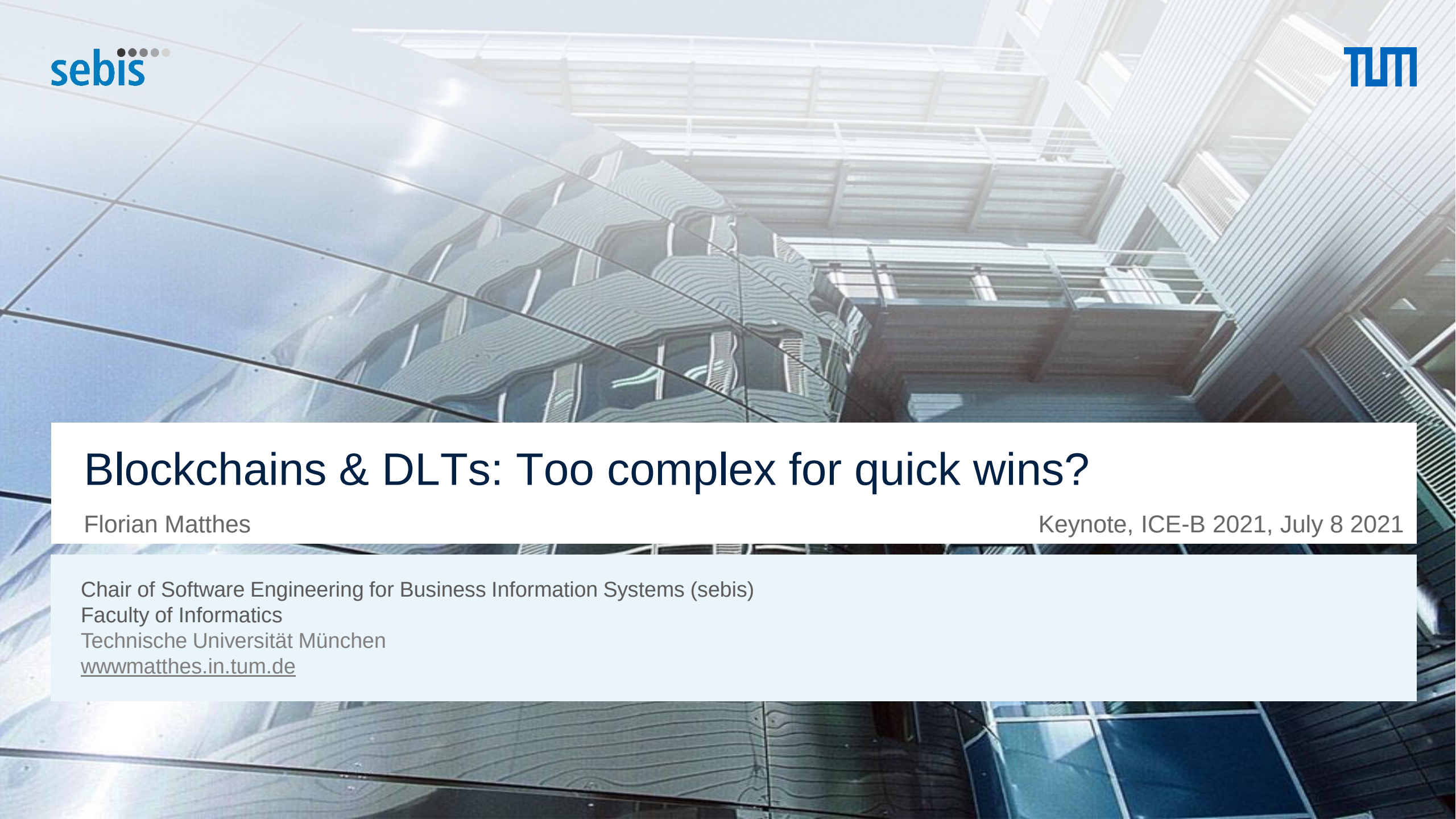


Blockchains & DLTs: Too complex for quick wins?

Florian Matthes

Keynote, ICE-B 2021, July 8 2021

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
wwwmatthes.in.tum.de

Outline

1. Potential of Blockchain-based solutions
2. Characteristics of permissioned and permissionless Blockchain-based platforms
3. Getting beyond the technical proof of concept
    - SWOT of permissionless Blockchain solutions
    - SWOT of permissioned Blockchain solutions

What is a „Blockchain“?

Technical definition

“A blockchain […] is a **distributed database** that maintains a continuously-growing list of ordered records called blocks. Each block contains a timestamp and a link to a previous block. **By design** blockchains are **inherently resistant to modification** of the data: once recorded, the data in a block cannot be altered retroactively.”

https://en.wikipedia.org/wiki/Blockchain_(database)

Functional description

[...] are **systems** that enable parties who don’t fully trust each other to **form and maintain consensus** about the **existence, status and evolution** of a set of shared facts.

Richard Brown, R3 CTO

The potential of blockchain technologies

They enable **intermediary-free** transactions of **digital, non-copyable goods** without the need to trust the other party.

Digital identities of people or **machines** can enter into secure transactions and all transaction details are stored **immutable** and **decentralized**.

Automated, programmable contracts can ensure contract compliance.

"We believe that the Blockchain will have the greatest influence on contracts, logistics and supply chain, healthcare, public administration, asset clearing, property and transactions."

- Greg LaBlanc

Berkeley UNIVERSITY OF CALIFORNIA

Current and future use cases (B2B & B2C)

Industries

Finance

- Crypto currencies
- Microcredit and crowdfunding peer-to-peer
- ICOs: Start-up financing
- Replacement of intermediaries in transactions

Pharma und Medical

- Access to decentralized patient records
- Prevention of prescription abuse
- Prevention of counterfeit drugs

Automotive

- Supply chain tracking
- Digital identity of a car
- Digital mobility solutions (e.g. car sharing)

Energy

- Private suppliers of electricity
- Micro power networks
- Electricity trading

Cross-industry, peer to peer

Documentation

- Elimination of some notary services
- Traceable supply chain
- Service & maintenance protocols
- Digital certificates of origin

IP Management

- Preservation of patents, art or ideas on the blockchain (incl. time stamp)
- Securing 3D printer models
- Direct remuneration of license holders

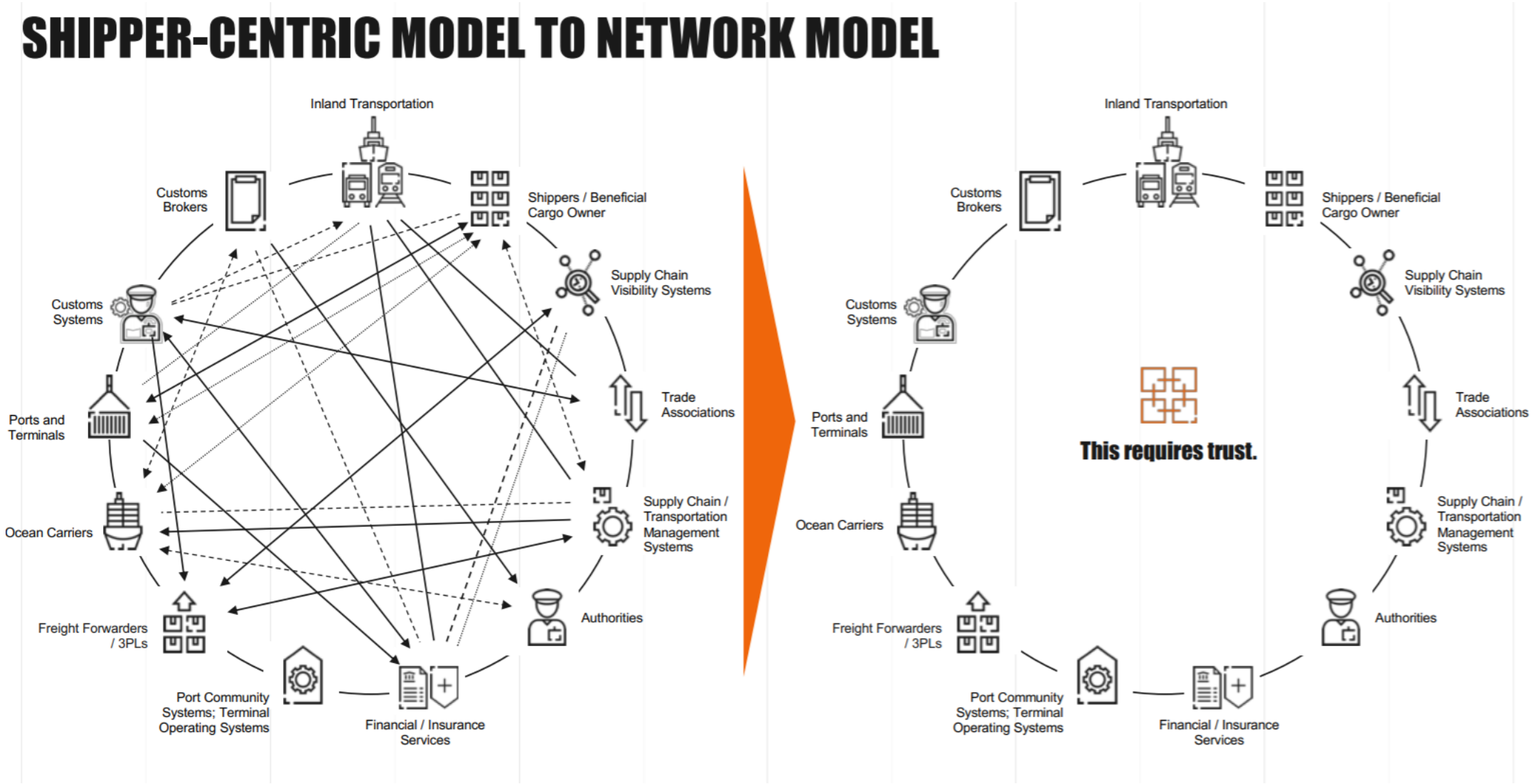
Digital Identity

- Refugees pay by retina scan
- Education & training certificates
- Self-sovereign identities

Sharing Economy

- Transactions without a central platform provider
- Decentralized documented bartering
- Pay-as-you-use insurances

TradeLens: Transforming global container logistics

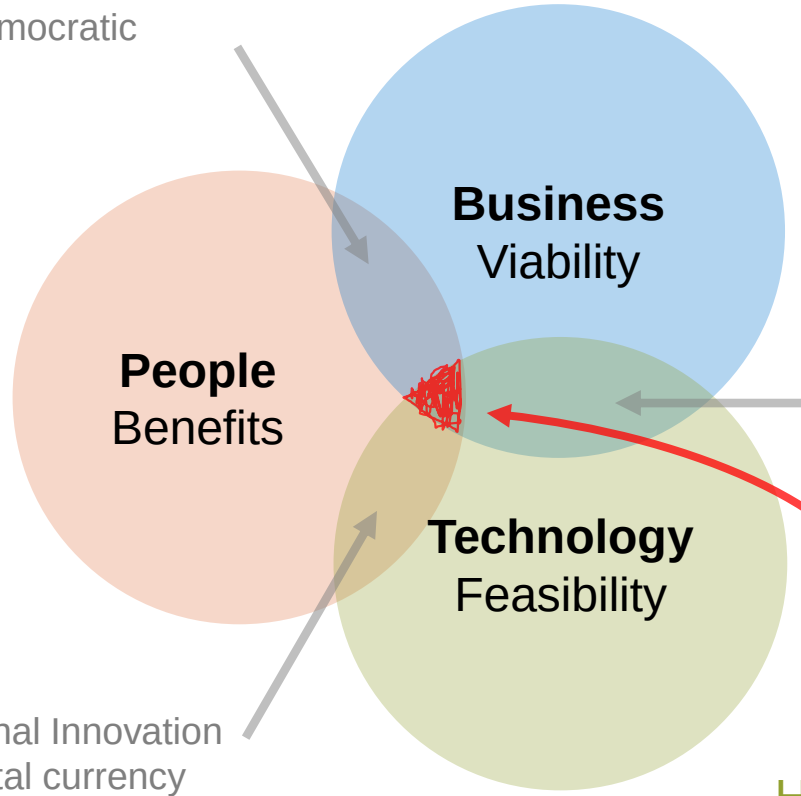


https://merehead.com/blog/maersk-blockchain-use-case/

Applying design thinking to blockchain-based solutions

Emotional Innovation
- Trust
- Decentralized
- Democratic
- ---

How to create a sustainable business?



Which pain of which people / businesses do we solve?

Process Innovation
- Peer 2 Peer Network
- Decentralized Governance
- …

Innovative Solution

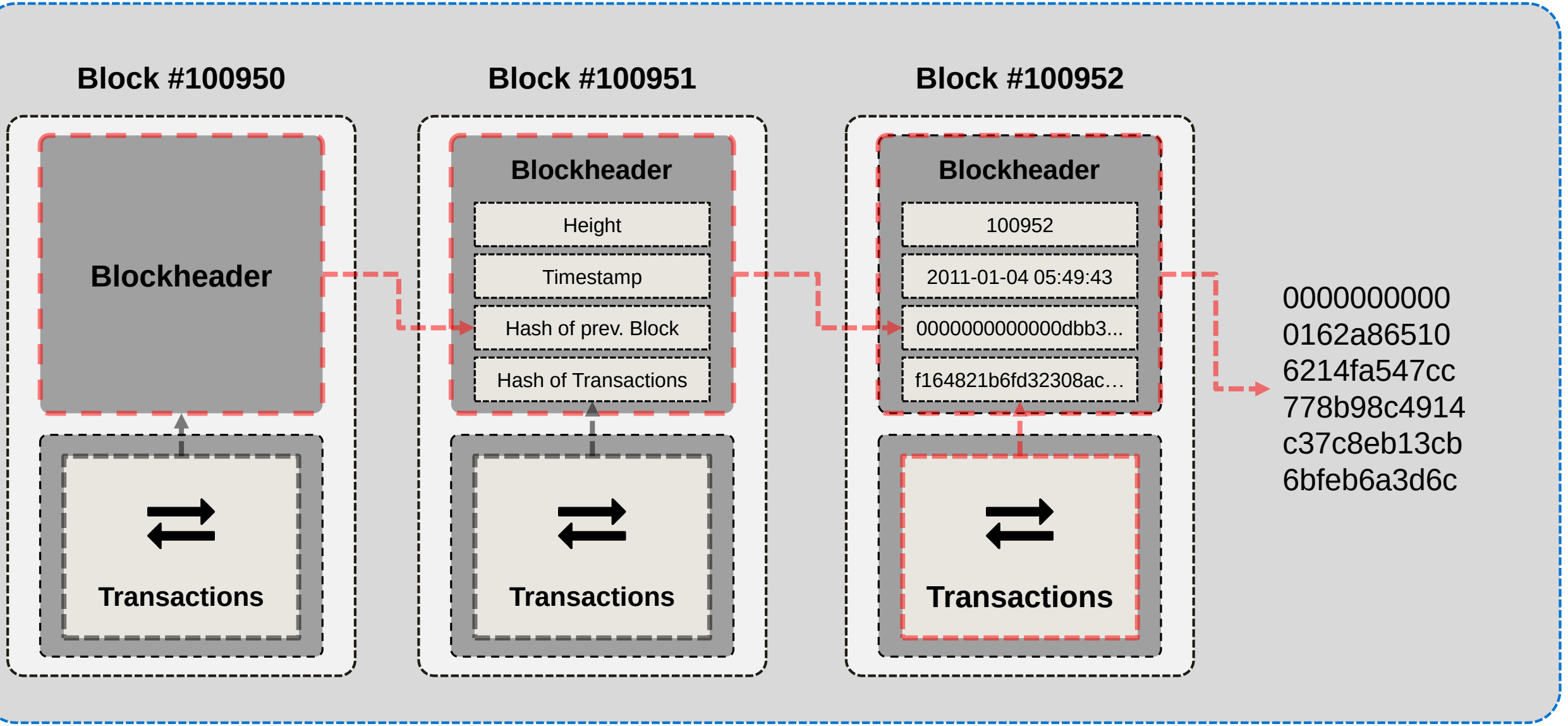
Functional Innovation
- Digital currency
- Digital token
- Digital wallets
- …

How to solve the problem?

Outline

1. Potential of Blockchain-based solutions
2. Characteristics of permissioned and permissionless Blockchain-based platforms
3. Getting beyond the technical proof of concept
    - SWOT of permissionless Blockchain solutions
    - SWOT of permissioned Blockchain solutions

The structure of the Bitcoin blockchain

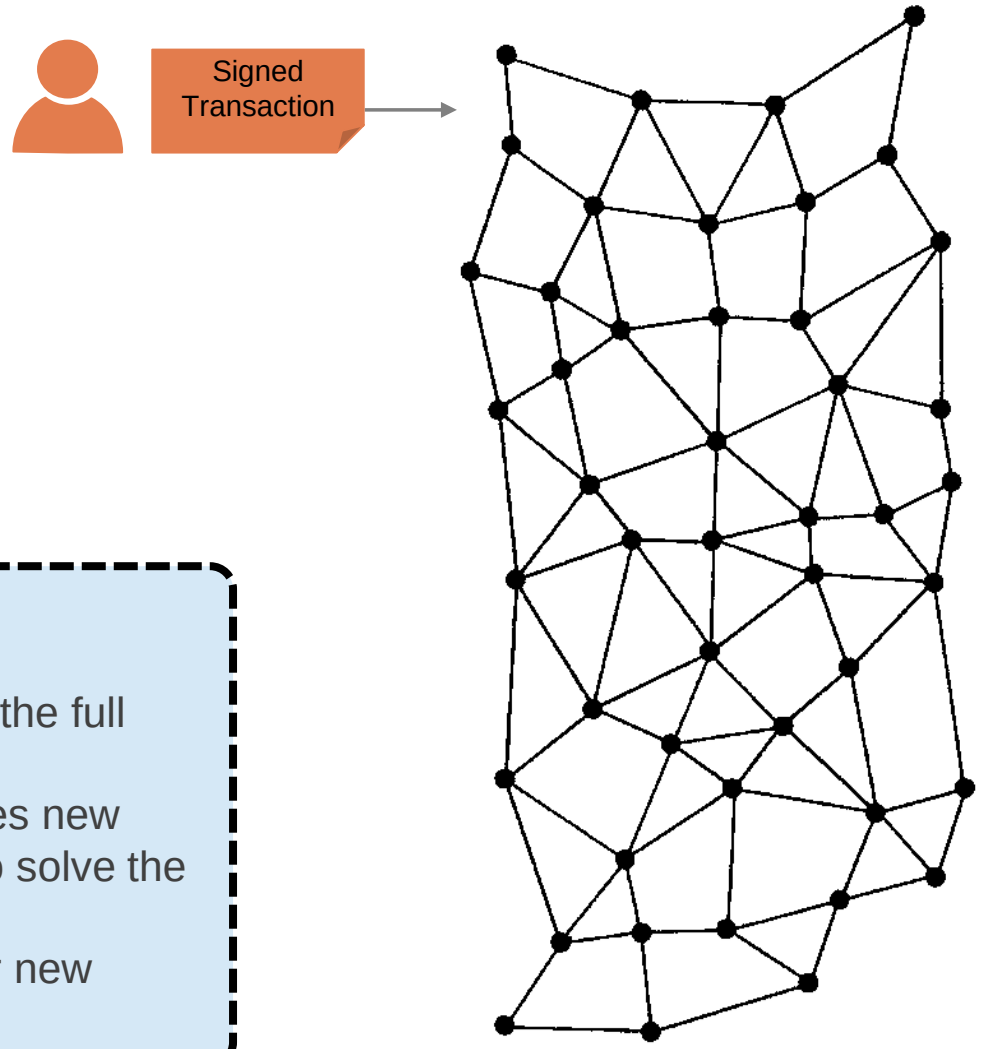


[1]In Bitcoin, the height is included in the Coinbase Transaction.

Roles in the network

Wallet Owner

- Has private key to unspent transactions
- Owns the money
- Sends money by singing and publishing new transactions



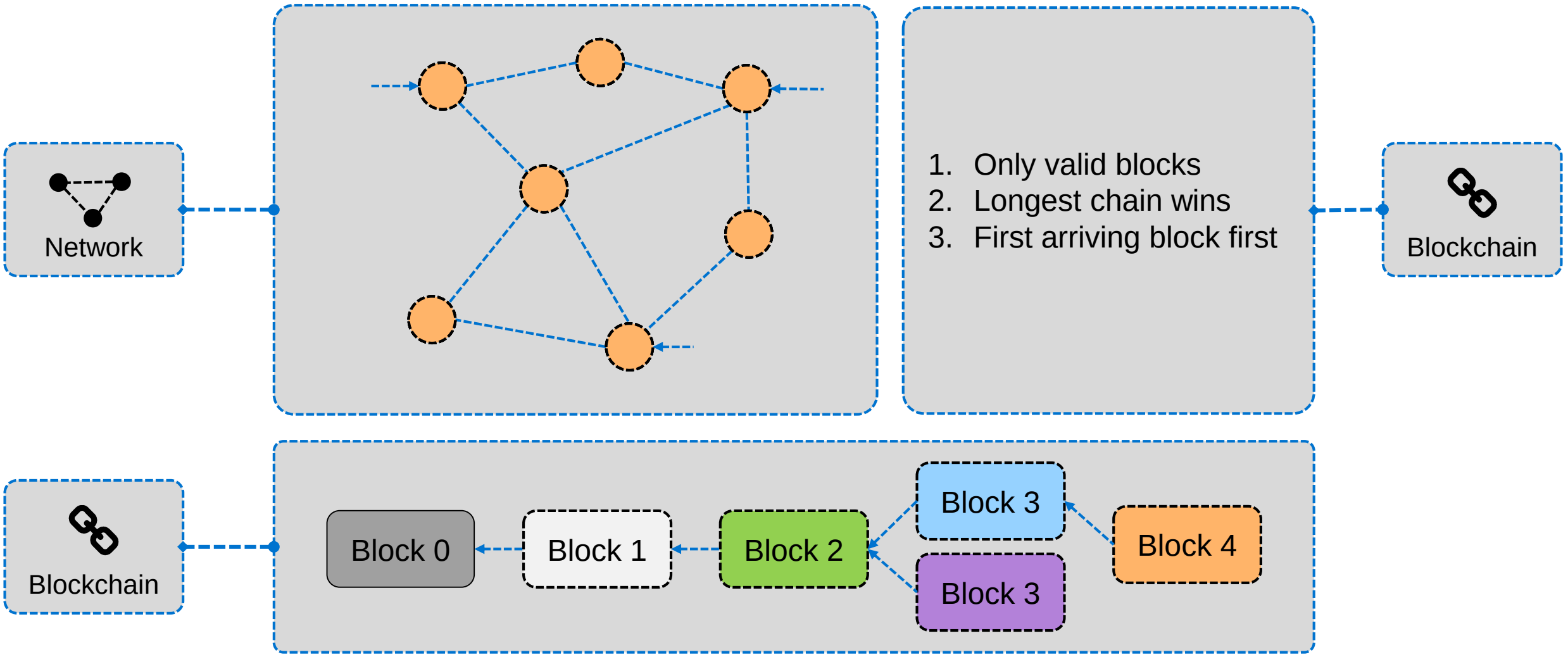
Full Node

- Maintains the complete blockchain
- Validates every transaction and block
- Relays all new transactions

Miner

- Acts the same as the full node
- Additionally creates new blocks and tries to solve the mining puzzle
- Gets rewarded for new blocks

Reaching consensus in the network



Which node is allowed to issue new blocks?

Constraints

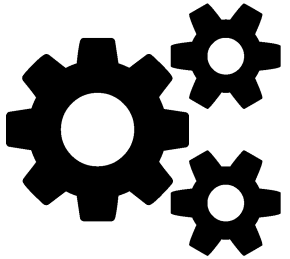
- Keep the network fully decentralized ➔ Random selection of node

- Avoid a **51% attack** by a group of nodes allowing them to
  - prevent new transactions from gaining confirmations, to halt payments between some or all users, or
  - reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins.

Approaches

- Proof of work ➔ Increase cost / difficulty of creating new blocks
  - Solve a time-consuming mathematical puzzle
  - Solve a puzzle that requires a lot of computer memory

Mining



- Proof of stake ➔ Increase cost of creating invalid blocks
  - Deposit an amount of money that gets transferred if an invalid block is detected

Historical development of the concept of *Smart Contracts*

- The term “Smart Contract” was coined long before blockchain technology emerged (Szabo, 1994).
- Initially described the formalization of processes in public networks like the Internet.
- Possible applications:
  - DRM (Digital Rights Management)
  - Payment
  - Connection to the “real world” through sensors and actuators

➔ However, there was a lack of technology to realize these ideas at that time.

Szabo, Nick (1994): Smart Contracts.
https://web.archive.org/web/19971008001022/http://www.virtualschool.edu/mon/Economics/SmartContracts.html

Smart Contracts on blockchain-based platforms

In 2015, Vitalik Buterin revived the idea in his white paper "*Ethereum: A Next Generation Smart Contract & Decentralized Application Platform*"

Idea

- Replace the fixed data structures, algorithms and protocols of individual blockchain solutions (e.g. Bitcoin, voting, bidding, lottery, proof of ownership, …) by programs, written in a domain-specific programming language (e.g. **Solidity**) on top of a single public blockchain (**Ethereum**) and currency (**Ether**).
- Use cryptography to secure the immutability of the program code (**contract**)
- Wallet owners agree on the contract(s) to be used for their future interactions
- No or very limited access of the code to the "real world" (sensors, actuators)

➔ Similar to data-centric architectures for workflow management and automated case management

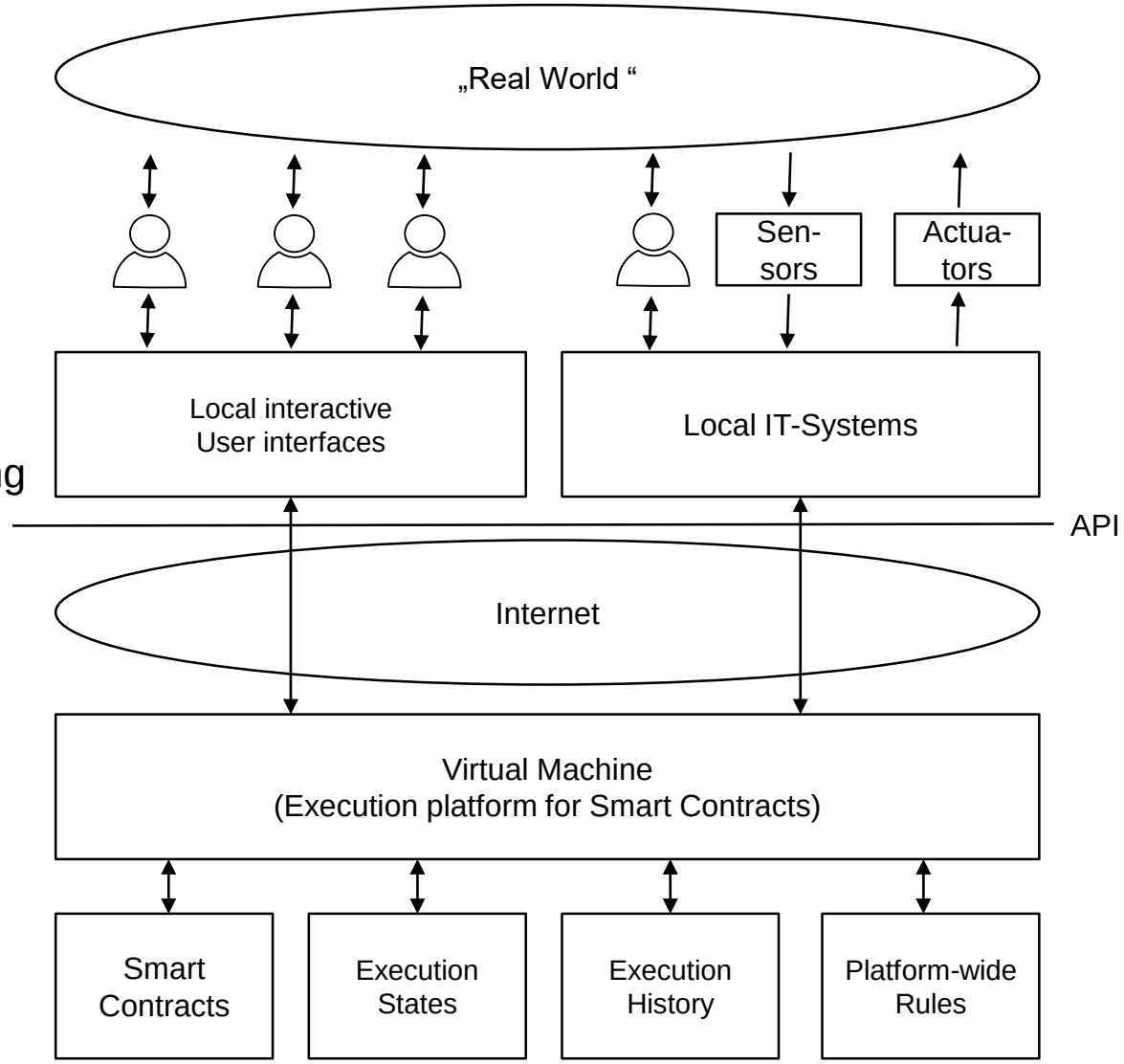
A reference architecture for a Smart Contract platform

Example:

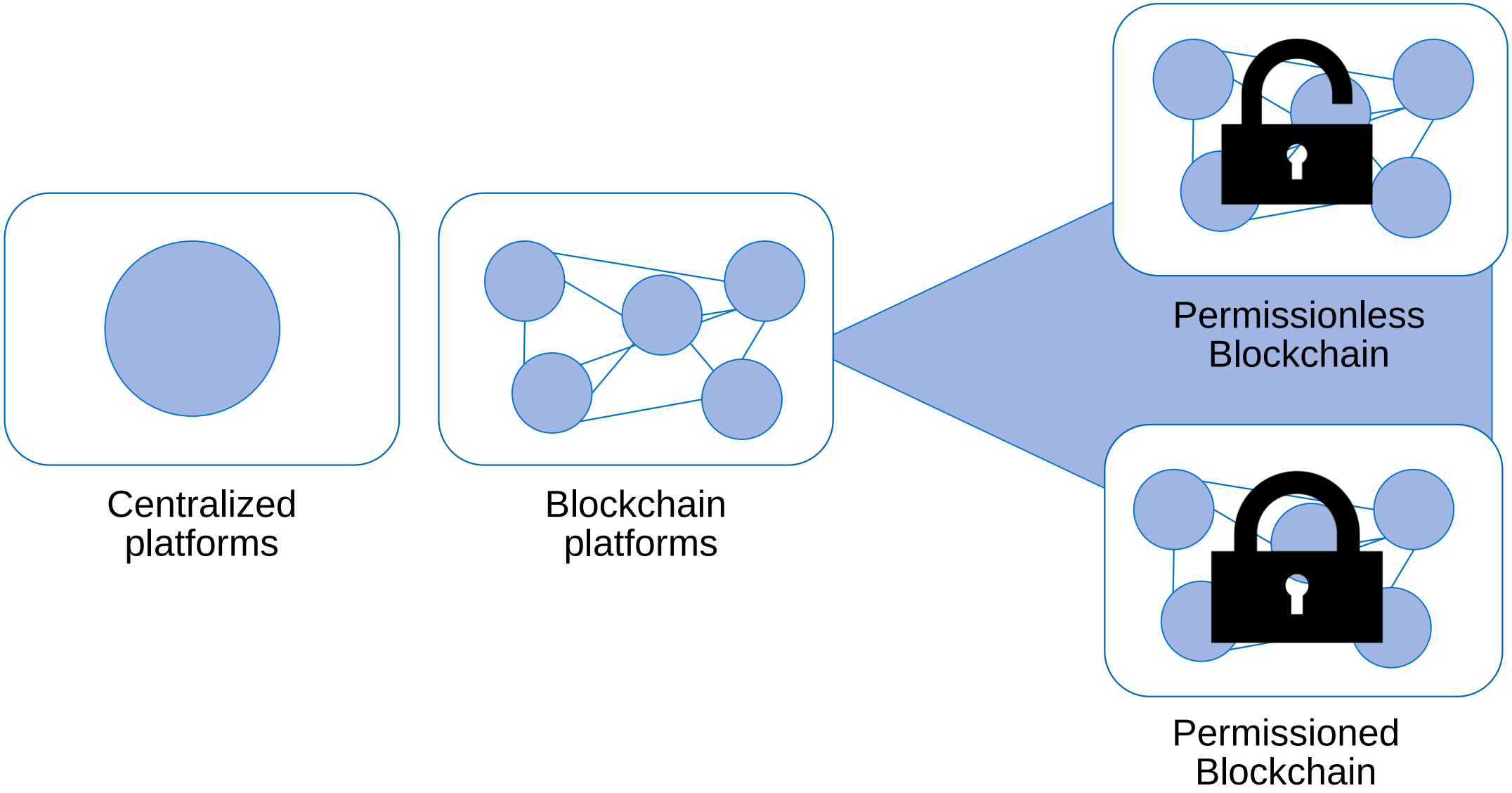
Safe transfusion medicine

Blood product supply chain involving

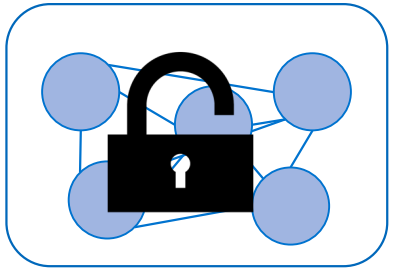
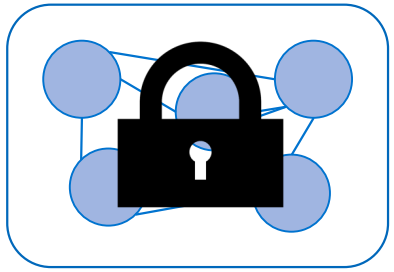
- Clinics
- Labs
- Logistic companies
- Blood donor centers



Implementations of the reference architecture



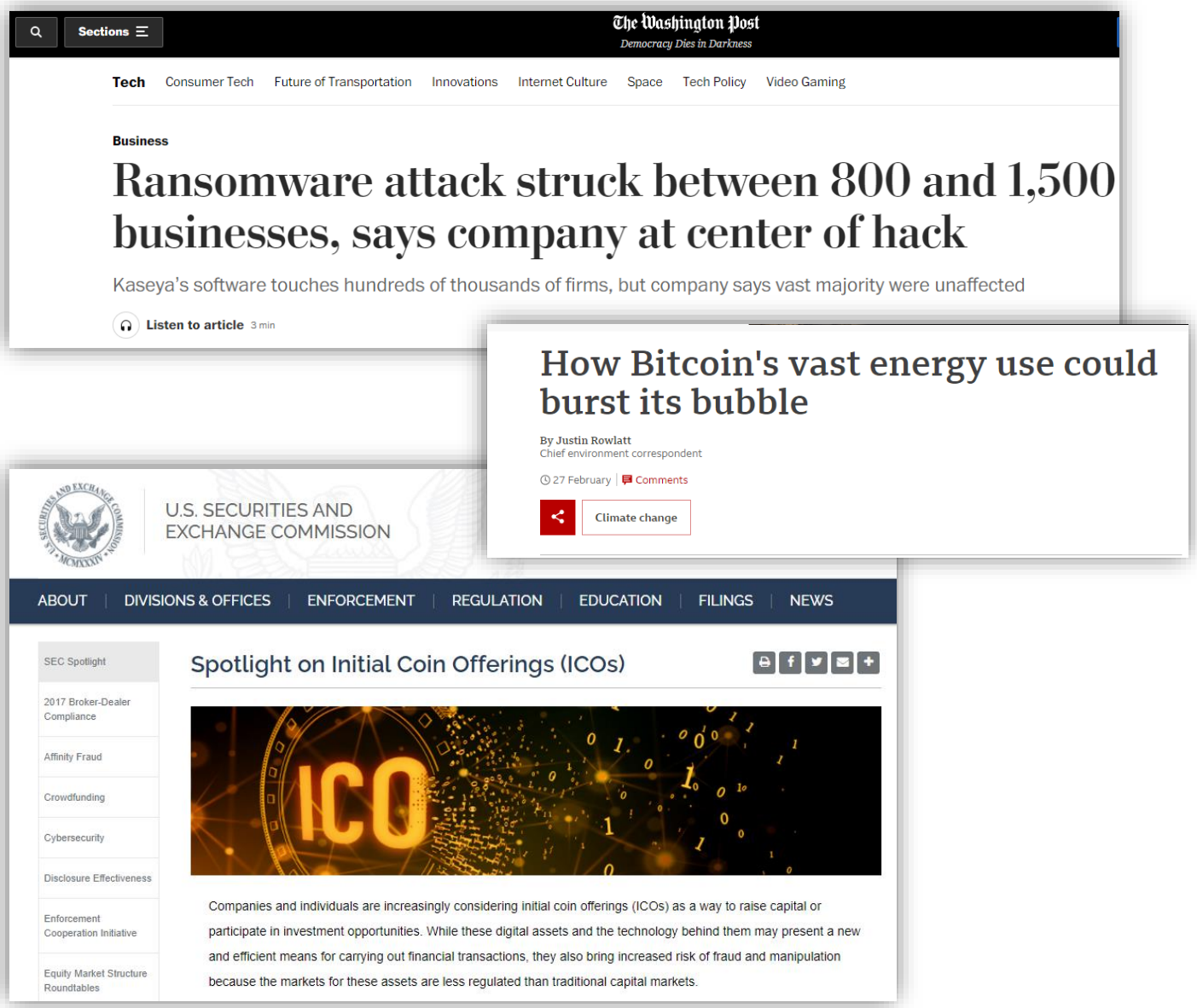
Who can take which role in a blockchain network?

	User	Node (Reader)	Miner (Writer)	Examples
 **Permissionless**	▪ **Everybody** ▪ Pseudonymous users / wallets	▪ **Everybody** ▪ All transactions are public	▪ **Everybody** ▪ Mining hardware ▪ Mining pools ▪ Mining rewards	▪ **Bitcoin** ▪ **Ethereum**
 **Permissioned**	▪ **Managed** (by consortium) ▪ KYC, AML, …	▪ **Consortium members** ▪ Transactions are visible to (a subset of) the consortium	▪ **Consortium members** ▪ Notary / ordering services	▪ **Corda** ▪ **Hyperledger**

Outline

1. Potential of Blockchain-based solutions
2. Characteristics of permissioned and permissionless Blockchain-based platforms
3. Getting beyond the technical proof of concept
   - SWOT of permissionless Blockchain solutions
   - SWOT of permissioned Blockchain solutions

Permissionless Blockchains have a reputation problem



- Incredible waste of energy and resources due to proof of work
- Use for shady business models
  - Speculative trading
  - Gambling
  - Trafficking (humans, drugs, …)
  - Cyber crime
  - Ransomware attacks
  - …
- Casino economy
  - ICO scams
  - Exchange frauds
  - “Lost” or “locked” crypto money
  - …
- Huge gap between expectations and maturity of the technology

Permissionless Blockchains continue to fuel business innovations

What are NFTs and why are some worth millions?

12 March

A digital-only artwork has sold at Christie's auction house for an eye-watering $69m (£50m) - but the winning bidder will not receive a sculpture, painting or even a print.

https://www.bbc.com/news/technology-56371912

Permissionless Blockchain-based platforms

Strengths

- Fault-tolerant and resilient infrastructure
- Fully decentralized
- Utility model
- Open source
- Innovation-friendly (soft and hard forking)
- Domain-specific languages
- Expressive data model / type system
- Rich developer tool support
- Comparatively large developer community

Weaknesses

- No data privacy (on-chain)
- Energy consumption
- Extremely limited transaction throughput
- High transaction latency
- “Tiny data” solutions only
- Dependency on a crypto currency
- Greenfield approach ignoring enterprise IT (languages, libraries, tools, operating models)

Opportunities

- Web 3.0 leverages Web 2.0 technology stack
- Low entry barrier for application provider
- Financial incentives for growth and innovation
- De-facto protocol standards for DeFi
- Ecosystem of complementing innovations (SSI, ZKP, IPFS, Ocean Protocol, Trusted Computing, …)

Threats

- High regulatory risks
- Untested planetary scalability
- Centralization at the network level
- Centralization at the application level
- Centralization at the “gates” (e.g. exchanges, oracles, …)

Permissionless Blockchain-based platforms

Currently suitable only for a very specific set of **business scenarios:**

- Cryptocurrencies and their derivatives
- Public registers and logs (of potentially encrypted or hashed data)
- Token economy

Vibrant innovation ecosystem

- Open source communities
- Academic researchers
- Startups
- Venture capitalists

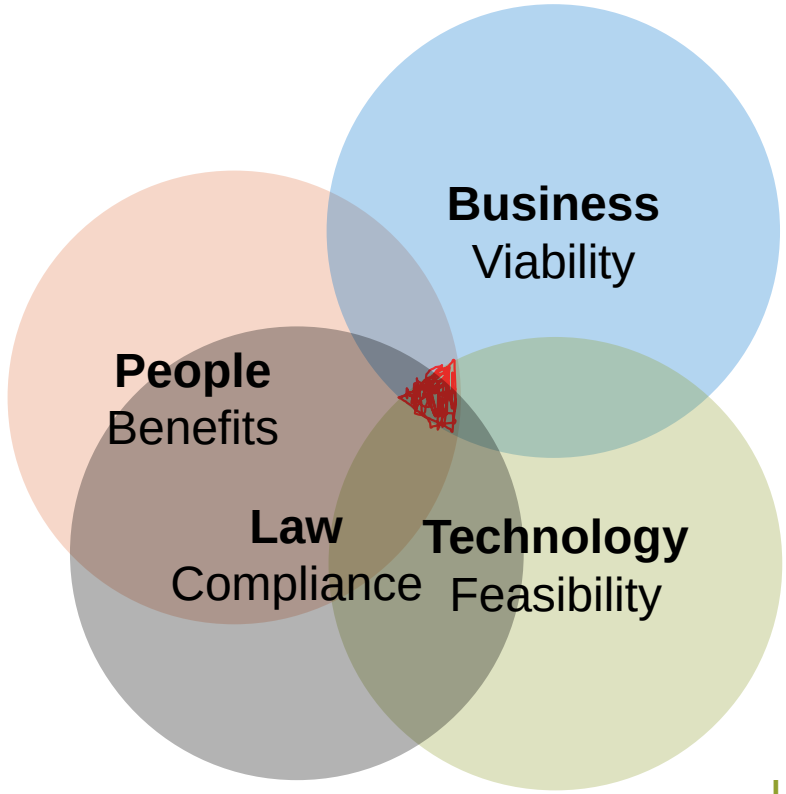
This may lead to disruptive new use cases with a rapid global adoption.

Outline

1. Potential of Blockchain-based solutions
2. Characteristics of permissioned and permissionless Blockchain-based platforms
3. Getting beyond the technical proof of concept
   - SWOT of permissionless Blockchain solutions
   - SWOT of permissioned Blockchain solutions

Interdisciplinary collaboration is required

How to create a sustainable business?

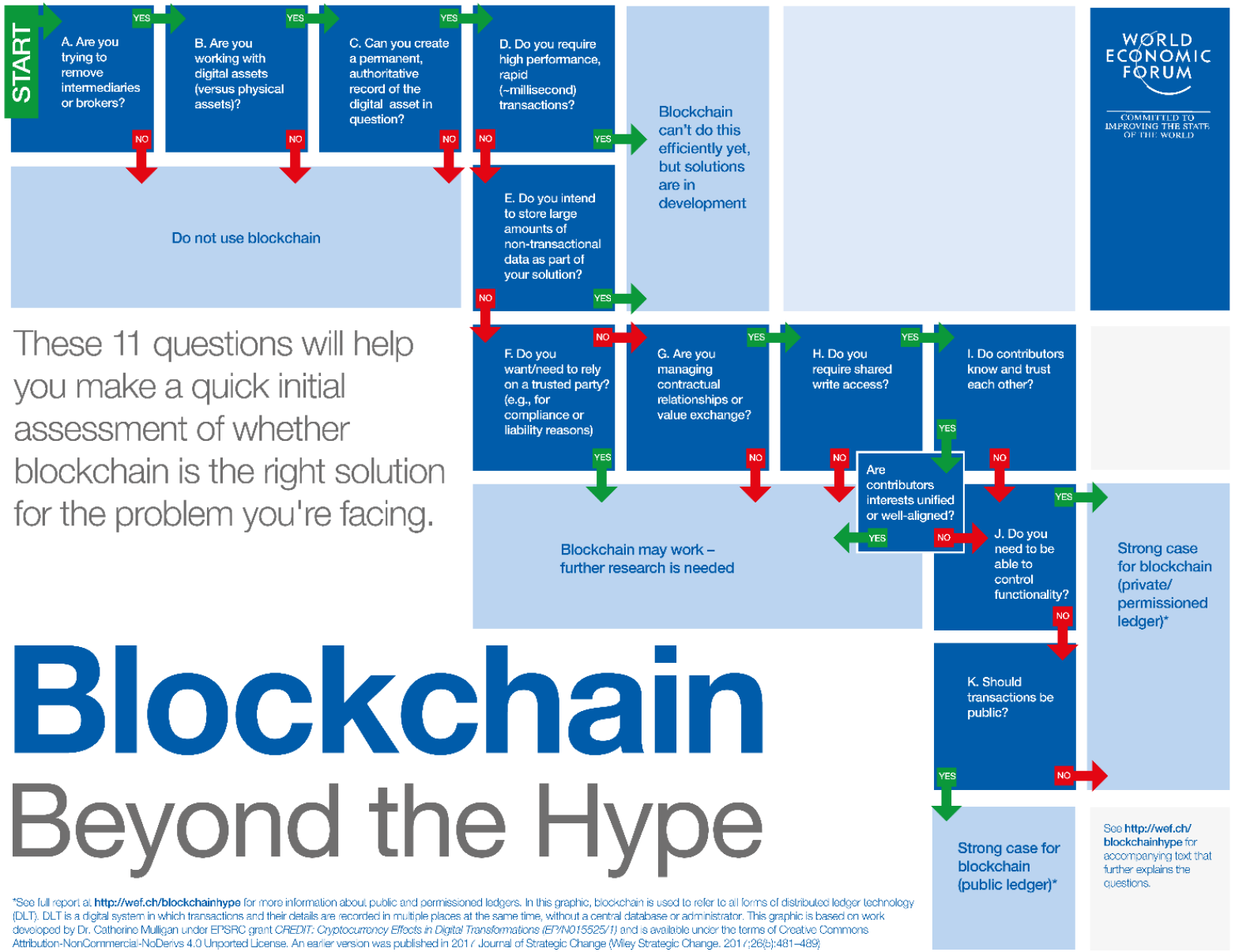


Which pain of which people / businesses do we solve?

How to ensure compliance with the law?

How to solve the problem?

Decision model by the World Economic Forum



These 11 questions will help you make a quick initial assessment of whether blockchain is the right solution for the problem you're facing.

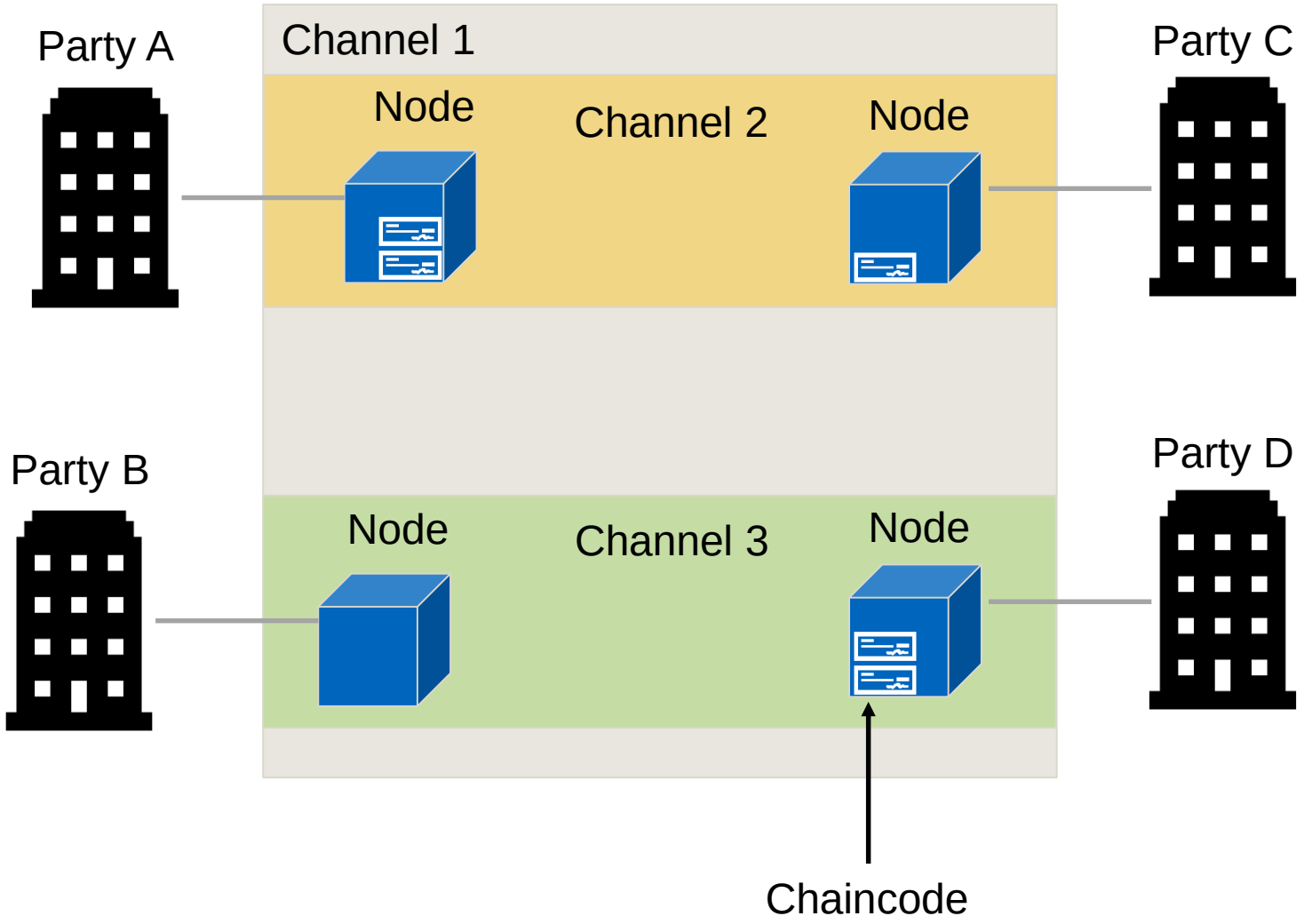
WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Blockchain
Beyond the Hype

*See full report at **http://wef.ch/blockchainhype** for more information about public and permissioned ledgers. In this graphic, blockchain is used to refer to all forms of distributed ledger technology (DLT). DLT is a digital system in which transactions and their details are recorded in multiple places at the same time, without a central database or administrator. This graphic is based on work developed by Dr. Catherine Mulligan under EPSRC grant *CREDIT: Cryptocurrency Effects in Digital Transformations (EP/N015525/1)* and is available under the terms of Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Unported License. An earlier version was published in 2017 Journal of Strategic Change (Wiley Strategic Change. 2017;26(5):481–489)

Source: https://www.weforum.org/agenda/2018/04/questions-blockchain-toolkit-right-for-business

Hyperledger Fabric: Channels



Blockchains are a team sport

The parties in the ecosystem interact via shared executable contracts on shared blockchains.

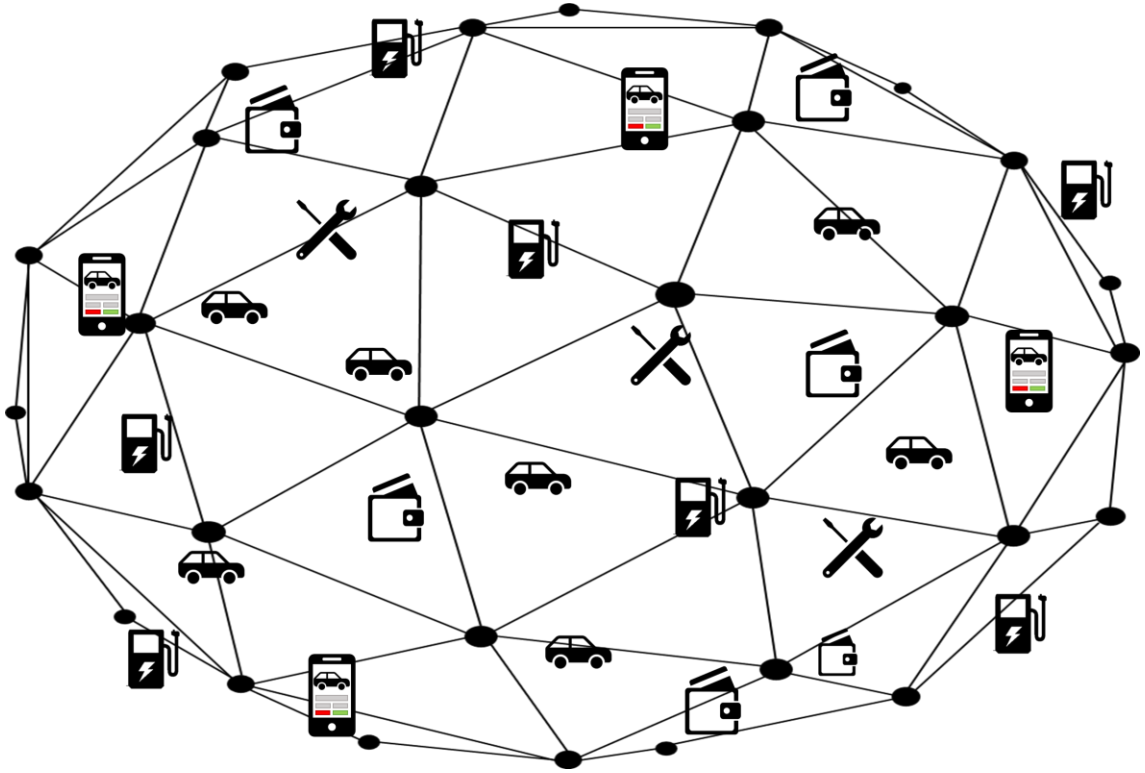
Banking: R3 Consortium (2014)

- 200+ members

Energy: Energy Web Foundation (1/2018)

Insurance: B3i Consortium (3/2018)

- Achmea, Aegon, Ageas, Allianz, Generali, Hanover Re, Liberty Mutual, Munich Re, SCOR, Swiss Re, Tokio Marine, XL Catlin, Zurich Insurance Group



Mobility: Mobi Open Blockchain Initiative (5/2018)

- BMW, General Motors, Renault, Ford, Bosch, ZF, Hyundai, …

Permissioned Blockchain-based platforms

Strengths

- Privacy (data and transactions)
- Authentication and authorization
- Scalability
- Familiar programming languages
- Familiar development environments and tools
- Established IT service providers
- Professional consulting and training services
- Interoperability with standard enterprise IT

Weaknesses

- Low-level data models
- Cumbersome process modelling
- Complex distributed software deployment
- Low maturity of development tools

Opportunities

- Regulatory compliance
- Heavy EU funding
- Domain-specific architectures and abstractions (data marketplaces, IoT, public administration)
- Blockchain as a (cloud) service
- National blockchains

Threats

- Unfamiliar organizational structure (cooperative, association, …)
- Complex consortium contract negotiations
- Complex governance (boards, voting rights, on boarding, off boarding, …)
- Limited availability & cost of IT experts
- Market fragmentation

Permissioned Blockchain-based platforms

- First wave of technology-driven innovation projects did not reach a critical mass of consortium members and users or switched to a central database solution.

Recommendations

- Focus on business cases for which no digital solution exists today
- Start with the right size and mix of the consortium
- Involve legal experts early on

Innovation ecosystem

- IBM, SAP, Microsoft, …
- Startups with a B2B focus
- Business consortia
- Industry researchers

Prof. Dr.

Florian Matthes

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289.17132
Fax +49.89.289.17136

matthes@in.tum.de
wwwmatthes.in.tum.de

Abstract

Blockchains and Distributed Ledger Technologies (DLTs) enable intermediary-free transaction for digital, non-copyable goods without the need to trust the other party. People, organizations and machines can enter into secure transactions and all transaction details are stored immutable and decentralized. Automated, programmable contracts can ensure contract compliance.

Despite these compelling and disruptive value propositions, the adoption of public and consortium-based blockchain-based system solution outside the narrow scope of crypto finance is limited.

In this talk, we identify the technical, organizational, legal and governance challenges business blockchain initiatives have to address to reach a maturity beyond a successful technical proof of concept.

We hope to also provide guidance how to resolve some of these challenges.

60 min. incl. Q&A