The Basic Building Blocks of a Blockchain Application

May 2018

In memory of our father

By

Nikola Kotarov
Orlin
Svetoslav Kotarov
Violeta Gotcheva

Outline

A. The problem with Safety Certification Quiz Application

B. What is a blockchain?

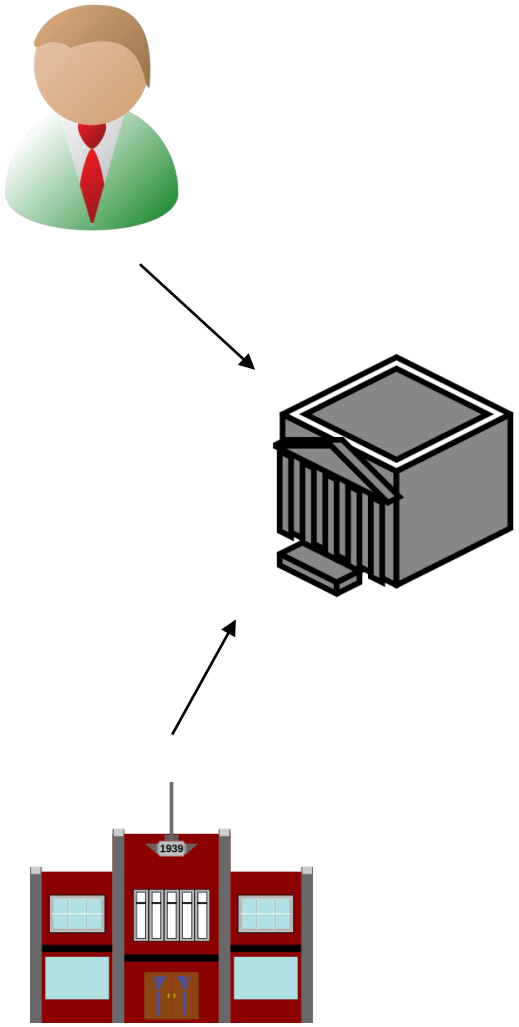
C. Blockchain Terminology
- C1. Assets and Identities
- C2. Transactions
- C3. Digital Signatures
- C4. Cryptography Hashes

D. The Basic Building Blocks of A Blockchain Solution
- D1. Immutable
- D2. Trustless
- D3. Secure
- D4. Private
- D5. Autonomous

E. Summary

A. The problem …

Employee



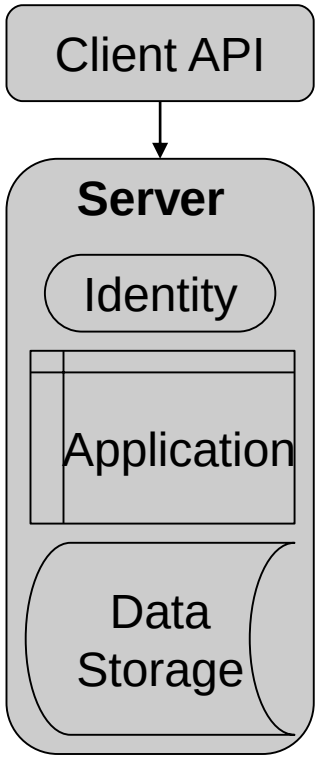
Employer

Employer grants building access if employee is health and safety certified

Certification Authority

- Issue certificate
- Protect the integrity of the certificates
- Validate the certificates when requested

A. The Problem: Health and Safety Training Record




```
mysql> select * from safety_results where
trainee='violet';
+----+----------+----------+-------------------------+
| id | trainee  | score    | input_date              |
+----+----------+----------+-------------------------+
|  1 | violet   |       24 | 2015-05-07 16:38:15|
+----+----------+----------+-------------------------+
1 row in set (0.00 sec)
```

Can we protect the record better?

https://bitcoin.org/bitcoin.pdf

Naivecoin: a tutorial for Building a cryptocurrency
https://lhartikk.github.io/

Bitcoin: A Peer-to-Peer Electronic Cash System

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

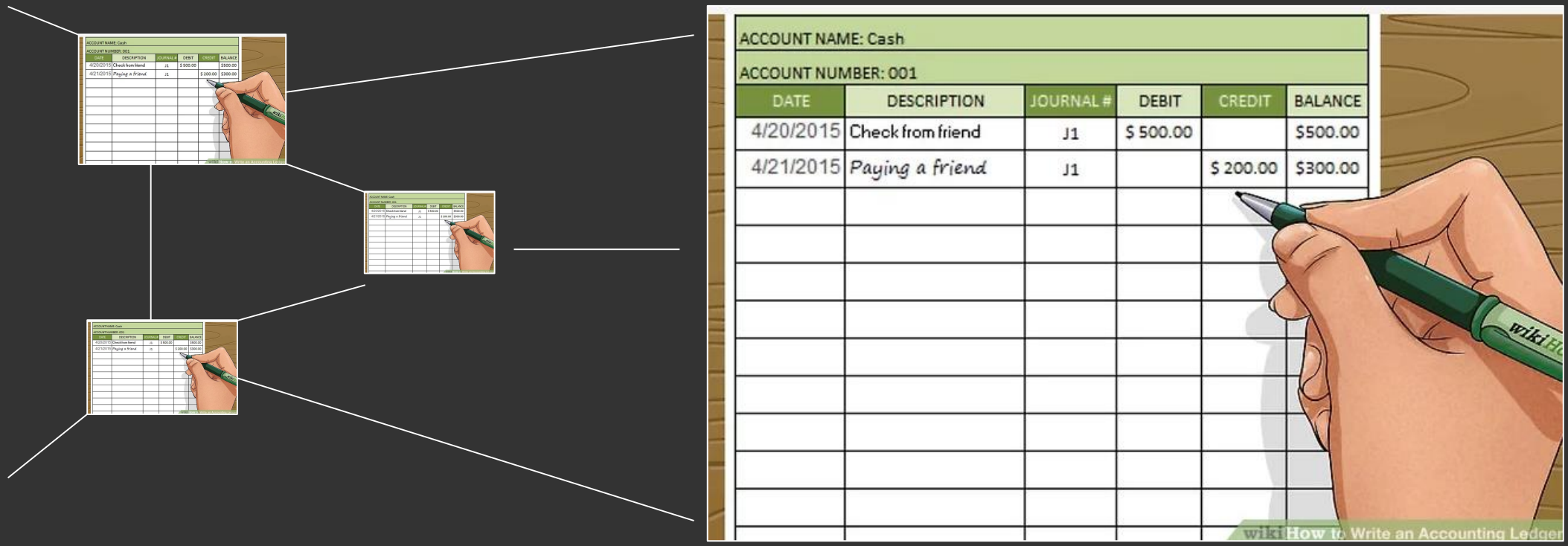
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

B. What is a blockchain?

A Distributed Ledger



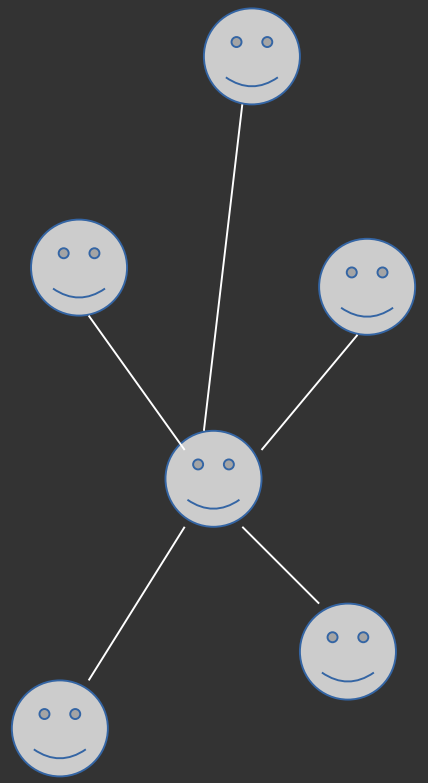
ACCOUNT NAME: Cash

ACCOUNT NUMBER: 001

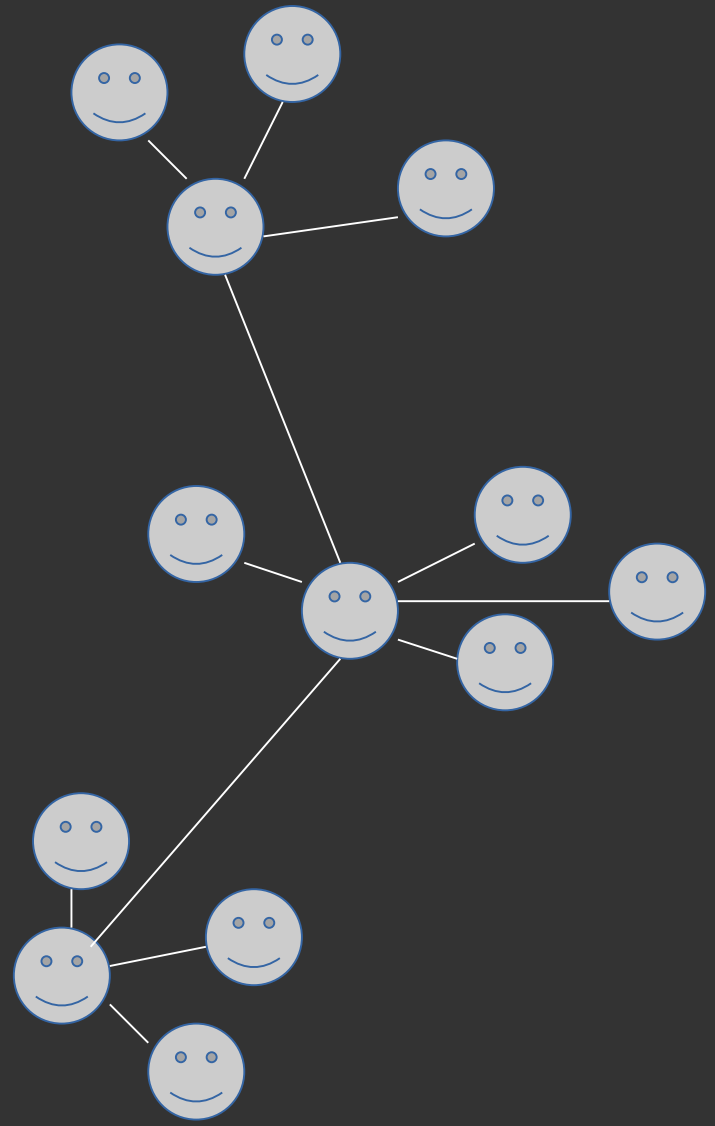
DATE	DESCRIPTION	JOURNAL #	DEBIT	CREDIT	BALANCE
4/20/2015	Check from friend	J1	$ 500.00		$500.00
4/21/2015	Paying a friend	J1		$ 200.00	$300.00

From https://www.wikihow.com/Write-an-Accounting-Ledger

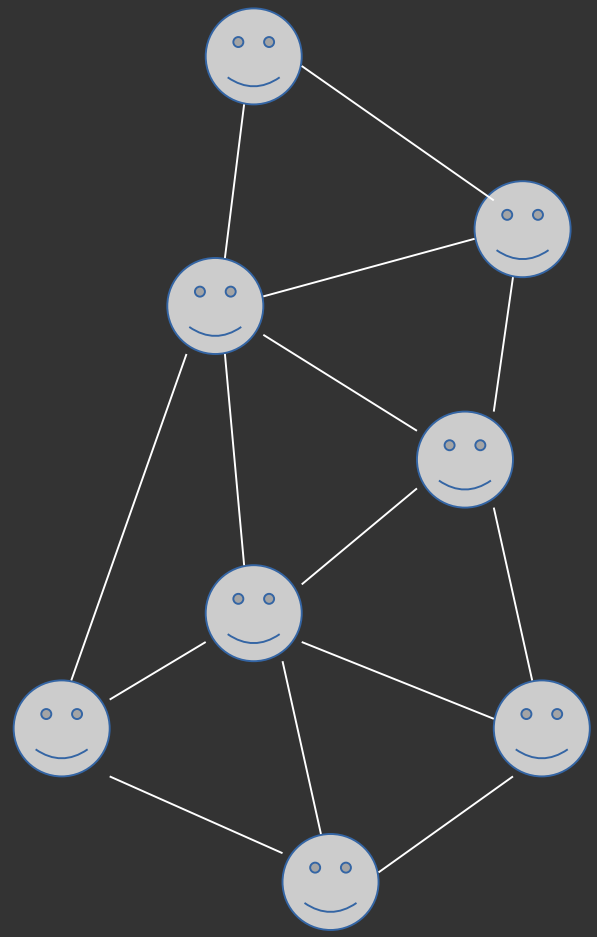
Centralized



Decentralized



Distributed



B.Public and Private networks

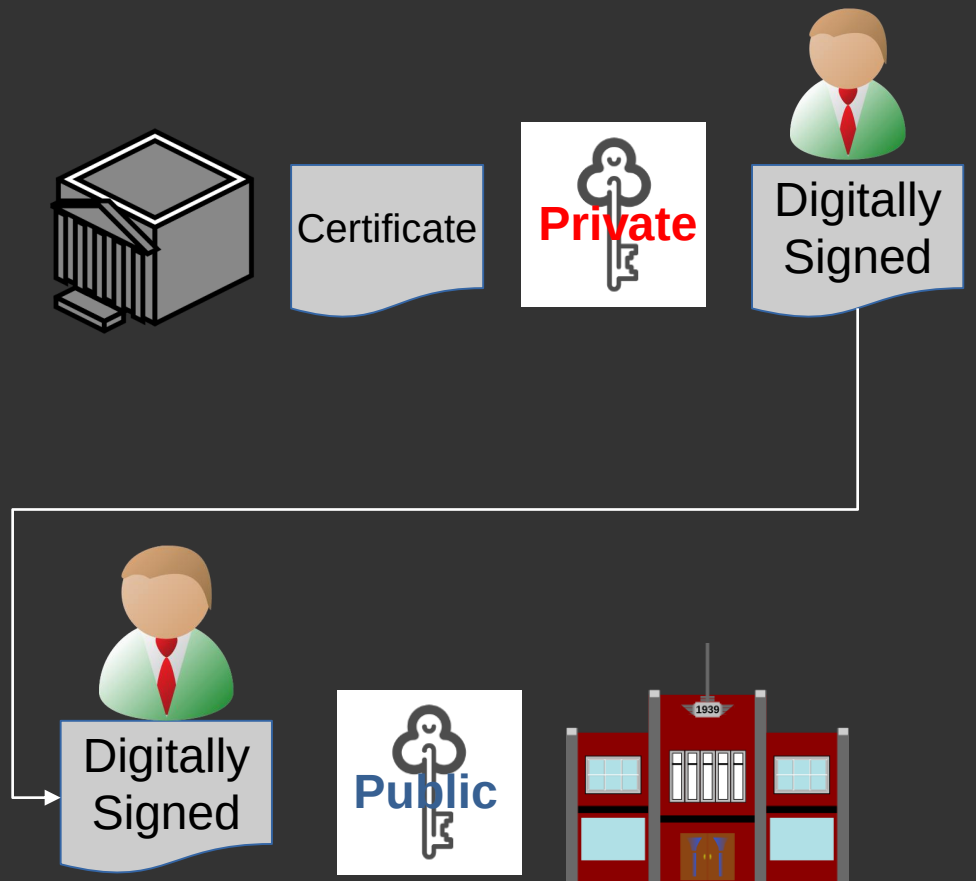
Public Permissionless	Private Permissioned
Bitcoin	HYPERLEDGER
Ethereum	HYPERLEDGER FABRIC
	HYPERLEDGER SAWTOOTH

C.Blockchain terminology – Assets and Identities

An **asset** is the certificate.

Public/Private keys are used to identify employer and employee

C.Blockchain terminology – Transactions and Signatures



The issuance of the certificate is a transaction.

The transactions are digitally signed

C.Blockchain terminology – Cryptography Hashes

Integrity is protected by secure hashes

Message with arbitrary length

violet | 24 | 2015-05-07

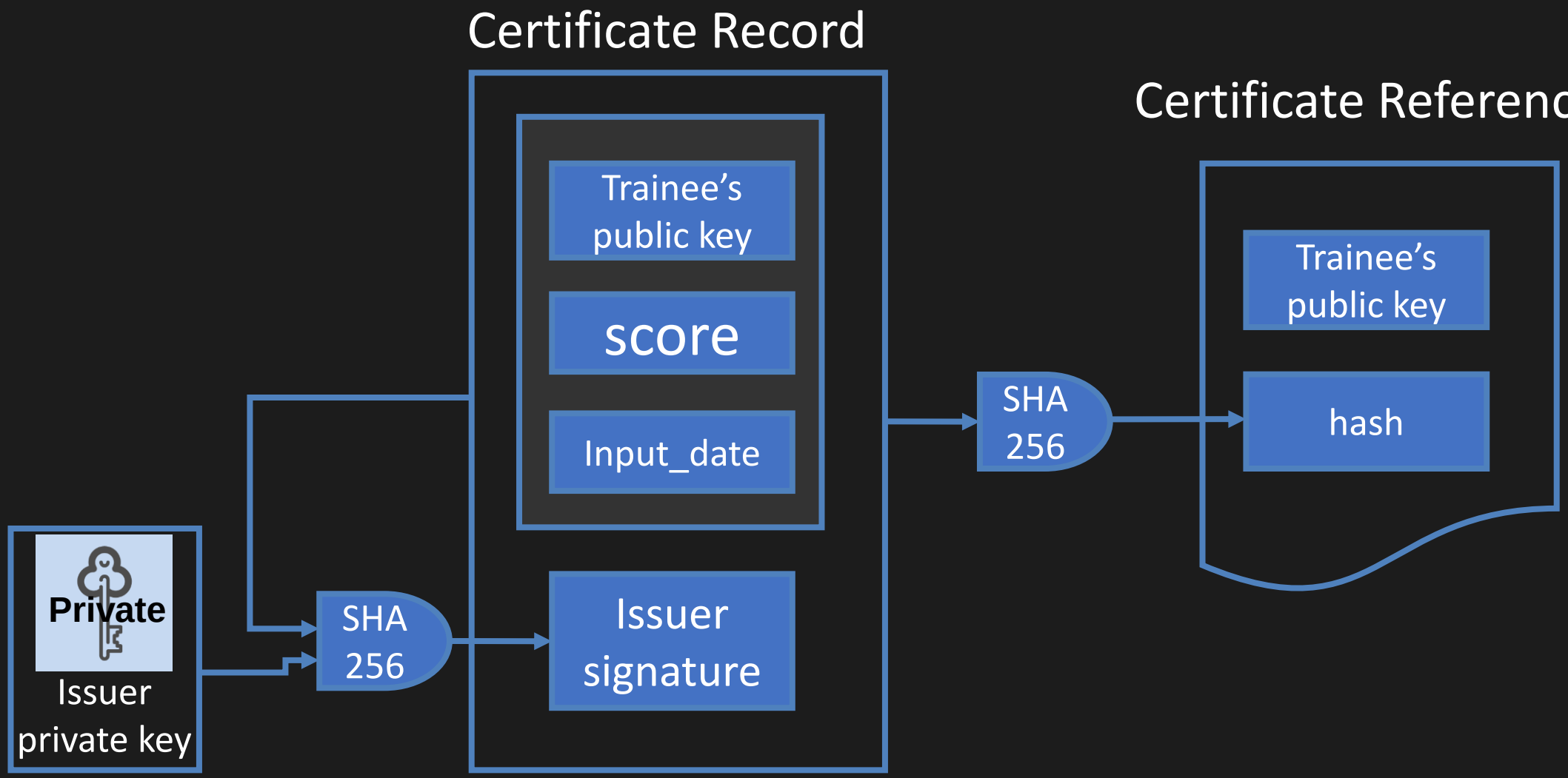
Hash value with fixed length

a623246fe526351ca78bf28d67d432d5f01789fda188910bd23fb9482e21f5cc

can we create an immutable ledger?

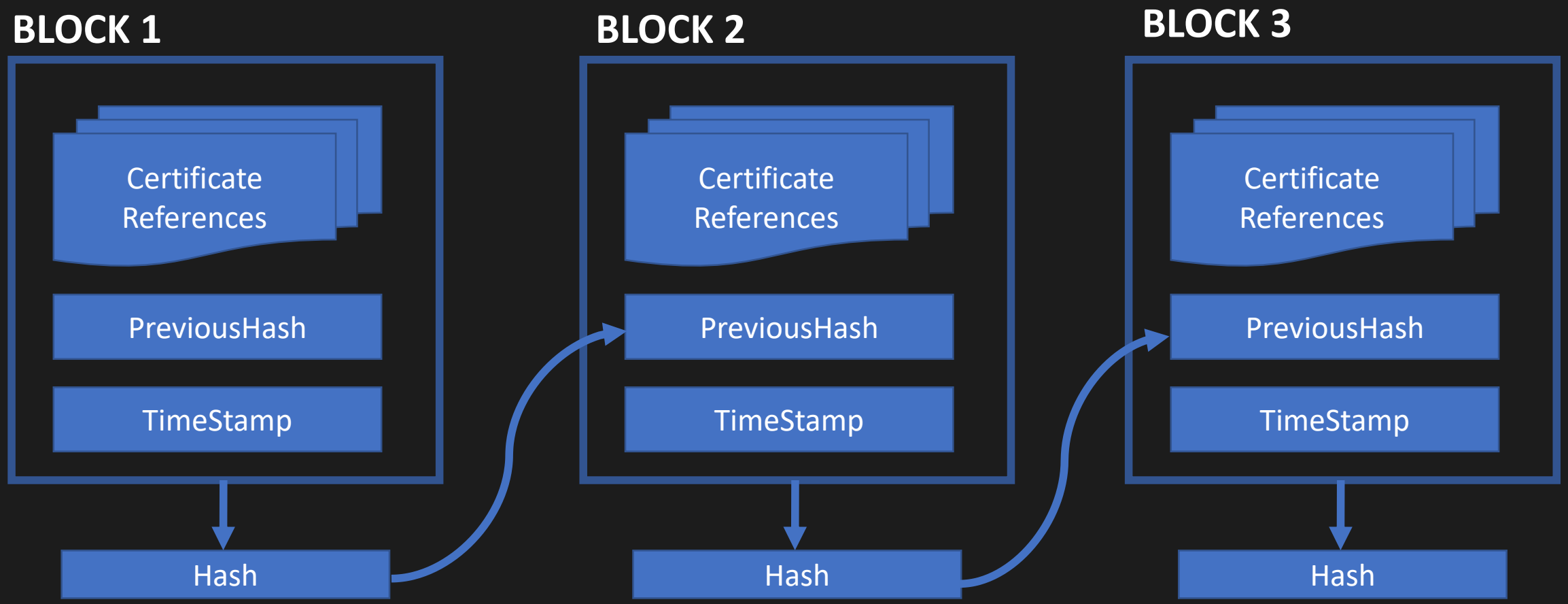
the blockchain (ledger) is
immutable

D1.Immutable: Create a Reference Record for each (digital) Asset



D1.Immutable: Chain of Blocks

And all validated transactions are permanently stored in the data blocks which cannot be altered or deleted by anyone.

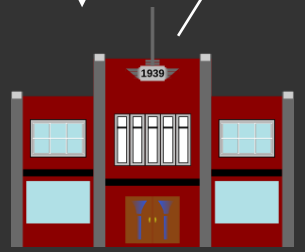


how do we trust the source(s) with the integrity of the records?

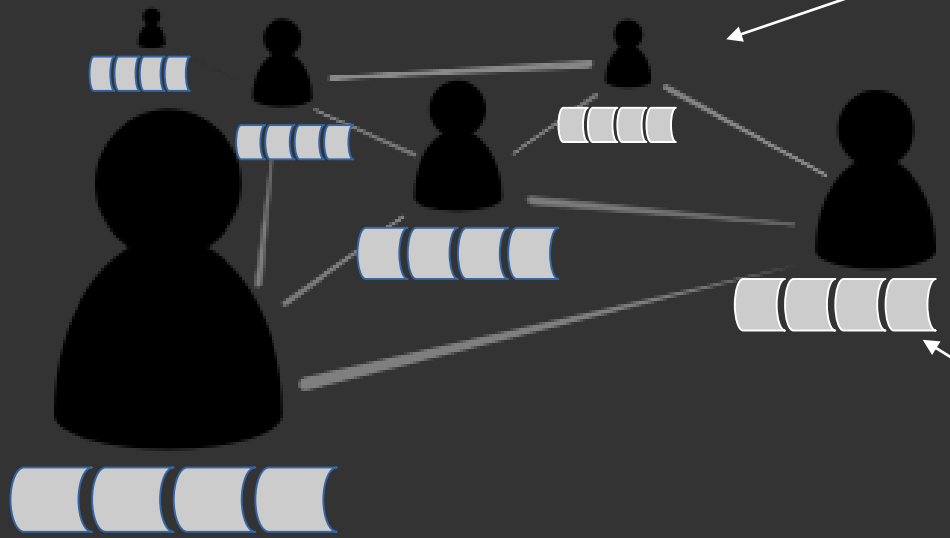
the blockchain (ledger) is **trustless.**

D2.Trustless: A distributed network of peer nodes each maintaining an identical copy of the blockchain

Traditional
Certification
Authority



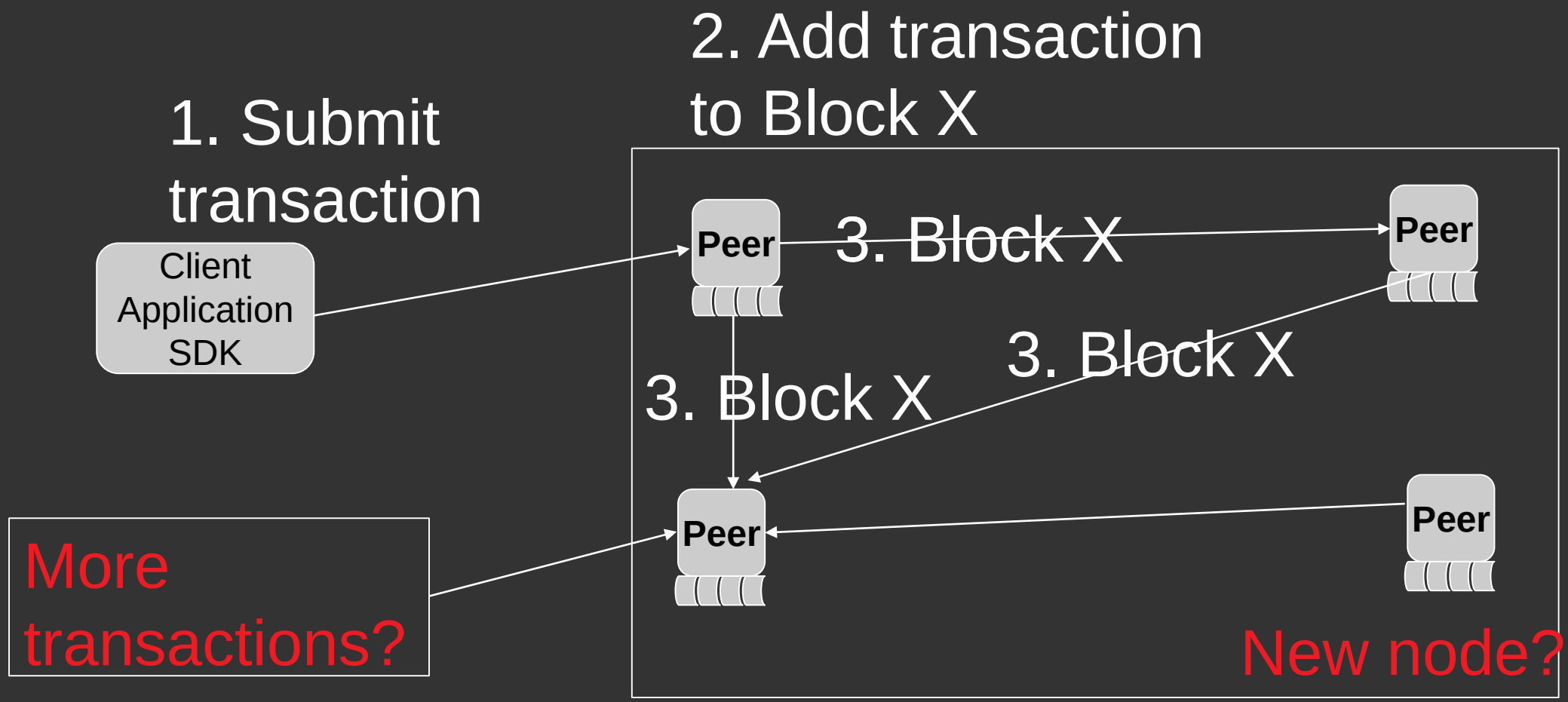
Blockchain
No intermediary



D2.Trustless : Rai stones used as money on the pacific island of Yap

https://youtu.be/A-L2M0l5dEY?t=30s

D2.Trustless: Blockchain peers do not trust each other



how do peers sync the different copies of the blockchain?

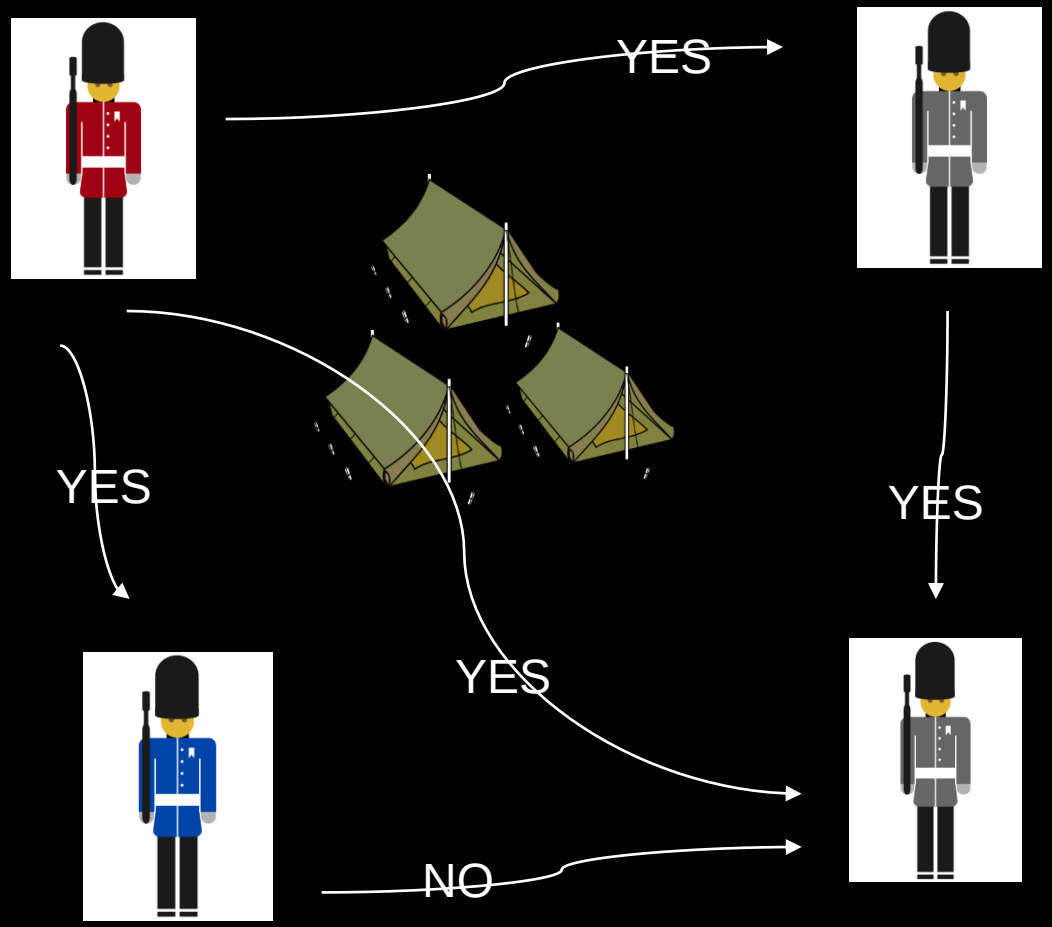
The blockchain ledger is
secure

D3.Secure: Consensus about the truth

- **The technology relies on a consensus from all network members for the validation of a transaction.**

- **A decentralized system makes it difficult for hackers to breach the transaction by targeting one unit, a common pain point in a centralized system where the data is stored at a single core.**

D3. Secure: Byzantine Fault Tolerance Consensus Algorithm



Byzantine General's Problem

https://www.youtube.com/watch?v=_MwqAaVweJ8

51% attack

https://youtu.be/DHa5w1jWGuw

D3.Security: Consensus by Proof of work (POW)

Bitcoin POW

scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits.

Mining

Representation in majority decision making
One CPU = One VOTE

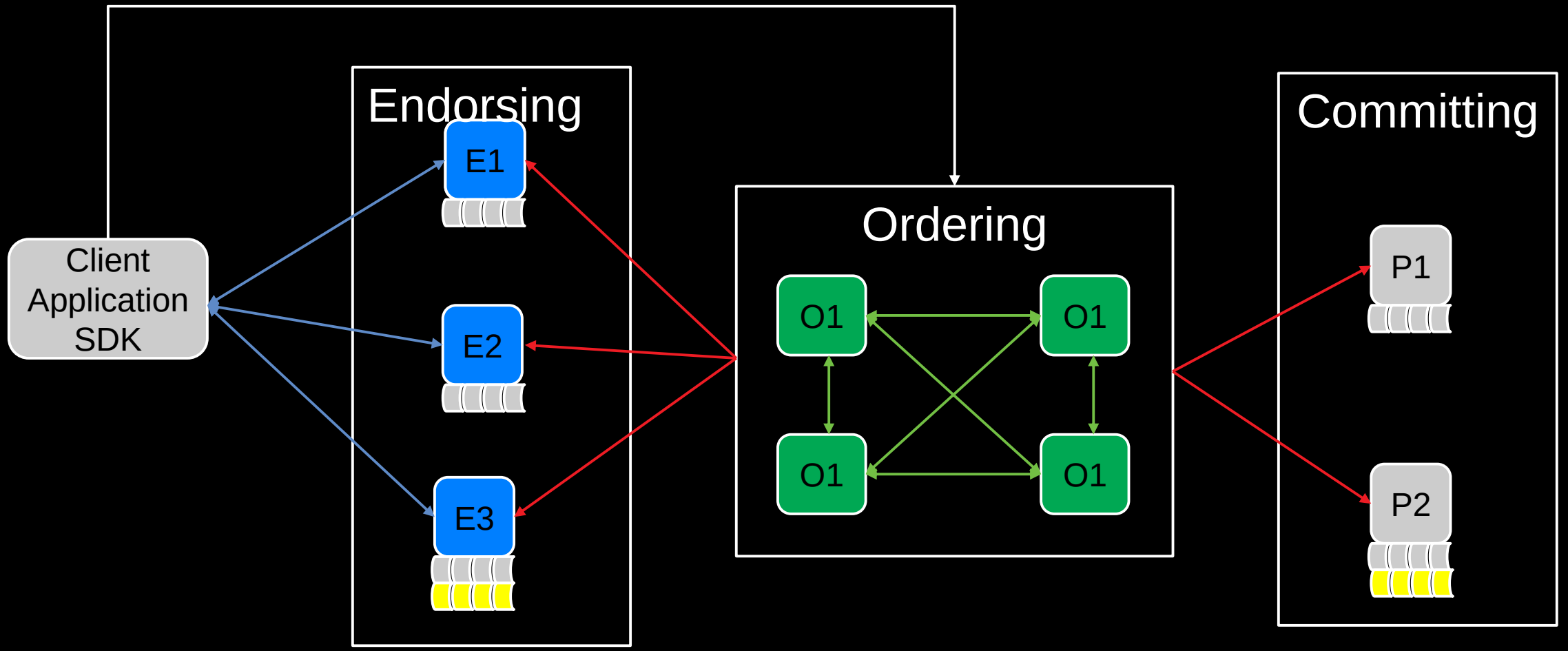
Useful Proof-of-Work

Primecoin requires clients to find unknown prime numbers of certain types, which can have useful side-applications
https://bitcoinmagazine.com/articles/primecoin-the-cryptocurrency-whose-mining-is-actually-useful-1373298534/

The majority decision is represented by the longest chain

D3.Security: Consensus in Hyperledger Fabric (private, permissioned blockchain)

Consensus = Transaction Endorsement + Ordering + Validation

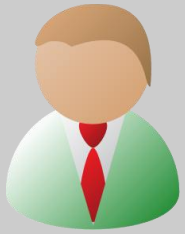


From https://docs.google.com/presentation/d/1p-5obfijoC1gBn9_FcUfOI7QytX8Oacekz9THd4-e00/edit#slide=id.p25

D4.the blockchain (ledger) can guarantee privacy

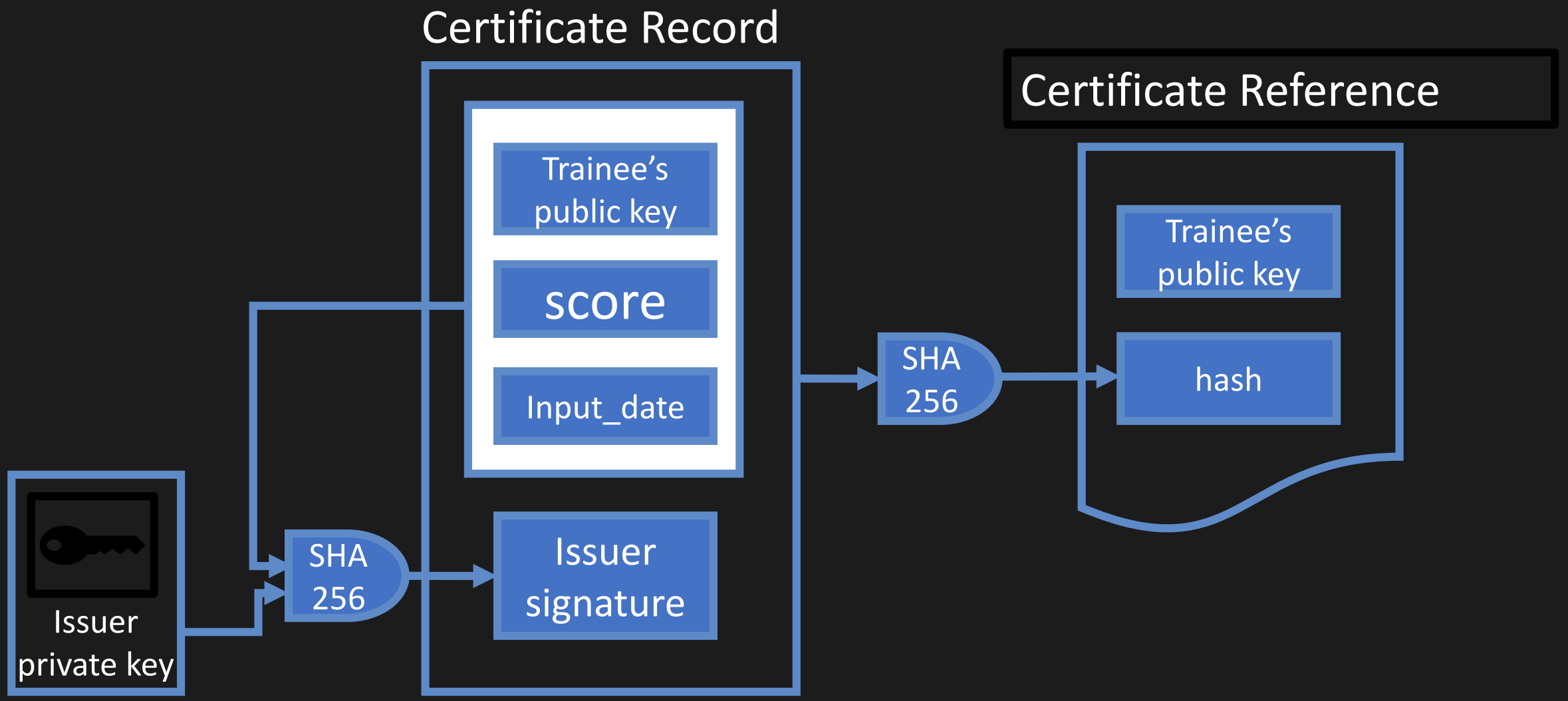
The Certificate is public

The Certificate contains personal data



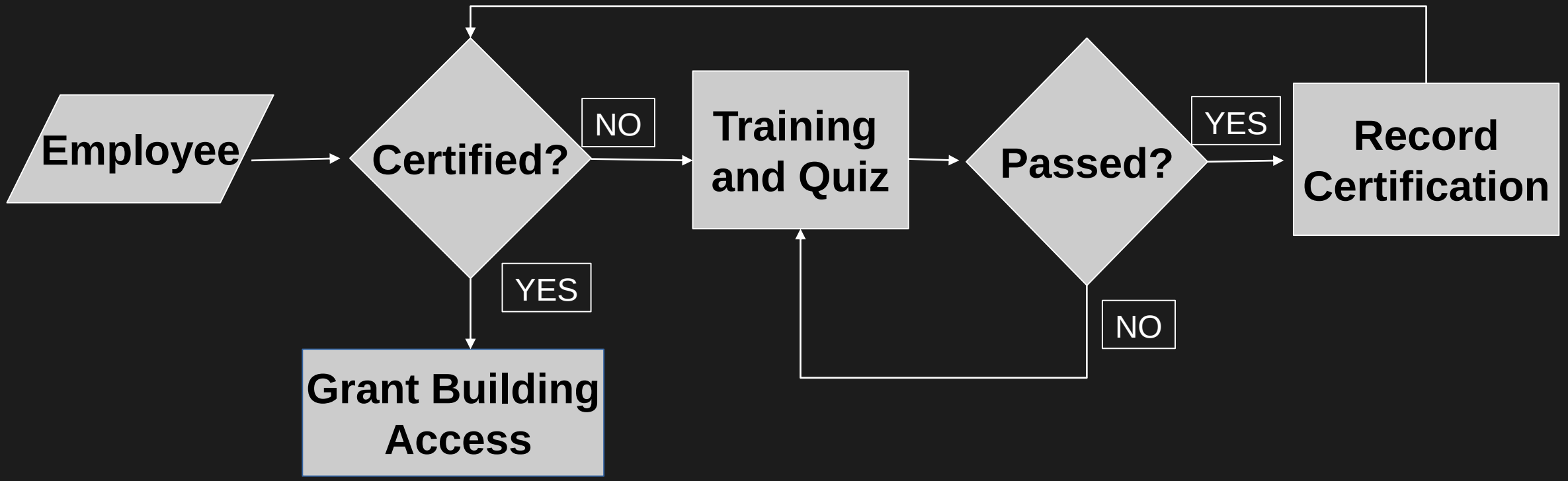
How can the owner choose what to share with whom?

D4.Private: Zero knowledge proofs



The blockchain ledger is **autonomous**

D5.Employer grants building access if employee has a health and safety certification



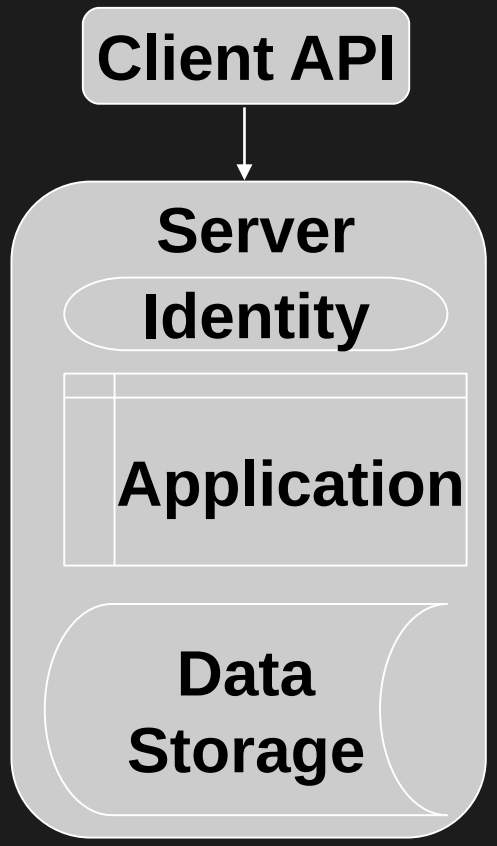
Autonomous: Smart Contracts

Computer code on the blockchain • Business relationship • Automatic execution

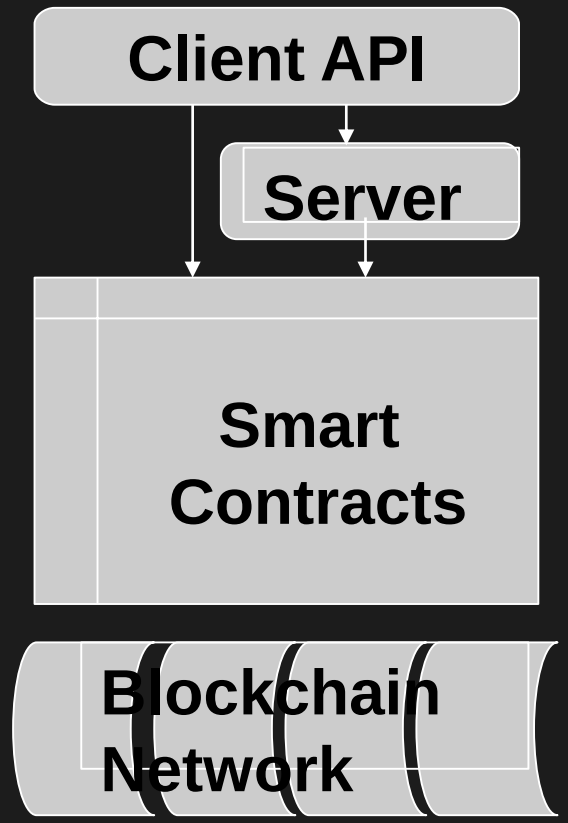
Don’t we already run computer code with business logic and automation?

D5.Autonomous – Smart Contracts

Traditional



Blockchain



32/36

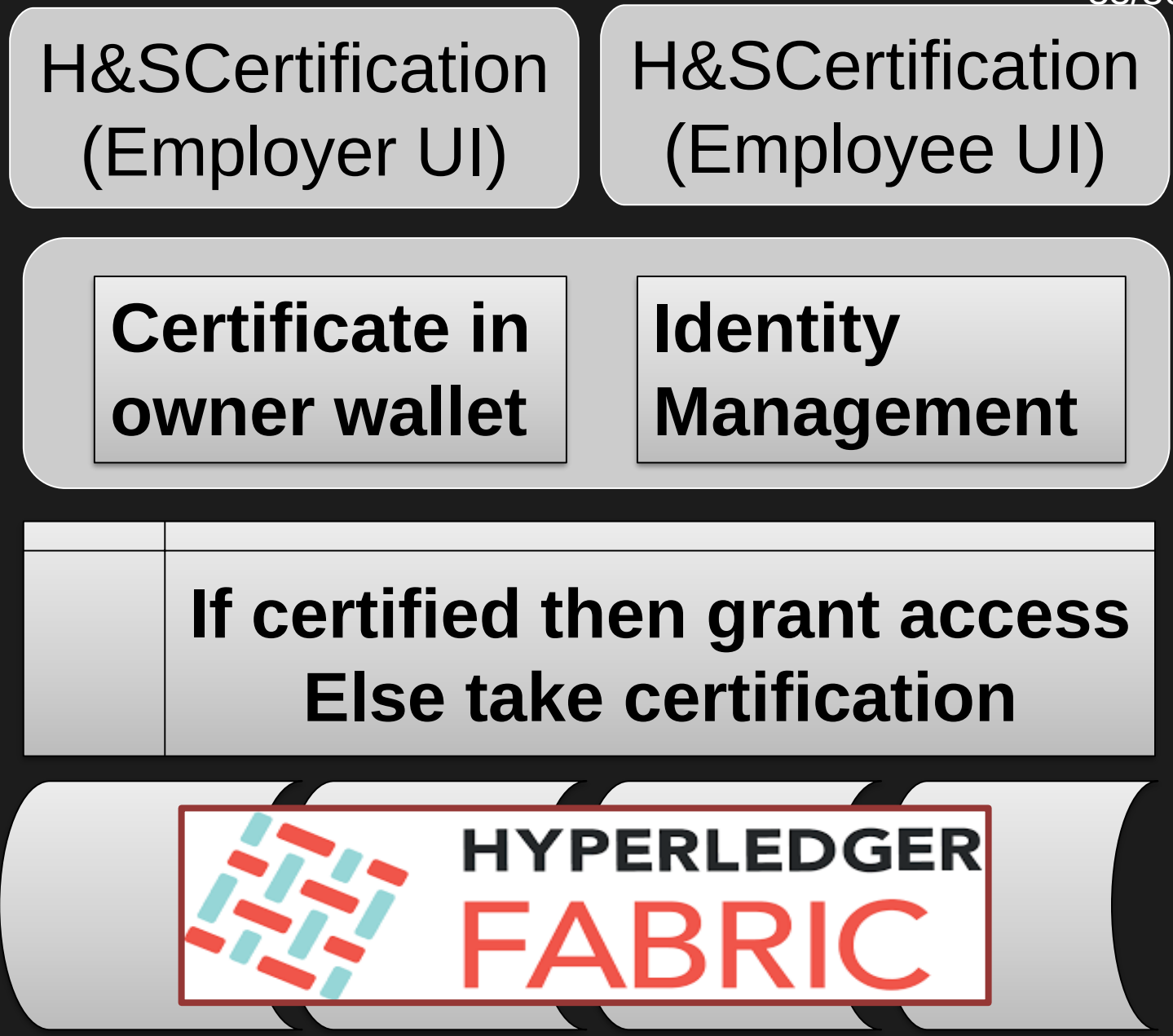
Catena

gun

LotionJS

COSMOS
INTERNET OF BLOCKCHAINS

E. Summary: The Solution …



E: Summary: cryptocurency?

“Public, decentralized networks require high levels of security and spam-prevention that are best achieved by economic means: participants in the consensus must incur some economic cost, and all transactions processed by the network must pay a fee. “

From: https://cosmos.network/faq

E. Summary: Beyond mining

How many prospectors got rich during the California gold rush?

E. Summary: Beyond Cryptocurrencies

Immutable
thrustless
Secure
Private
Autonomous

Identity Management
Academic Certification
Talent Recognition
Supply chain traceability
Voting
Land Registration
Health Care
Voting
Corporate registration
Energy trading

From
https://www2.deloitte.com/insights/us/en/industry/public-sector/understanding-basics-of-blockchain-in-government.html