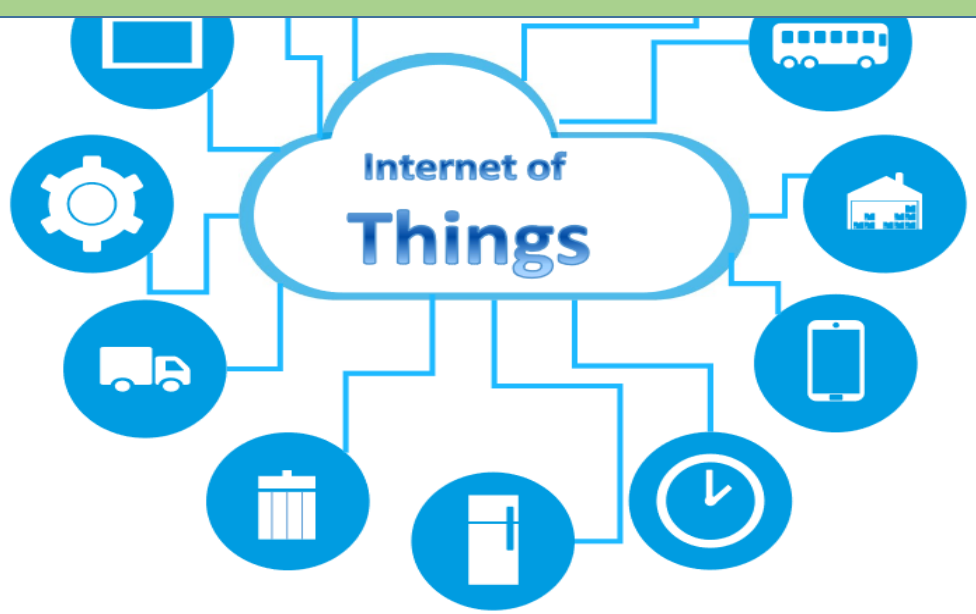
Blockchain for the Internet of Things

Bacem Mbarek, Ph.D.
Masaryk University, Czech Republic
Lasaris Lab (Lab of Software Architectures and Information Systems)

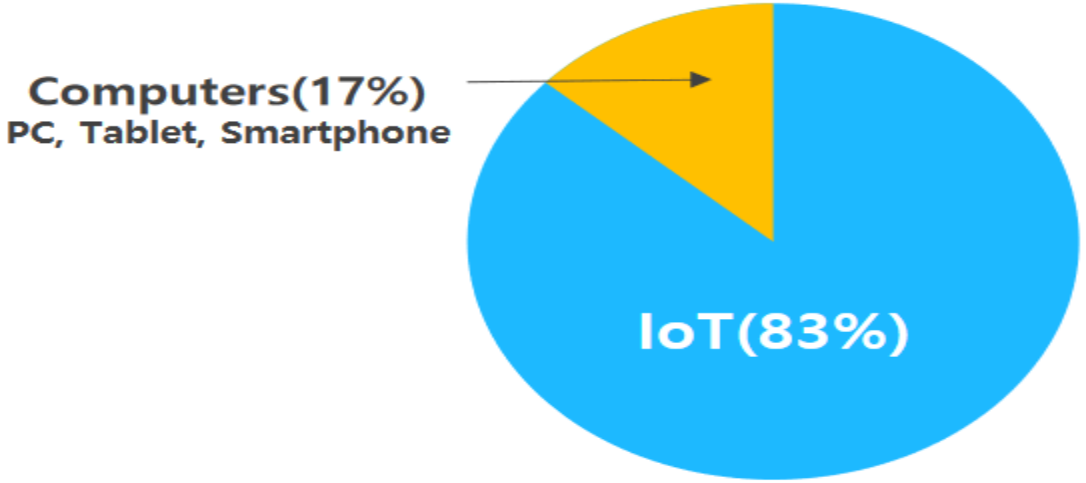
It's Internet of Things!

FACULTY OF INFORMATICS
Masaryk University

Blockchain has begun to have a significant influence in the Internet of Things by enhancing security, empowering the incorporation of an increasing number of devices into the ecosystem.



- **…ay, about 15 billion IoT devices are …nected to internet.**
- **50 billion IoT devices are estimated to be connected to internet by 2020**



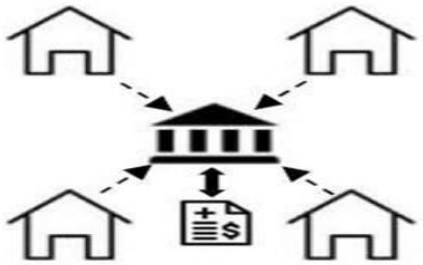
※ Source : "IoT in Logistics" by Cisco

What is Blockchain Technology?

FACULTY OF INFORMATICS
Masaryk University

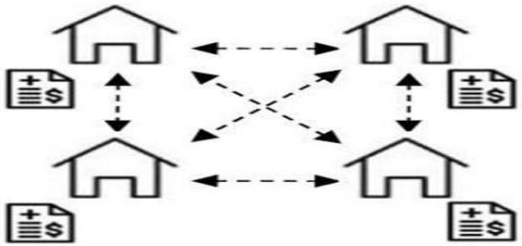
- Blockchain is a distributed ledger.
- In general terms, a Blockchain is an immutable transaction ledger, maintained within a distributed network of peer nodes.

Centralized Ledger



- All transactions are recorded into centralized server belonged to specific entity
- Single point of weakness

Distributed Ledger



- Each node has an identical ledger that contains transaction after “consensus”
- Network effect holds transaction immutability

Three “Levels” of Blockchain

FACULTY OF INFORMATICS
Masaryk University

1. Storage for digital records
2. Exchanging digital assets (called tokens)
3. Executing smart contracts
   - Ground rules – Terms & conditions recorded in code
   - Distributed network executes contract & monitors compliance
   - Outcomes are automatically validated without third party

Blockchain use cases

FACULTY OF INFORMATICS
Masaryk University

Financial

- Trade Finance
- Cross currency payments
- Mortgages

Public Sector

- Asset Registration
- Citizen Identity
- Medical records
- Medicine supply chain

Retail

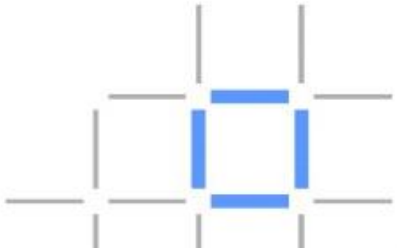
- Supply chain
- Loyalty programs
- Information sharing (supplier – retailer)

Insurance

- Claims processing
- Risk provenance
- Asset usage history
- Claims file

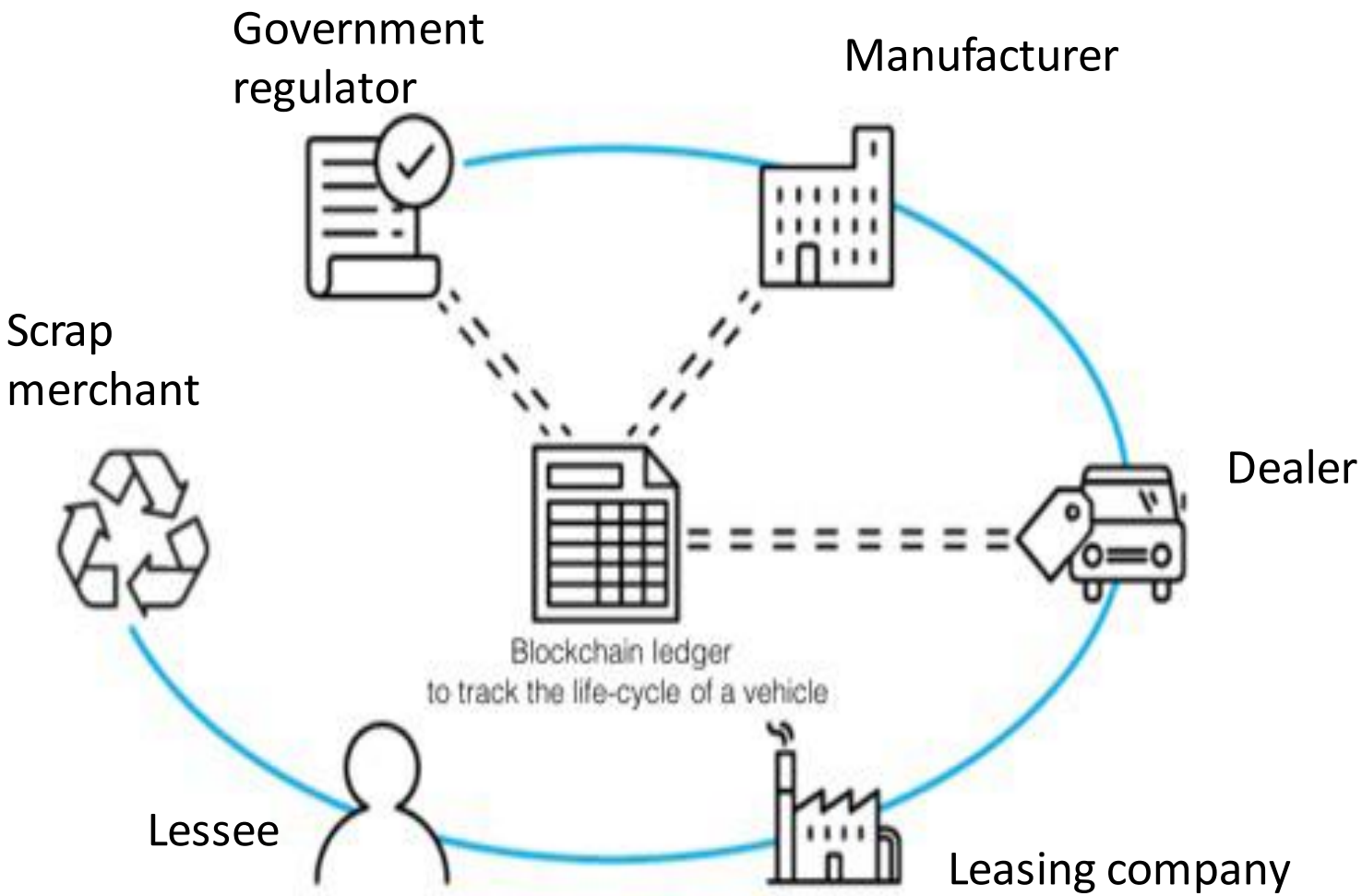
Manufacturing

- Supply chain
- Product parts
- Maintenance tracking



Blockchain: IoT use cases

FACULTY OF INFORMATICS
Masaryk University

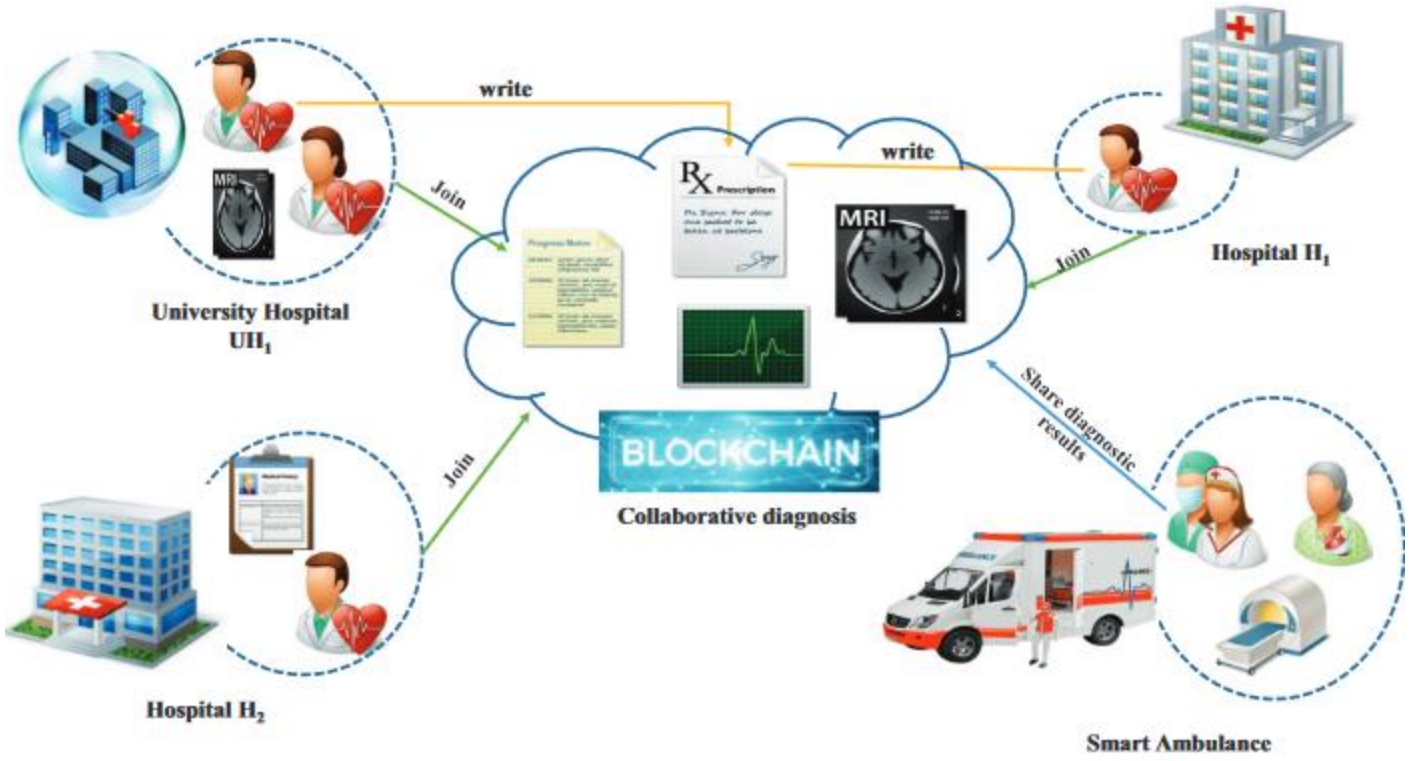


Healthcare Framework using Blockchain

FACULTY OF INFORMATICS
Masaryk University

Channels

Channels are private subnets of the Blockchain network where clients and peers communicate and transact privately.



- Channels provide privacy between different ledgers
- Peers can participate in multiple channels
- Ledgers exist of the scope of a channel
- Channels provide concurrent execution for performance and scalability

IoT Challenges and Blockchain

FACULTY OF INFORMATICS
Masaryk University

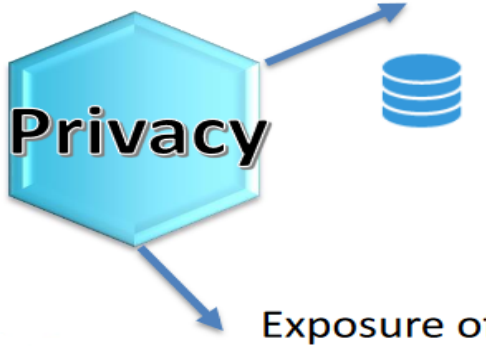
Device Identity solutions

Need for certification authorities

Communication from edge to cloud

Centralized Control

Decentralized Control



Centralized Data Management & need for trusted parties

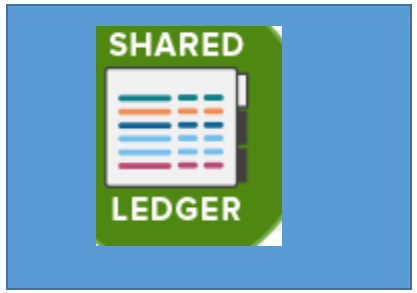
Exposure of data flows in the network

Secured Decentralized Storage

Blockchain for business requirements

FACULTY OF INFORMATICS
Masaryk University

Append-only distributed system of records that are shared across business networks



Business terms that are run with transactions

Transactions are secure with appropriate visibility

Transactions are provably endorsed by relevant participants.

Popular Blockchain Platforms:

FACULTY OF INFORMATICS
Masaryk University

- The list of Blockchains is becoming longer every day.
- Many Blockchain Consulting companies are currently active using some of the Blockchain Platforms like Bitcoin, Ethereum, Hyperledger and Quorum.

Bitcoin

MultiChain

How does a Blockchain work?

FACULTY OF INFORMATICS
Masaryk University

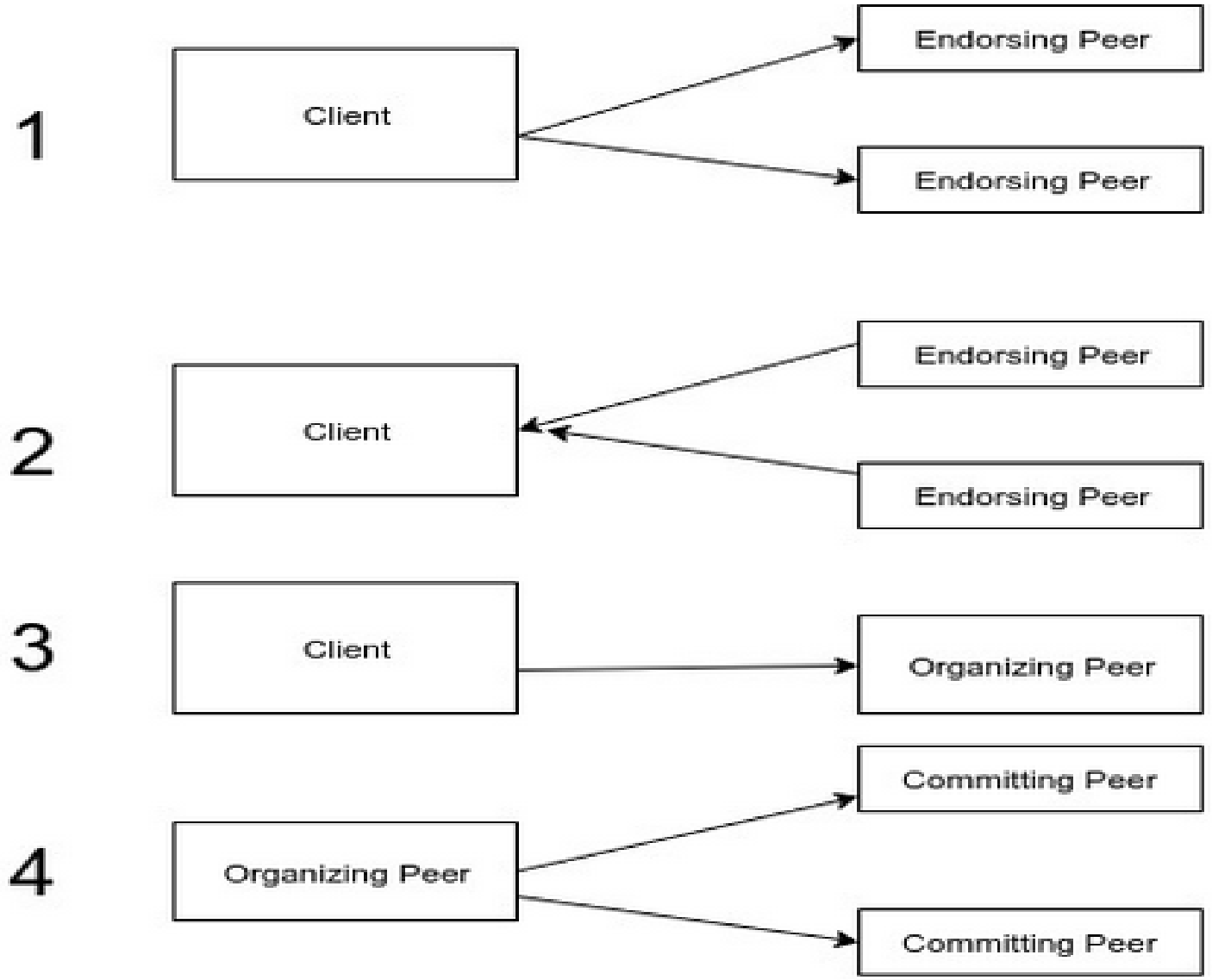
1) A transaction has to be proposed and then endorsed before it can be submitted successfully to the Blockchain.

2) **Endorsing peer** is the peer that will "endorse"/provide the seal of approval to a transaction when it is proposed. After the transaction is endorsed, the transaction(plus the endorsement) will be submitted to Blockchain.

3) Once the Transaction is submitted, it will make way to the peers that are supposed to get that transaction. These peers will then "commit"/save the transaction in their Ledger, and these are the **committer** peers.

How does a Blockchain work?

FACULTY OF INFORMATICS
Masaryk University



Client sends request for endorsement/approval

Endorsing Peer sends Approved or rejected status after checking for consstency

Client sends collected approvals to organizing peer which creates Blocks

Organizing Peer sends created blocks to all committing Peers

Smart contract

FACULTY OF INFORMATICS
Masaryk University

- Smart contract are a set of programs that are executed on Blockchain in order to support several types of transactions between users.
- Code simply denotes software written in programming language.
- Verifiable and signed.
- Business rules, which are written in programming languages, and supported by the blockchain technology.
- Examples:
  - Defines contractual conditions under which a bond transfer occurs.
  - Defines rules on which a vehicle can be transferred to a new owner.

Hyperledger

FACULTY OF INFORMATICS
Masaryk University

- Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, IoT, supply chain, manufacturing, and technology.
- Business Blockchain Frameworks are hosted with Hyperledger.

- Hyperledger addresses important features for a cross-industry open standard for distributed ledgers. The Linux Foundation hosts Hyperledger as a Collaborative Project under the foundation.

- To learn more, visit: https://www.hyperledger.org/.

Conclusion

FACULTY OF INFORMATICS
Masaryk University

Blockchain Challenges

- Immutability: A Blockchain is an add-only list. Once data is added, it can't be removed. Perhas not a good fit when updating data is a regular occurrence.

- The CIA security triad model, composed of three areas; (1) Confidentiality, (2) Integrity and (3) Availability will be referenced to assess the current maturity level of Blockchain technology,

- Authentication, Authorization and Audit (AAA), and Non Repudiation, fundamental security aspects for protecting information and designing / managing new systems and networks1will also be addressed

FACULTY OF INFORMATICS
Masaryk University

Questions and Discussion

My Contacts

bacem.mbarek@mail.muni.cz