Networks
Immutability : High | Scalability : Low
Decentralized
Groups or Organizations
Immutability : Medium | Scalability : Medium
Permissionless
Permissioned
Intra-Organization
Groups or Networks
Immutability : Medium | Scalability : Medium
Organizational
Restricted Ledgers
Immutability : Low | Scalability : High
Private

Smart Contract

and Blockchain Software

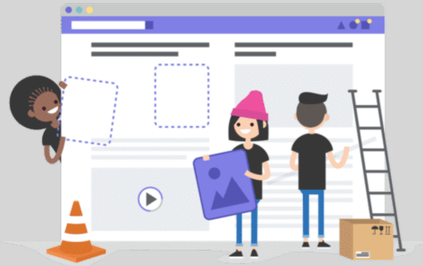
Bitcoin Script

Ethereum Solidity

Hyperledger Chaincode

… and many more

Smart contract development



Front end development of application

Supervision of full stack

Backend development

Scalability

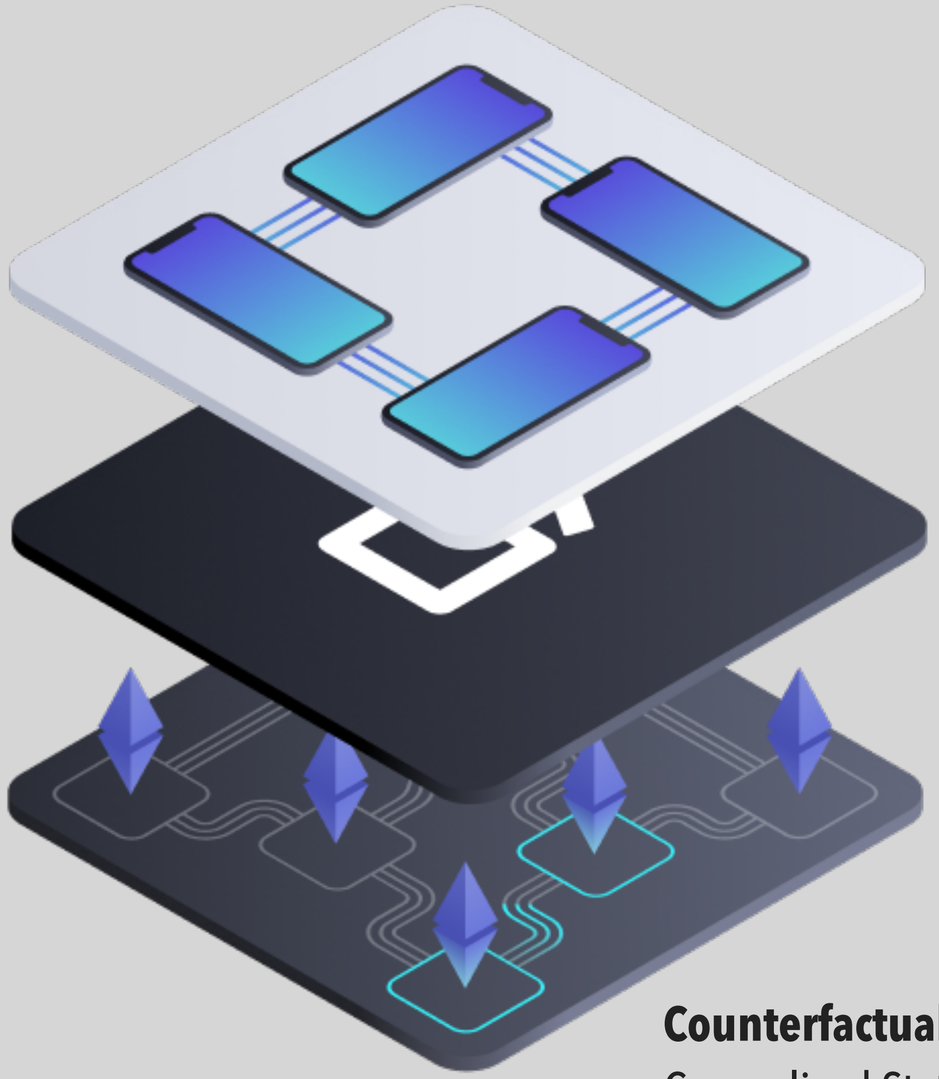
for Usable Latency

Off-Chain Transactions

Sharding Mechanisms

Layer N and Channels

… and many more



Counterfactual
Generalized State Channels

Interoperability

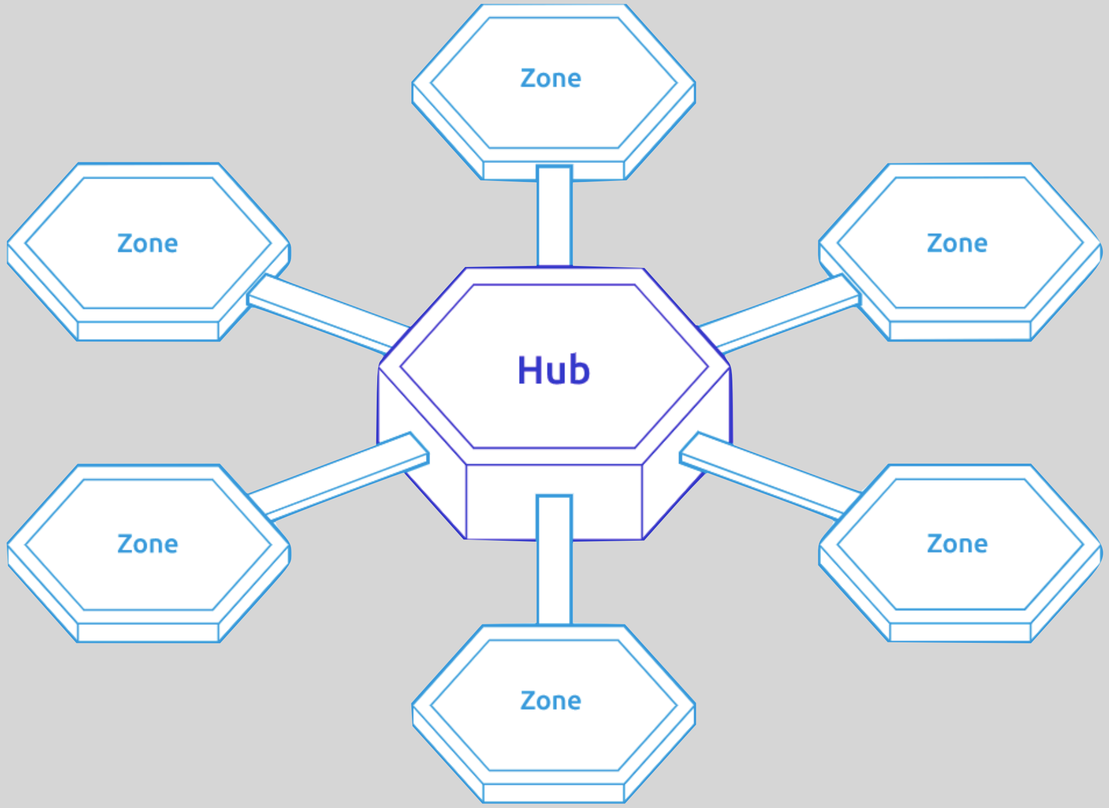
for “Internet of Blockchains”

Decentralized Exchanges

Atomic Swaps on Chains

Cosmos and Tendermint

… and many more

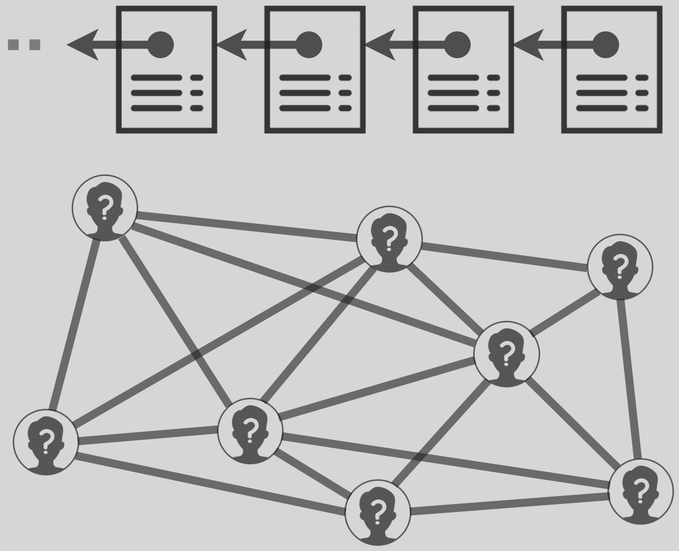


Cosmos Network

Tendermint Consensus

Security

Chain of Layers



Smart Contracts	Integrity*, Verifiability*, **Correctness**
Transaction Recording	**Integrity***, Availability*, Verifiability
Consensus Mechanism	Integrity*, Availability*, **Consistency**
Storage and Database	**Confidentiality**, Integrity, Availability
Peer-To-Peer Network	Confidentiality, Integrity, **Availability**

Each layer in a Blockchain architecture has its requirements for Security

Attacks

- Smart Contracts
- Transaction Recording
- Consensus Mechanism
- Storage and Database
- **Peer-To-Peer Network**

Routing Attacks

Attacker controls enough nodes or IPs in the network to isolate one or more valid miners or participants in the Blockchain protocol.

Hijacking Bitcoin (IEEE S&P 2017), Eclipse (USENIX Security 2015)

Attacks

- Smart Contracts
- Transaction Recording
- Consensus Mechanism
- **Storage and Database**
- Peer-To-Peer Network

Private Key Stealing

Attacker steals, destroys or compromises the private keys of miners/validators and regular participants in the Blockchain protocol.

Attacks

- Smart Contracts
- Transaction Recording
- **Consensus Mechanism**
- Storage and Database
- Peer-To-Peer Network

Majority Control

Attacker controls the majority of the "power" in mining/validating the transactions posted by participants in the Blockchain protocol.

Hash Power (2014), Selfish Mining (2014), Block Withholding (2011)

Attacks

- Smart Contracts
- **Transaction Recording**
- Consensus Mechanism
- Storage and Database
- Peer-To-Peer Network

Transaction Malleability

Attacker changes or destroys the primary data or meta data of the transactions posted by participants in the Blockchain protocol.

Transaction Malleability (FC 2015), Time Jacking (2011)

Attacks

- **Smart Contracts**
- Transaction Recording
- Consensus Mechanism
- Storage and Database
- Peer-To-Peer Network

Buggy Contracts

Attacker exploits the software vulnerabilities discovered in Smart Contracts instantiated by participants in public Blockchain platforms.

The DAO Attack (2016), Parity MultiSig Attack (2017)

Prevention

- **Smart Contracts**
- Transaction Recording
- Consensus Mechanism
- Storage and Database
- Peer-To-Peer Network

Vulnerability Analysis

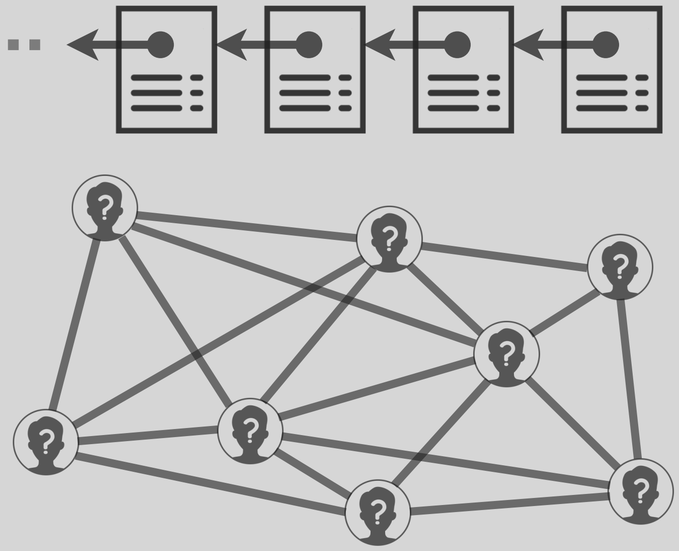
Discovers vulnerabilities in logic, through symbolic execution to capture the traces.

Checks both Source Codes and Byte Codes.
Uses the Blockchain VM with Satisfiability.

Oyente (2016), MAIAN (2017), Zeus , Securify (2018), Vultron (2019)

Privacy

Chain of Layers



Smart Contracts	Anonymity, **Verifiable Computation**
Transaction Recording	**Unlinkability**, Private Verifiability
Consensus Mechanism	Access Control, **Anonymity**
Storage and Database	**Access Control**, Private Retrieval
Peer-To-Peer Network	Data Confidentiality, **Anonymity**

Each layer in a Blockchain architecture has its requirements for Privacy

Attacks

- Smart Contracts
- **Transaction Recording**
- Consensus Mechanism
- Storage and Database
- Peer-To-Peer Network

Link Analysis

Primarily Graph Mining tools for Blockchain.

Clusters wallets and addresses in the network by heuristics learned through graph analytics. Use auxiliary data for user De-Anonymization.

Elliptic and ChainAnalysis provide solutions for AML, Law Enforcement.

Prevention

- Smart Contracts
- **Transaction Recording**
- Consensus Mechanism
- Storage and Database
- Peer-To-Peer Network

Anonymity and Unlinkability

Mixing Protocols – CoinJoin, CoinShuffle, etc.
Distributed Mixers – MixCoin, TumbleBit, etc.

Ring/Blind Signatures – Monero, BlindCoin.
Zero Knowledge Proof – ZeroCoin, ZCash, etc.

Linakability works over Tor as well. Monero is still somewhat linkable.

Attacks

- **Smart Contracts**
- Transaction Recording
- Consensus Mechanism
- Storage and Database
- Peer-To-Peer Network

Public Data Exploits

Attacker exploits the known inputs to invoke the Smart Contracts, posted by participants.

Example: Second-Price Auction with Bidders. Attacker can out-smart other bidders to Win.

Transactions in case of Smart Contracts are the Contracts and Inputs.

Prevention

- **Smart Contracts**
- Transaction Recording
- Consensus Mechanism
- Storage and Database
- Peer-To-Peer Network

Privacy-Preserving Contracts

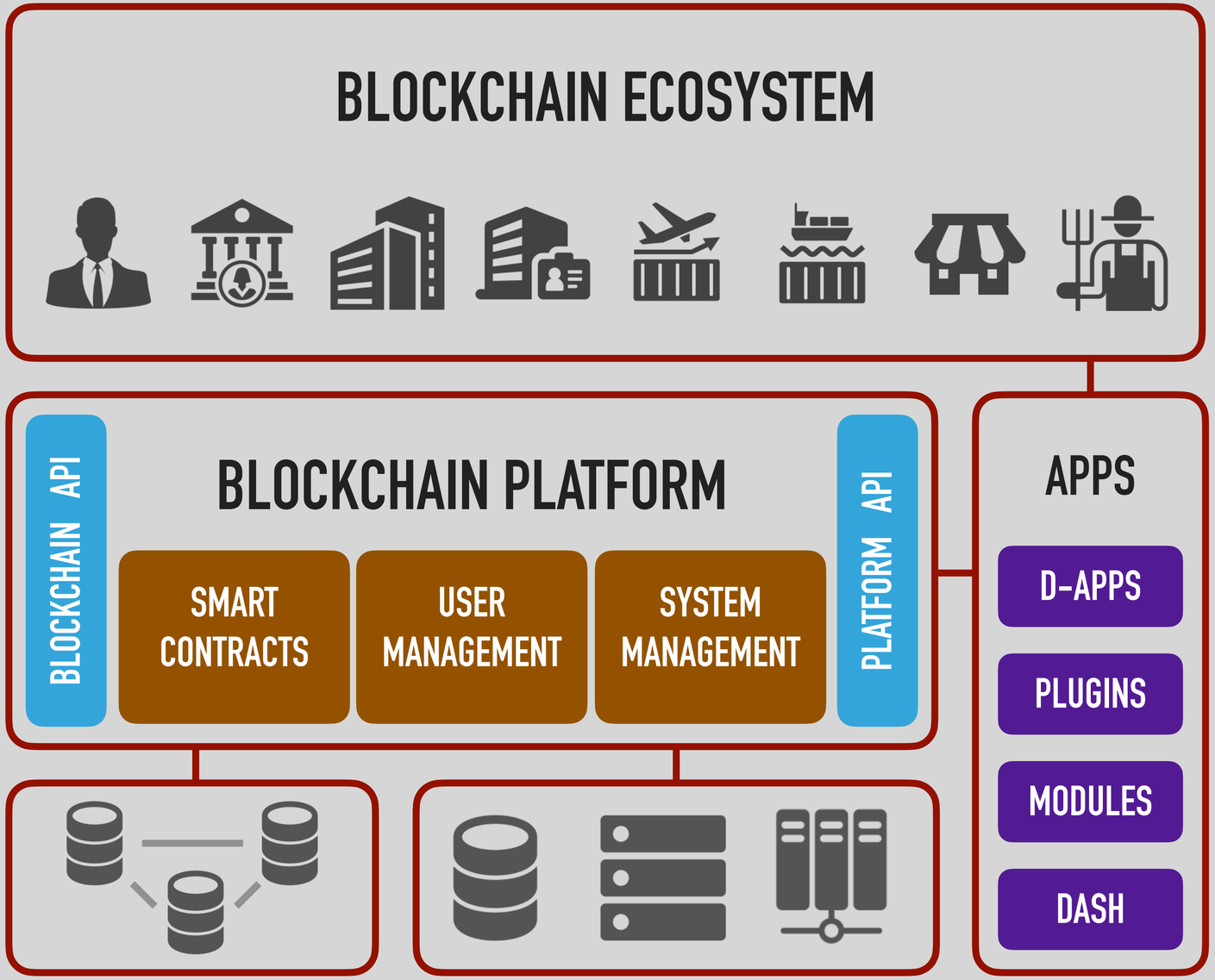
Uses zk-SNARK – Zero-Knowledge Succinct Non-Interactive ARgument of Knowledge

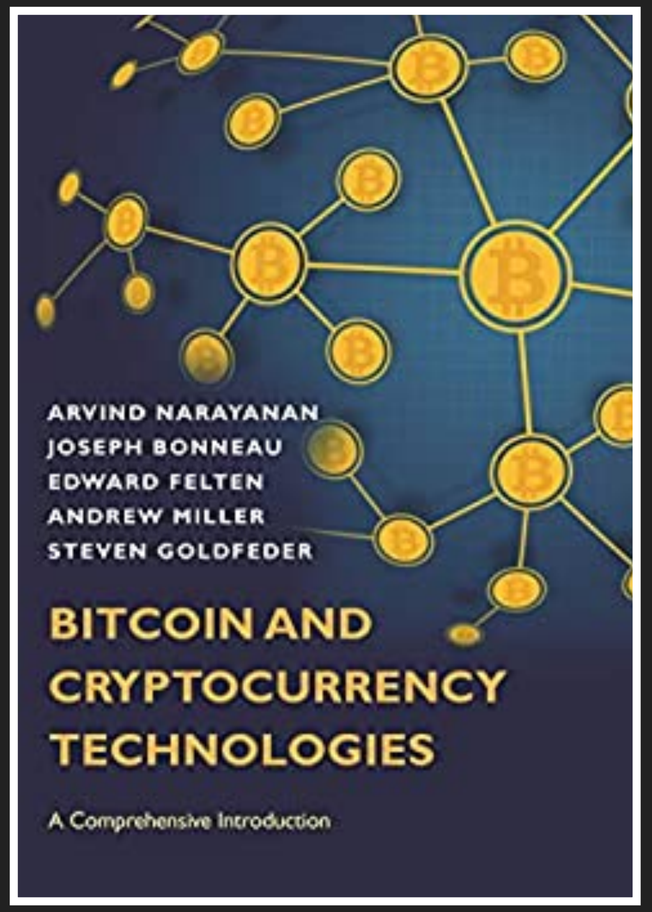
Pinochhio (2013) – Verifiable Computation
Bulletproofs (2018) – zk-SNARK using MPC

NuCypher : Proxy Re-Encryption and Fully Homomorphic Encryption

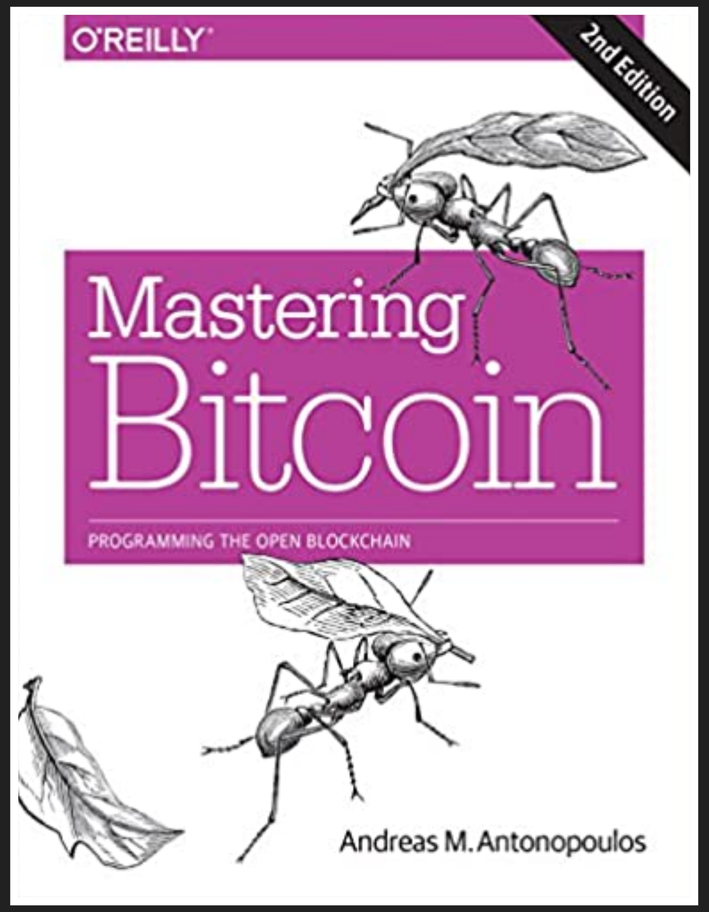
Pen-Tests?

- Smart Contracts
- Transaction Recording
- Consensus Mechanism
- Storage and Database
- Peer-To-Peer Network





for an ACADEMIC



for a DEVELOPER

If you have

more time to kill ...

for almost ANYONE