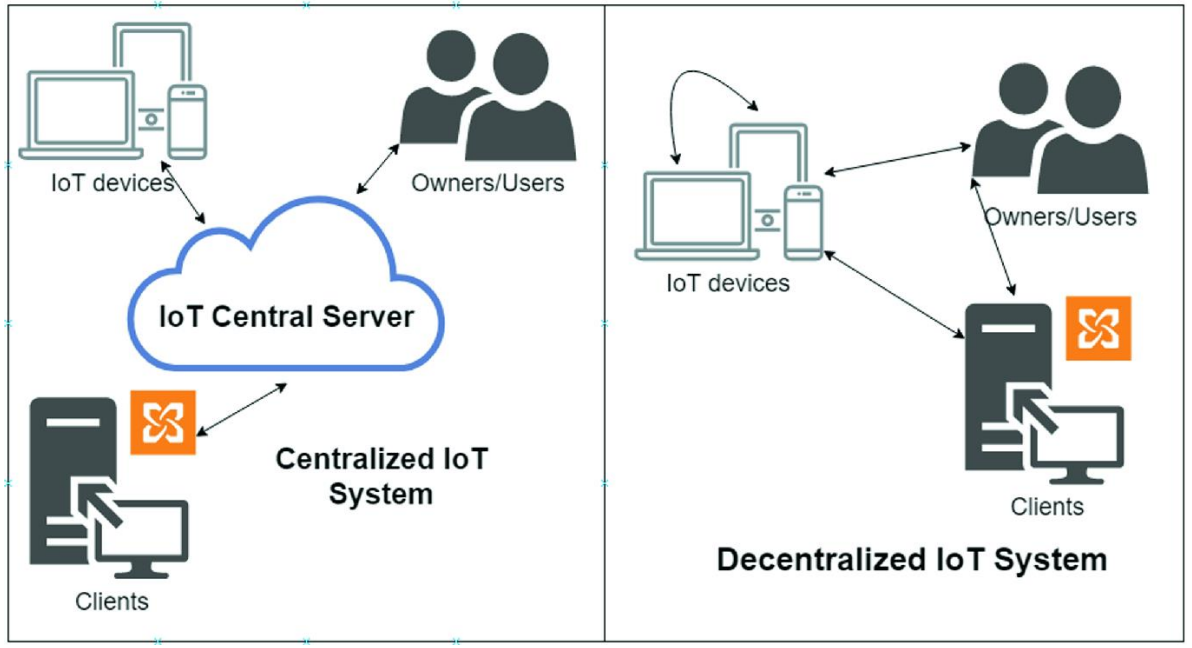
Non-standard applications of blockchain technology

Bc. Matúš Revický

Supervisor: doc. RNDr. Jozef Jirásek, PhD.

Problem Statement

- Traditional databases are susceptible to attacks, where an attacker can **permanently change or delete data** inside the database.
- Assumption that devices that are connected trust each other
- Hard to know which device to trust in the network.
- Need for a solution that can store data about every transaction in an environment where participants do not fully trust one another, and the data needs to be resistant to cyber-attacks.
- **Desired solution: Involved parties have access to data that can be trusted**.



Goals and motivation

- Review relevant literature about applications of blockchain technology not only in cryptocurrencies.
- Evaluate distributed trust models and capabilities of existing blockchain frameworks.
- Design of decentralized system that is suitable for the heterogeneous nature of IoT devices by employing a viable trust model (housing providers)
- Implement and evaluate a proof of concept in a real life scenario that could benefit from utilizing IoT devices.

Blockchain - Real world uses cases

GOVERNMENT

Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

essentia.one

HEALTHCARE

A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**

MEDREC

MOBILE PAYMENTS

The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

ripple

SUPPLY CHAINS

IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.

IBM

Walmart

IDENTIFICATION

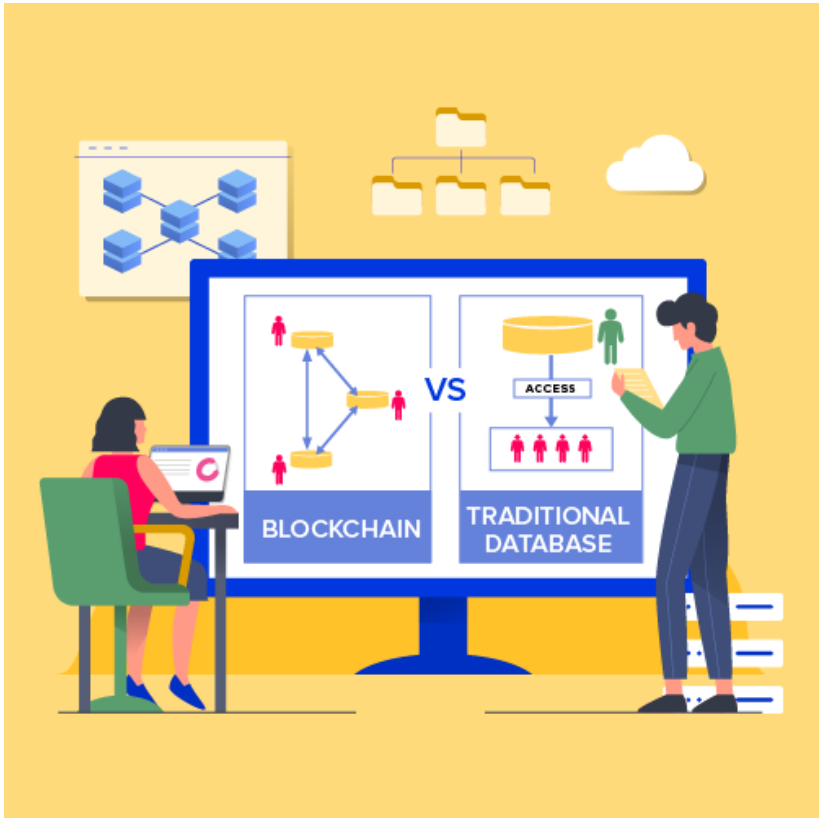
Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport.**

uport

SHIPPING

Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.

MÆRSK



Where blockchain could provide value

Situations that favor the use of blockchain technology include

- when multiple parties are sharing and updating shared data,
- there is a need for reliable records,
- there are intermediaries that add costs, and/or
- there is a lack of trust between involved parties.

Some of the **blockchain's key advantages** include disintermediation, improved product traceability, increased transparency of transaction histories, as well as enhanced security of records regarding fraud and unauthorized activities.

Types of Blockchain

Table 1. Classification of Blockchains

Types	Describe	#TA	SoC	Scenarios
Public Blockchain	Anyone can participate and is accessible worldwide	0	Slow	Global decentralized scenarios
Consortium Blockchain	Controlled by pre-selected nodes within the consortium	≥ 1	Slight Fast	Businesses among selected organizations
Private Blockchain	Write rights are controlled by an organization	1	Fast	Information sharing and management in an organization

Existing blockchain frameworks comparison

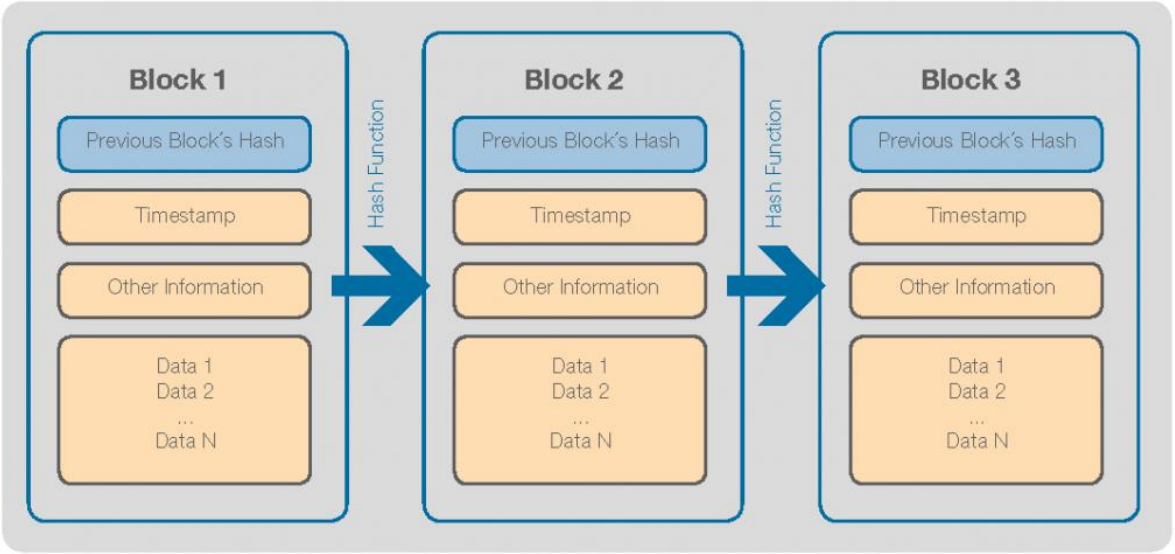
Characteristics	Ethereum	Hyperledger Fabric	R3 Corda
Programming Language	Solidity	Go, Java	Kotlin
Governance	Distributed among all participants	Linux foundation and organisation in the Chain	R3 and organisations involved.
Smart Contract	Not legally bounded	Not legally bounded	Legally bounded
Consensus Algorithm	PoW. Casper implementation PoS.	PBFT	Notary nodes can run several consensus algorithm
Scalability	Existing scalability issue	Not prevalent	Not prevalent
Privacy	Existing privacy issue	Not prevalent	Not prevalent
Currency	Ether	None Can be made using chaincode	None

Blockchain

Distributed, immutable database:

- **Cryptographic Digital Signature**
- **Distributed Ledger**
- **Consensus algorithm**

Consensus algorithm/ blockchains	Number of transactions per second	Confirmation latency	Features
Proof-of-Work (PoW)/ Bitcoin, Ethereum	Tens	6–60 min	High security Low throughput Low scalability
Proof-of-Stake (PoS)/ Peercoin	Tens	10–60 min	High security Low throughput Low scalability
Byzantine fault tolerance (BFT)/Hyperledger	Thousands	1–60 s	Low security High throughput High scalability
Delegated Proof-of-Stake (DPoS)/EOS	Thousands	<1 s	Low security High throughput High scalability
Proof-of-Formulation (PoF)/FLETA	More than 10,000	<1 s	High security High throughput High scalability



Key concepts

HYPERLEDGER FABRIC ARCHITECTURAL MODEL

ASSETS

Assets can be anything that holds a monetary value on the system.

CHAINCODE

Chaincode runs separately from transaction orders, which optimizes the network for more security.

LEDGER

It encodes all the transaction history in an immutable ledger. Also, comes with SQL query like capacity.

IDENTITY

Hyperledger Fabric offers a membership identity service that helps to manage all the identities in the permissioned network.

CONFIDENTIALITY AND PRIVACY

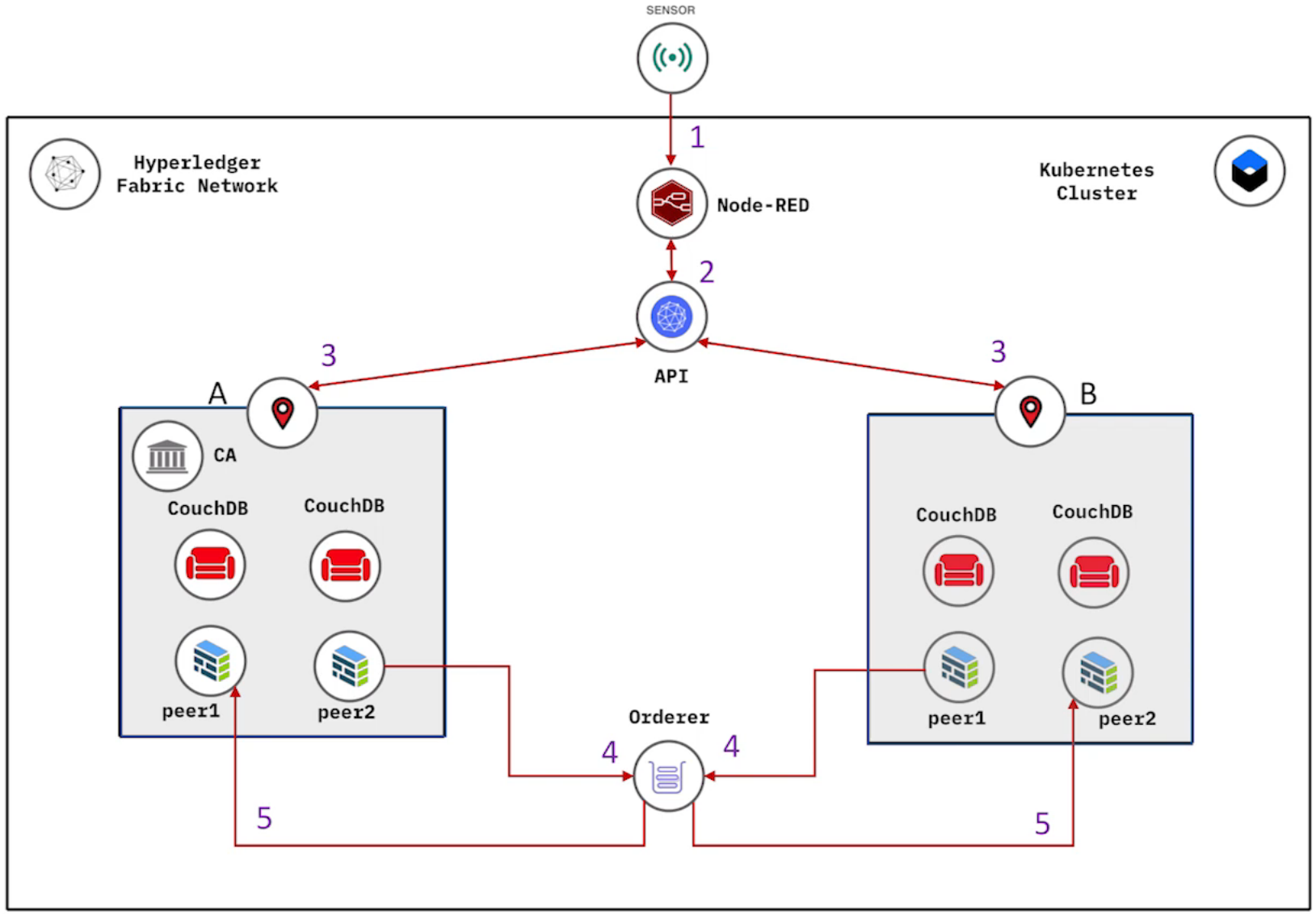
It comes with data restrictions and private transaction facilities.

SECURITY PROTOCOLS

You will get a higher degree of security protocols to safeguard the network from any attacks.

CONSENSUS

A unique approach for reaching consensus makes it perfect for the enterprise-grade solution.


SENSOR
IBM CLOUD
Hyperledger
Fabric Network
Kubernetes
Cluster
1
Node-RED
2
API
3
3
A
B
CA
CouchDB
CouchDB
CouchDB
CouchDB
peer1
peer2
peer1
peer2
Orderer
4
4
5
5

Smart contract

…

```
func (s *SmartContract) getHistory(stub shim.ChaincodeStubInterface, args []string) peer.Response {
        if len(args) != 1 {
                return shim.Error("invalid number of arguments")
        }
        sensorID := args[0]
```

…

Smart contract call from external app

…

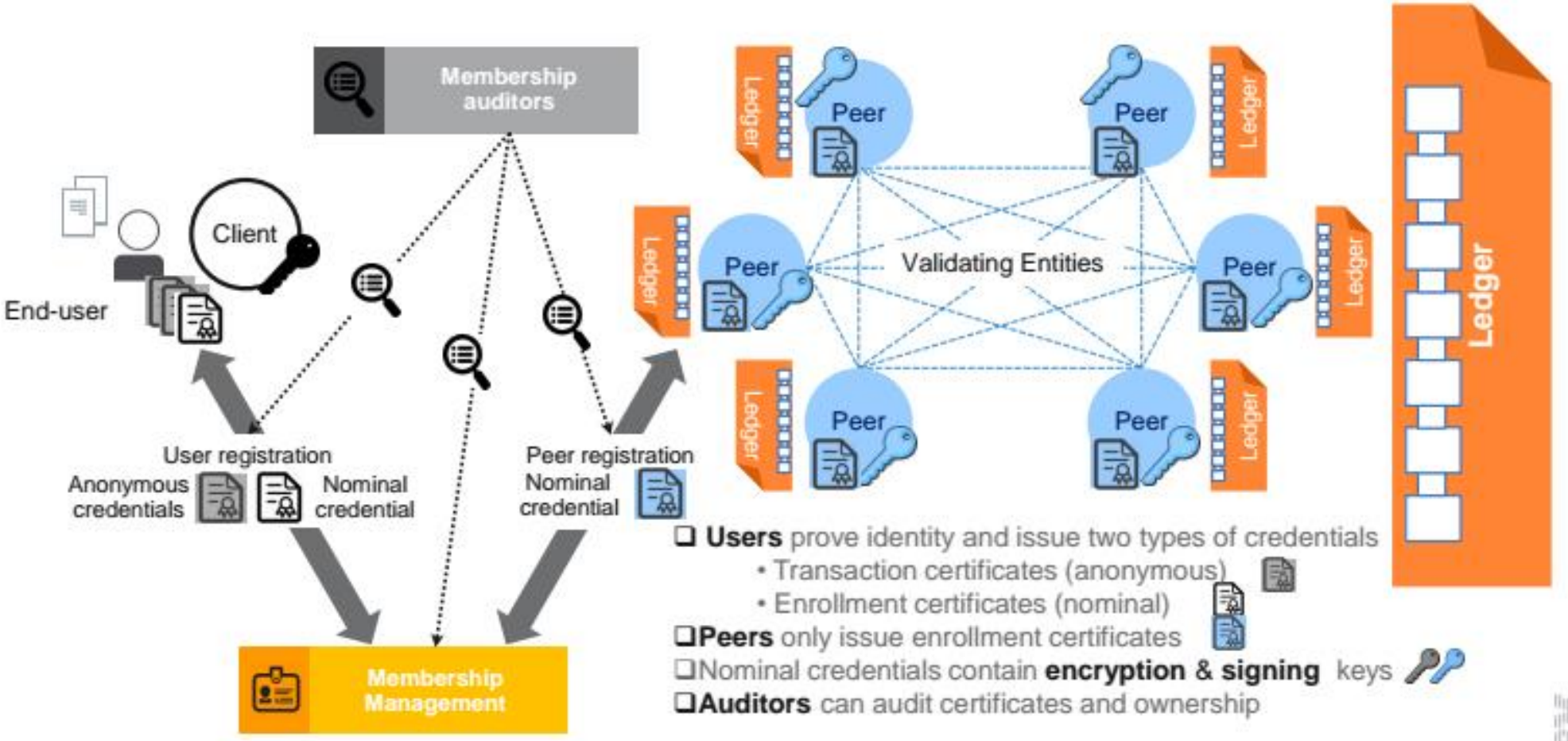
```
// Get the contract from the network.
const contract = network.getContract(smartcontract);

// Evaluate the specified transaction.
// queryCar transaction - requires 1 argument, ex: ('queryCar', 'CAR4')
// queryAllCars transaction - requires no arguments, ex: ('queryAllCars')
const result = await contract.evaluateTransaction('getHistory', args.sensorID);
console.log(`Transaction has been evaluated, result is: ${result.toString()}`);
return result.toString();
```

…

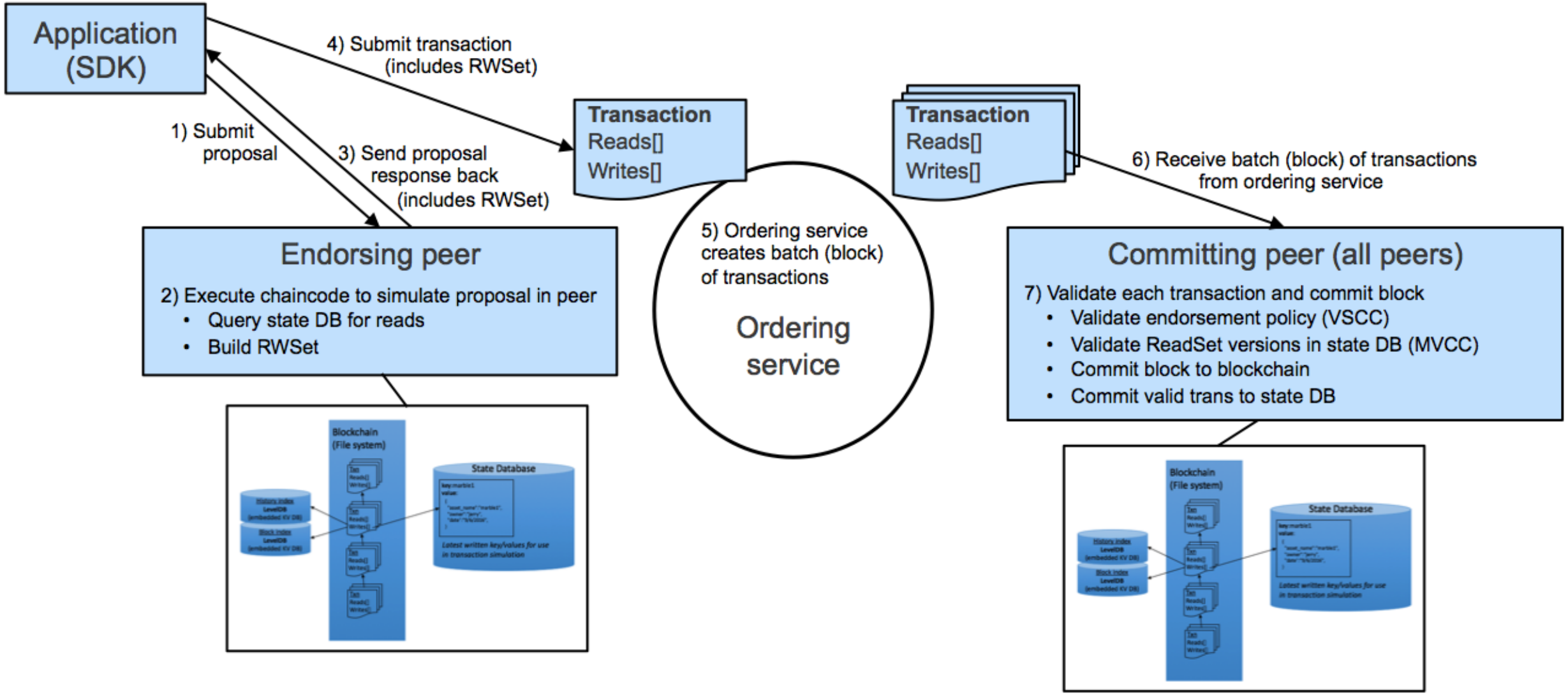
Key concepts

Membership



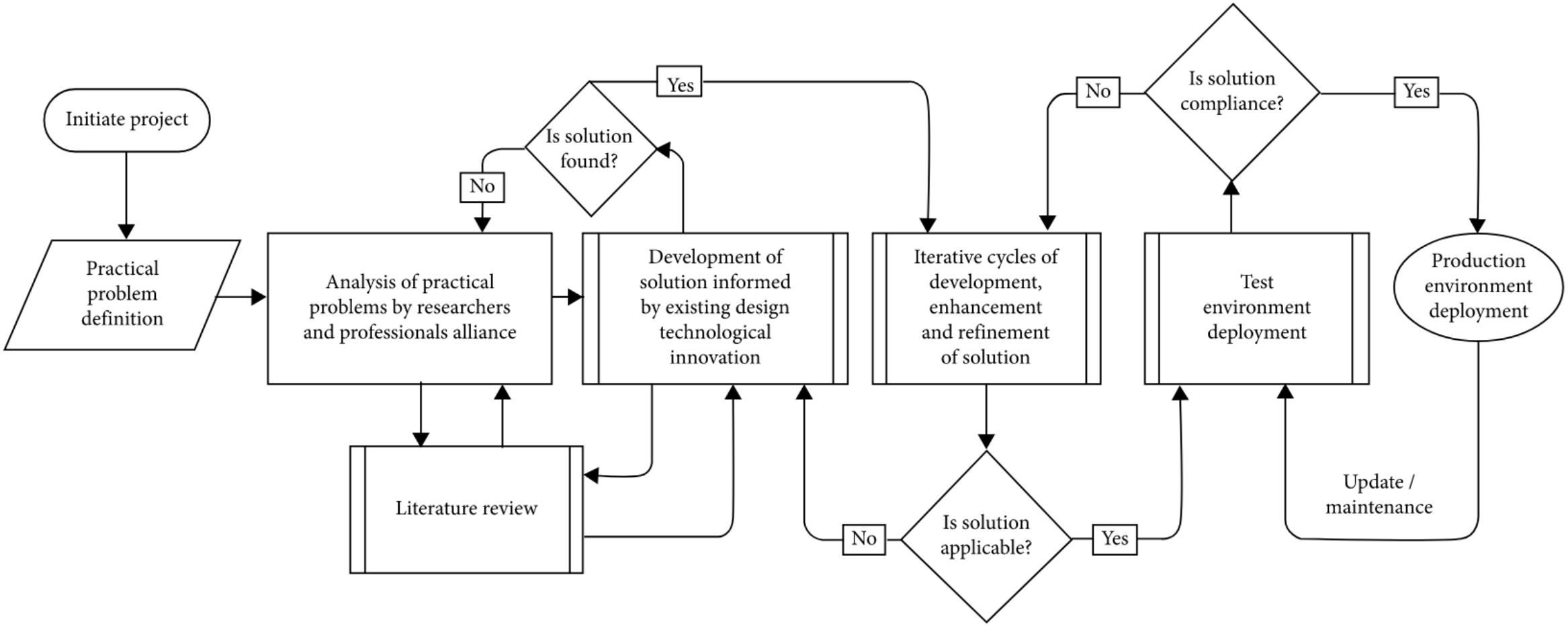
- **Users** prove identity and issue two types of credentials
  - Transaction certificates (anonymous)
  - Enrollment certificates (nominal)
- **Peers** only issue enrollment certificates
- Nominal credentials contain **encryption & signing** keys
- **Auditors** can audit certificates and ownership

Productivity, Scalability, and Level of Trust



Thank you for your attention

Methodology



Zdroje

1. R. Wattenhofer: The Science of the Blockchain, CreateSpace IndependentPublishing Platform, 2016, ISBN-13: 978-1522751830

2. M. Swan: Blockchain: Blueprint for a New Economy, O'Reilly Media, 2015, ISBN-13: 978-1491920497

3. D. Tapscott , A. Tapscott : Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Portfolio, 2016,ISBN-13: 978-1101980132

4. Chris Dannen: Introducing Ethereum and Solidity; Foundations of Cryptocurrency and Blockchain Programming for Beginners, Apress, Berkeley, 2017, ISBN 978-1-4842-2534-9, https://doi.org/10.1007/978-1-4842-2535-6

5. Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen, A Survey onthe security of blockchain systems, In Future Generation Computer Systems, 2017 , ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.08.020.

6. Steve Huckle, Rituparna Bhattacharya, Martin White, Natalia Beloff, Internet of Things, Blockchain and Shared Economy Applications, In Procedia Computer Science, Volume 98, 2016, Pages 461-466, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2016.09.074.