Relevance of Blockchain-based Systems Engineering

Blockchain-based Systems Engineering

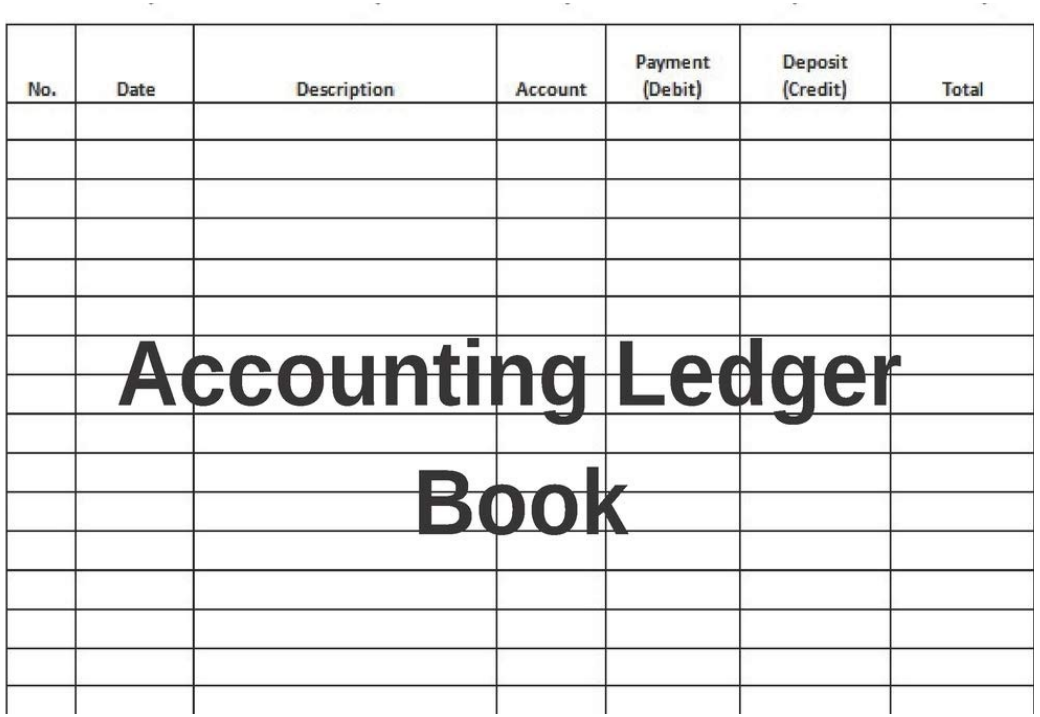
Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
wwwmatthes.in.tum.de

Outline

1. DLT and Blockchain Basics
   - Public Perception
   - Current and Future Use Cases of Blockchain Technology
2. From Smart Contracts to Blockchain-based Architectures
3. Blockchain-based Systems Engineering
4. Assessment of Blockchain Technology
   - Comparison to Established Centralized Solutions
   - Governance in Blockchain-based Systems

Distributed Ledger Technology (DLT)

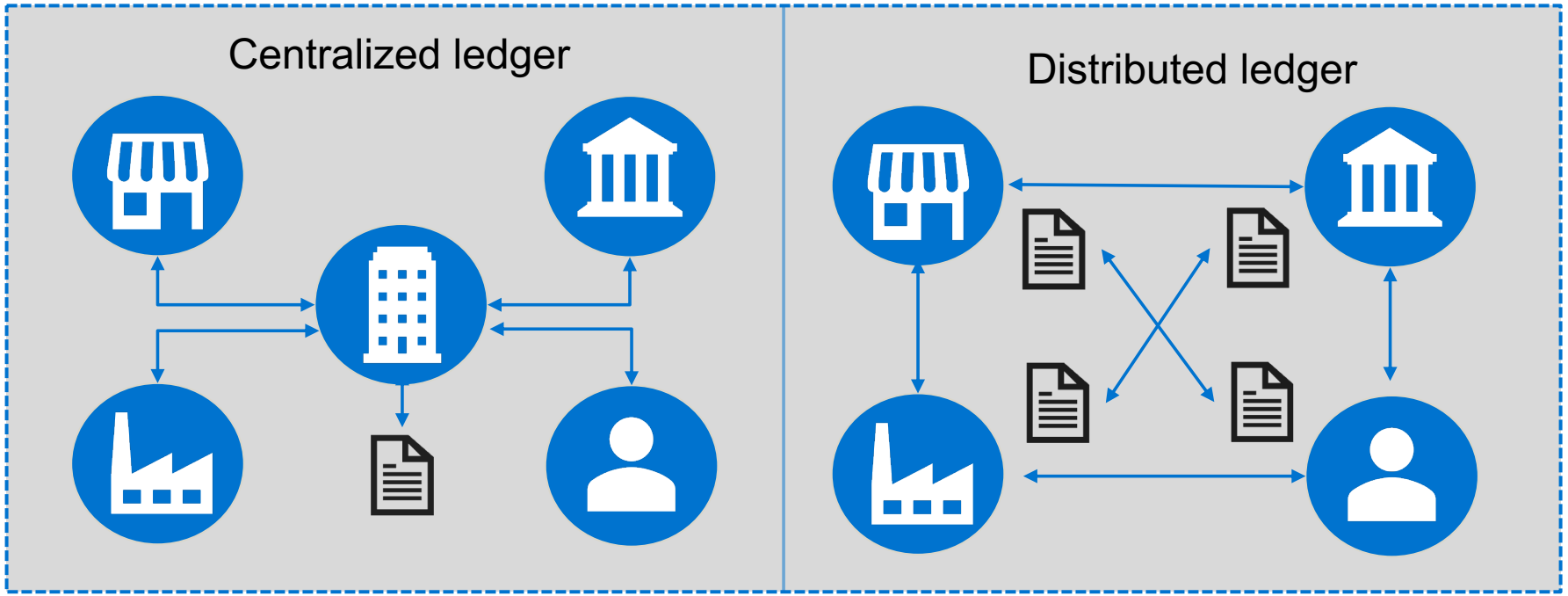
A financial ledger is a collection of accounts that records value/asset ownership and transactions that cause changes in ownership. Likewise, a **distributed ledger** also records ownership data and transactions in a digital format. Additionally, the ledger is maintained in a decentralized peer-to-peer network.



Distributed Ledger Technology (cont.)

Definition:

- DLT refers to the technical architecture and protocols that allow simultaneous access, validation, and record updating in an immutable way over a network that spans numerous entities or locations.
- Nodes of this network process and validate each item in order to reach an agreement on its validity.
- Distributed ledgers, unlike traditional databases, do not have central data storage or administration functions. The most well-known example of distributed ledger technology is **blockchain**.



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

Potential of Blockchain Technologies

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

Digital identities of people or **machines** can interact through 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

Blockchain in Media

Let's take a look at what you have possibly seen on social media about blockchain:

- In 2010, a programmer paid 10,000 Bitcoins for two pizzas.

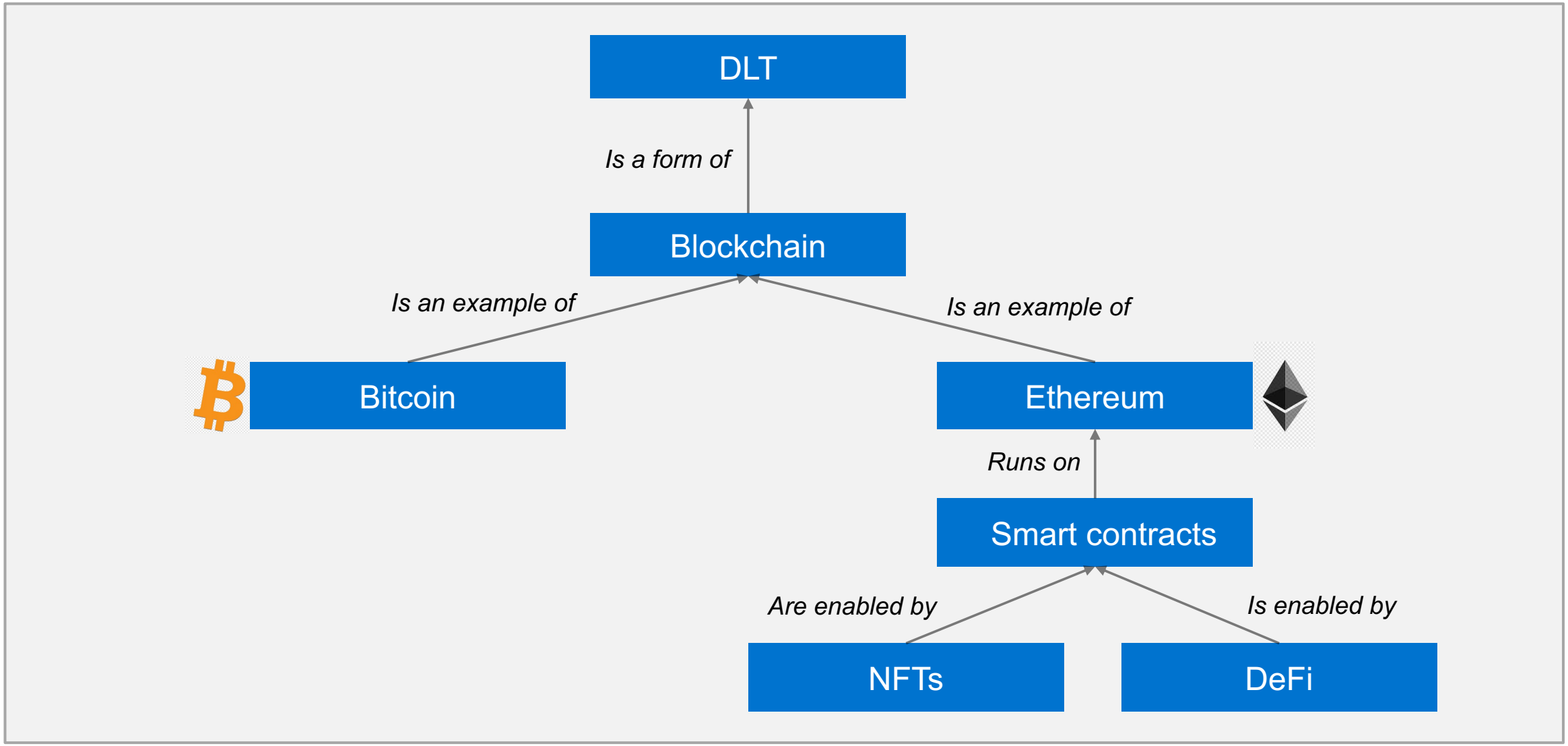
- In 2012, a German art student Max Albrecht built a vending machine that converts €1 coins into their equivalent Bitcoin value.

- In 2016, Bitcoin's price jumped 121% from $433 to $959 and entered the world of mainstream finance.

Reputation Problem of Blockchain

- Incredible waste of energy and resources caused by its Proof-of-Work (PoW) mechanism.
- Use for shady business models
  - Speculative trading
  - Gambling
  - Trafficking (humans, drugs, …)
  - Cybercrime, ransomware attacks
  - …
- Casino economy
  - ICO scams
  - Exchange frauds
  - “Lost” or “locked” crypto money
  - …
- Huge gap between expectations and maturity of the technology

Initial DLT Buzzwords Mindmap



Current and Future Use Cases (B2B & B2C)

Industries

Finance	▪ Cryptocurrencies ▪ Microcredit and crowdfunding peer-to-peer ▪ ICOs: Start-up financing
Automotive	▪ Supply chain tracking ▪ Digital identity of a car ▪ Digital mobility solutions (e.g. car sharing)
Pharma und Medical	▪ Access to decentralized patient records ▪ Prevention of prescription abuse ▪ Prevention of counterfeit drugs
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 Identity	▪ Refugees pay by retina scan ▪ Direct remuneration of license holders ▪ Certificates of origin of digital certificates
IP Management	▪ Preservation of patents, art or ideas on the blockchain (incl. time stamp) ▪ Securing 3D printer models ▪ Direct remuneration of license holders
Sharing Economy	▪ Transactions without a central platform provider ▪ Decentralized documented bartering ▪ Pay-as-you-use insurances

Outline

1. DLT and Blockchain Basics
   - Public Perception
   - Current and Future Use Cases of Blockchain Technology
2. From Smart Contracts to Blockchain-based Architectures
3. Blockchain-based Systems Engineering
4. Assessment of Blockchain Technology
   - Comparison to Established Centralized Solutions
   - Governance in Blockchain-based Systems

Smart Contracts

- As shown in the mind map, **smart contracts** are one of the additional features of blockchain technology.
- Briefly, a smart contract can be defined as a program that runs on the blockchain. It's a collection of code (functions) and persistent data (state).
- A deployed smart contract is identified by its unique address on the blockchain.
- Currently, Ethereum is the most popular blockchain for running smart contracts.[1]

On October 13th, 2018, Ethereum's founder, Vitalik Buterin, has expressed his regret about using the term smart contract. He claimed that he considers smart contracts as "persistent scripts", however, he is of the opinion that it wouldn't have been as catchy as calling them "smart contracts".

vitalik.eth @VitalikButerin · 13 Oct 2018

To be clear, at this point I quite regret adopting the term "smart contracts". I should have called them something more boring and technical, perhaps something like "persistent scripts".

[1] *for other blockchains that support smart contracts, see https://www.itransition.com/blog/smart-contract-platforms*

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, …) with 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) in order to ensure deterministic execution

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

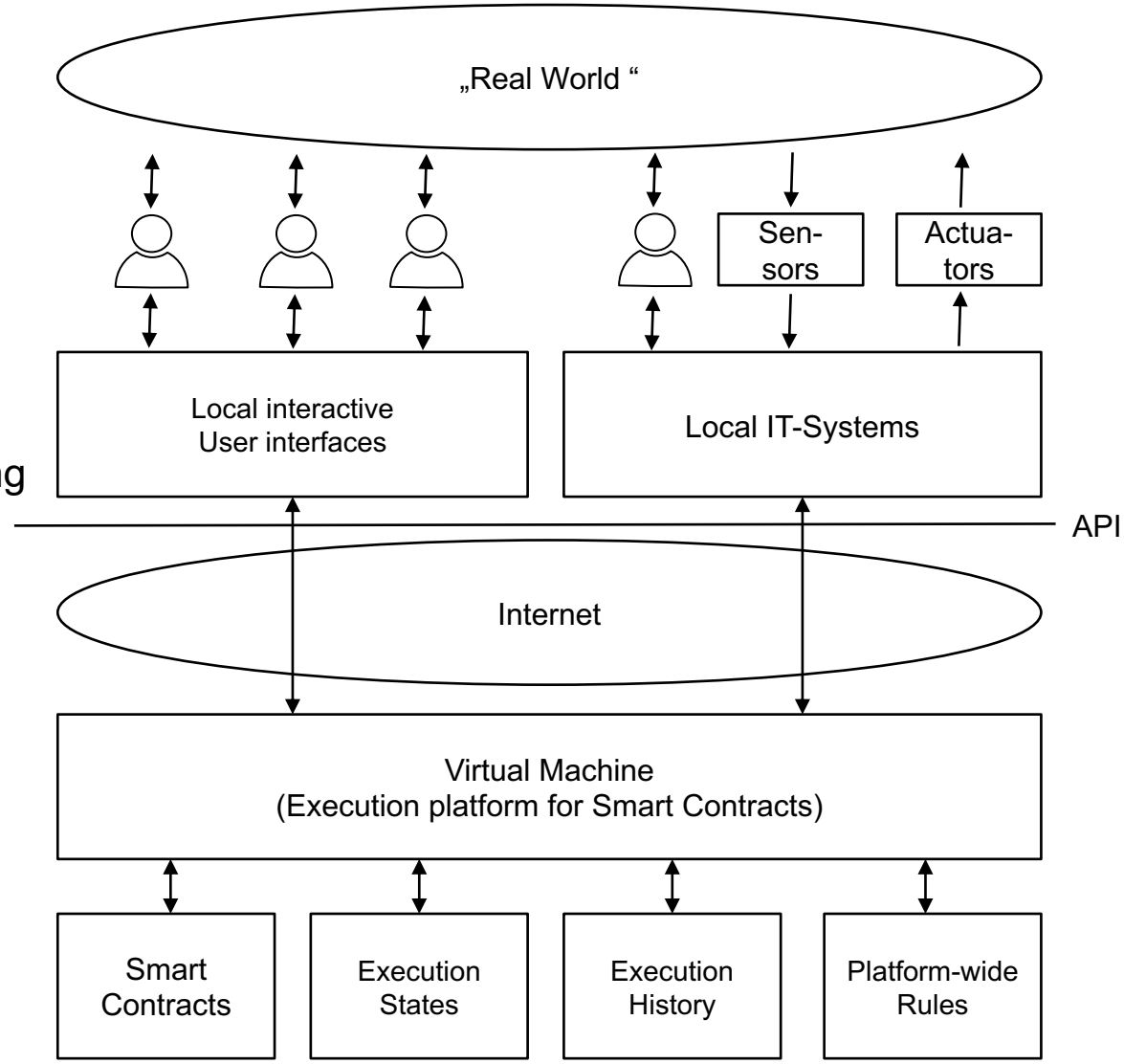
Reference Architecture for a Smart Contract Platform

Example:

Safe transfusion medicine

Blood product supply chain involving

- Clinics
- Labs
- Logistic companies
- Blood donor centers



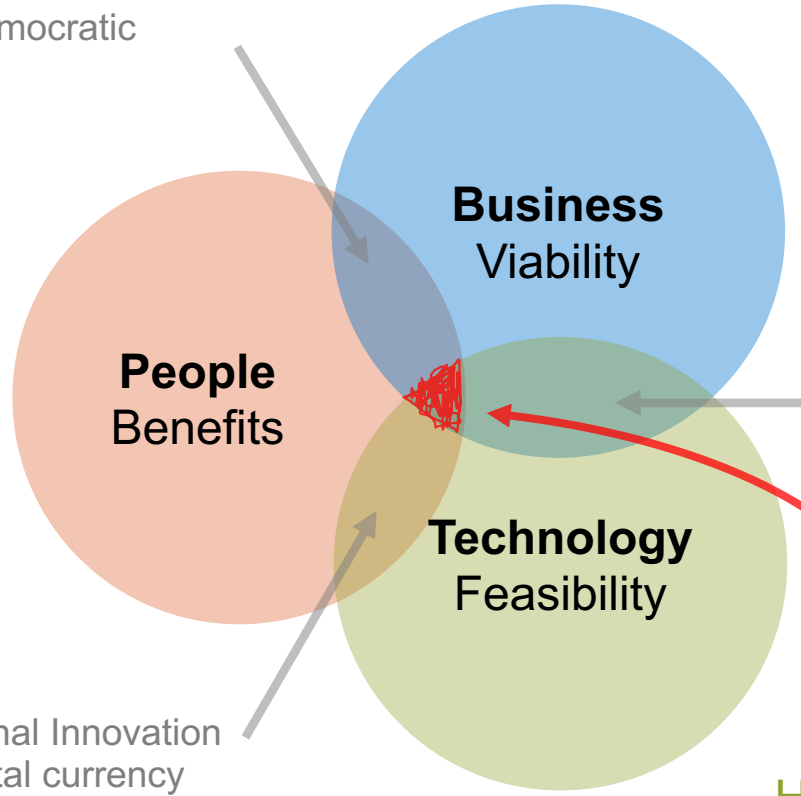
Outline

1. DLT and Blockchain Basics
   - Public Perception
   - Current and Future Use Cases of Blockchain Technology
2. From Smart Contracts to Blockchain-based Architectures
3. Blockchain-based Systems Engineering
4. Assessment of Blockchain Technology
   - Comparison to Established Centralized Solutions
   - Governance in Blockchain-based Systems

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

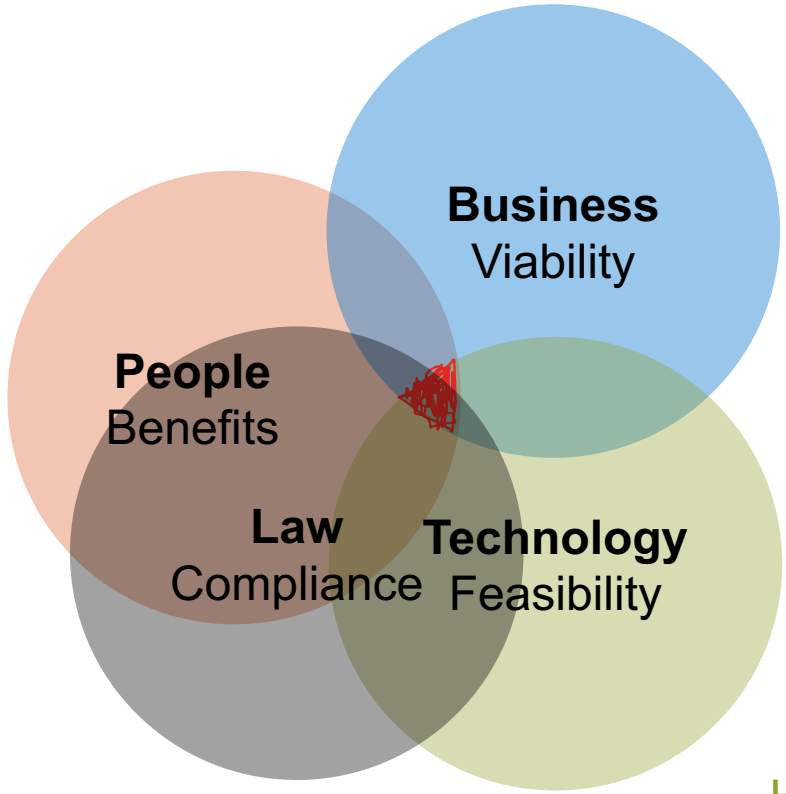
Functional Innovation
- Digital currency
- Digital token
- Digital wallets
- …

How to solve the problem?

Interdisciplinary Collaboration

How to create a sustainable business?

Which pain of which people / businesses do we solve?



How to ensure compliance with the law?

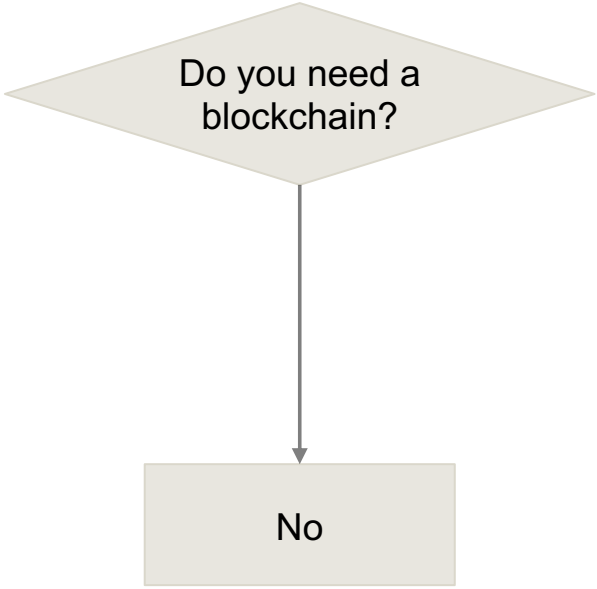
How to solve the problem?

Outline

1. DLT and Blockchain Basics
   - Public Perception
   - Current and Future Use Cases of Blockchain Technology
2. From Smart Contracts to Blockchain-based Architectures
3. Blockchain-based Systems Engineering
4. Assessment of Blockchain Technology
   - Comparison to Established Centralized Solutions
   - Governance in Blockchain-based Systems

Blockchain is not a Silver Bullet

The hype of blockchain has led to a large number of software applications using blockchain technology. Often these **proof-of-concepts** developed by startups or driven by innovation departments in enterprises, **never reach the production state**.



(Joke) Model by Dave Birch (https://twitter.com/dgwbirch?lang=de)

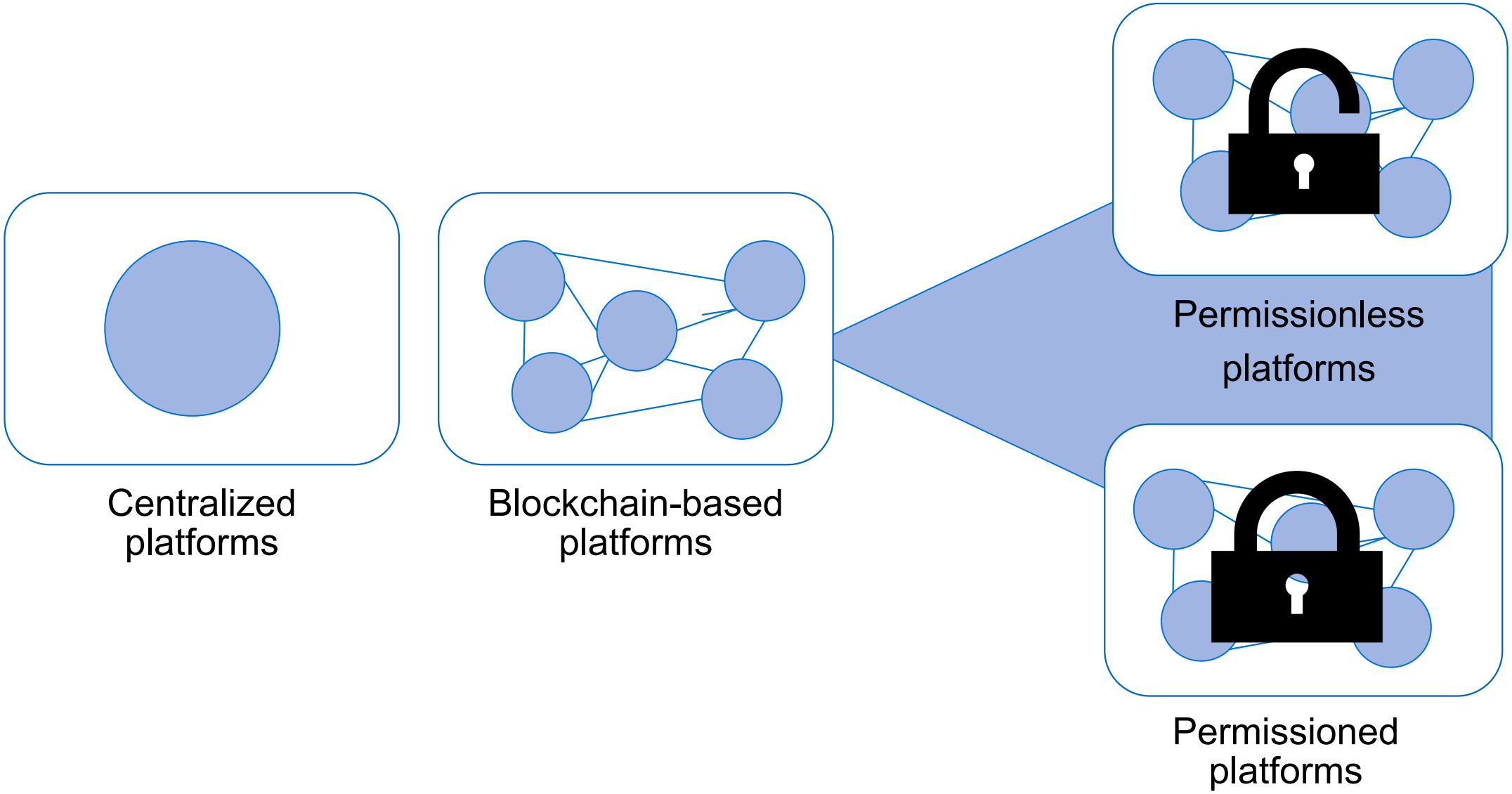
Finding a promising use case

- Understand the problem domain and the blockchain technology well
  - Blockchain might be a potential solution if:
    - Multiple parties are involved **and**
    - The parties do not trust each other or have different interests **and**
    - Shared write access is required **and**
    - All writes to the database need to be (publicly) verifiable

- Evaluate alternative solutions.

Search for blockchain decision tree

Comparison to Established Centralized Solutions



Comparison to Established Centralized Solutions (cont.)

Advantages

- Decentralized management (trust in one party ➔ trust in a system of multiple parties)
- Transparency of all transactions
- Traceability of the complete transaction history
- Pseudonymity of the wallet owners
- *Built-in* financial incentives for early adopters and network growth (➔ business model)

Opportunities

- Innovation thrust for IT solutions in the global finance system
- Lowered entry barriers for IT-savvy players with limited financial resources
- Impetus to re-evaluate established business models and economic mechanisms

Centralized Platforms

Benefits

- Efficient
- Scalable
- Standardized components

Drawbacks

- Requires **trust** in platform provider
  - Availability
  - Sufficient resources
  - Fair conditions (e.g. pricing)
  - No manipulations

There are established non-technical measures to ensure trust, e.g. cooperatives, third-party (or state) supervision, Open Source licenses, etc.

Permissionless Blockchain-based Platforms

Benefits

- Consensus of nodes on shared set of facts
- Traceability of the complete transaction history
- Optimized for cross-organization collaboration
- Decentralized and redundant

- (Transparency of all transaction details)
- Pseudonymity of the wallet owners
- Financial incentives for network growth

Drawbacks

- Dependency on a crypto currency
- Energy consumption
- Severely limited transaction throughput
- Risk of centralization at the network level

Permissioned Blockchain-based Platforms

Benefits

- Consensus of nodes on shared set of facts
- Traceability of the complete transaction history
- Optimized for cross-organization collaboration
- Decentralized and redundant

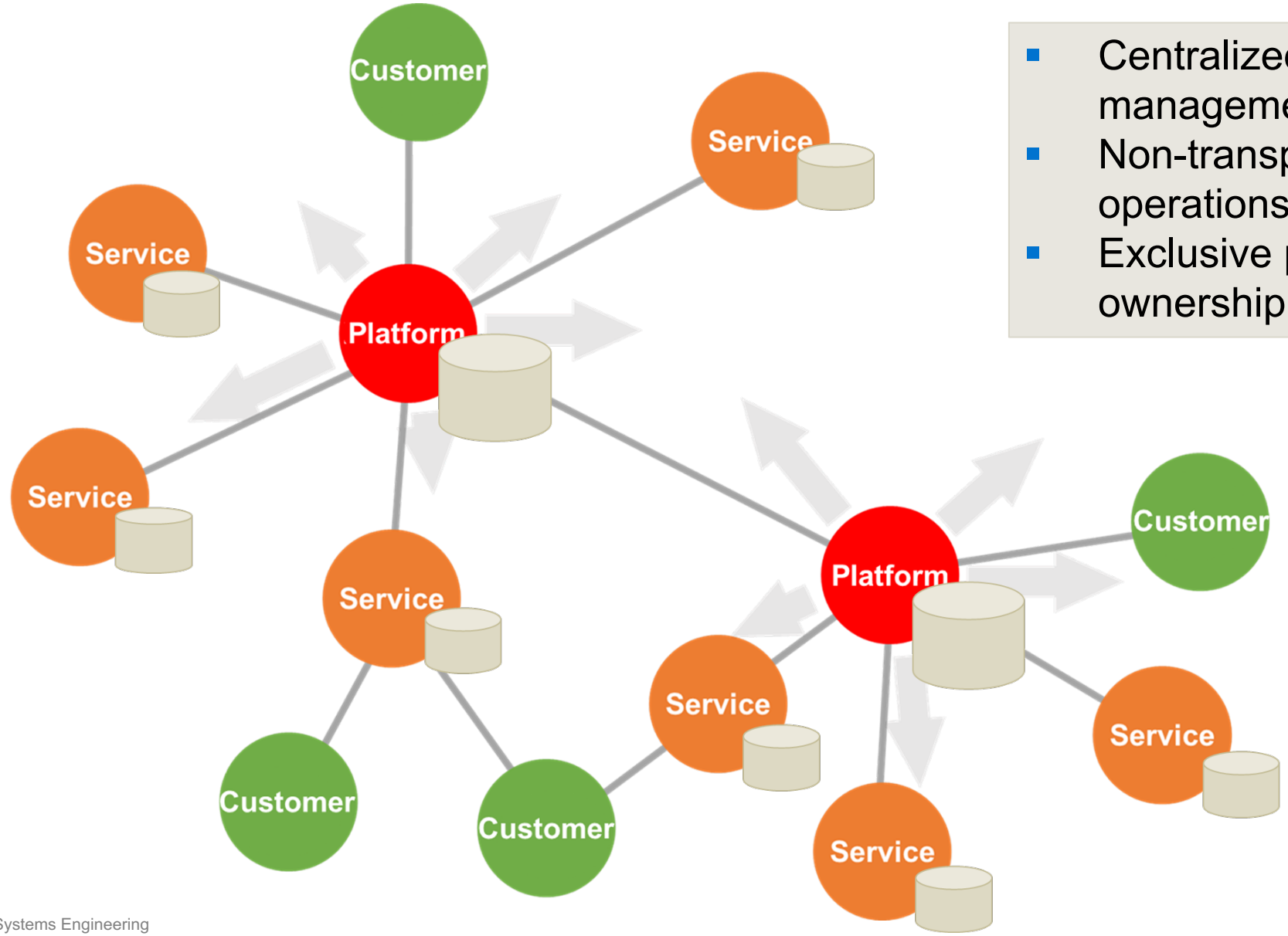
- Upward compatibility with established IT technologies
  - Identity management
  - Development tools
  - Data models & standards
  - …

Drawbacks

- Interoperability between different consortia
- System complexity
- Blockchain governance
  - Ecosystem / participants
  - Applications / contracts
  - Platform technology

The Governance Challenge

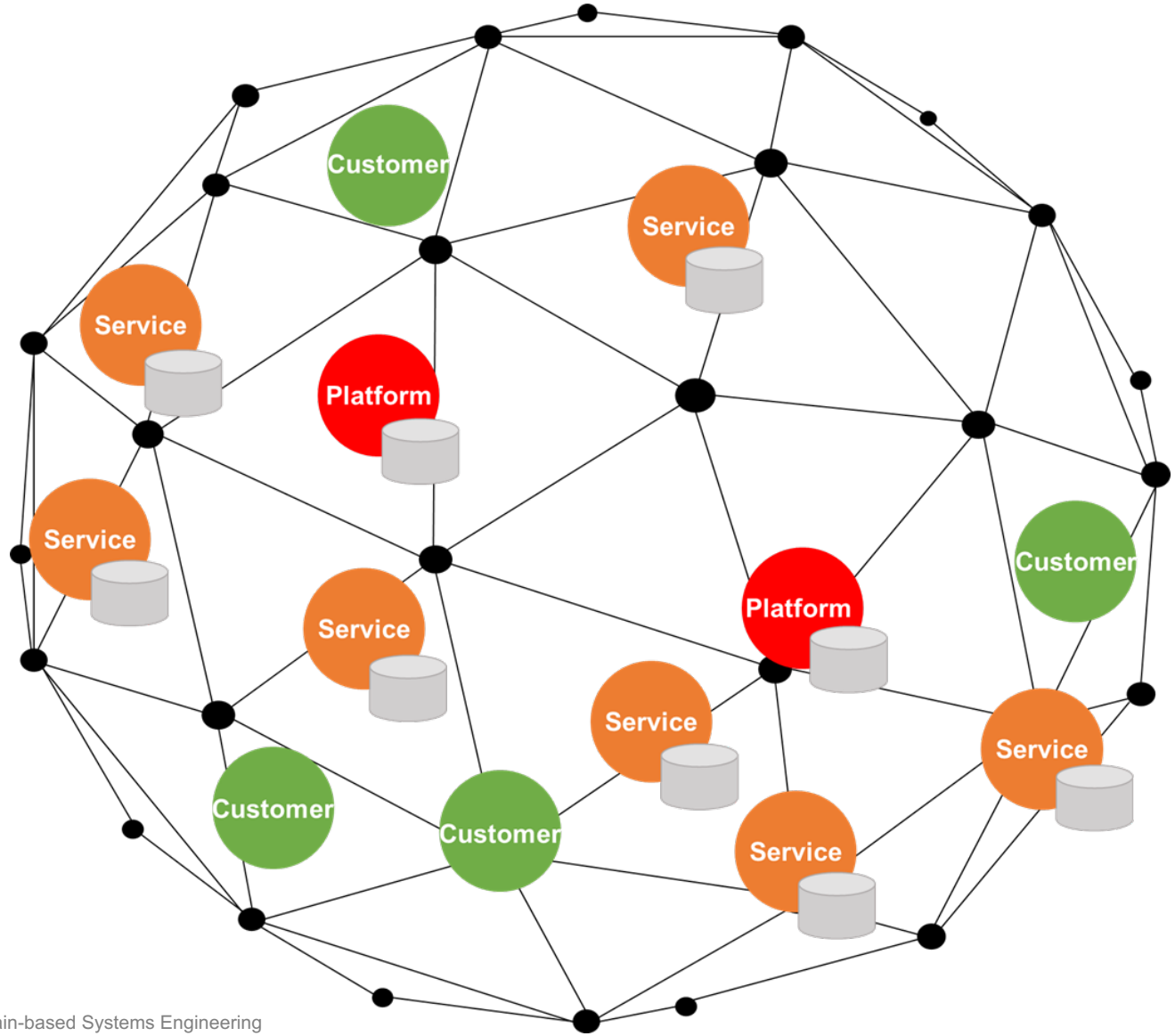
Centralized platforms today (e.g. Google Maps)



- Centralized data management
- Non-transparent platform operations
- Exclusive platform ownership

The Governance Challenge

Decentralized platforms tomorrow?



- Decentralized data management
- Transparent platform operations
- Shared platform ownership

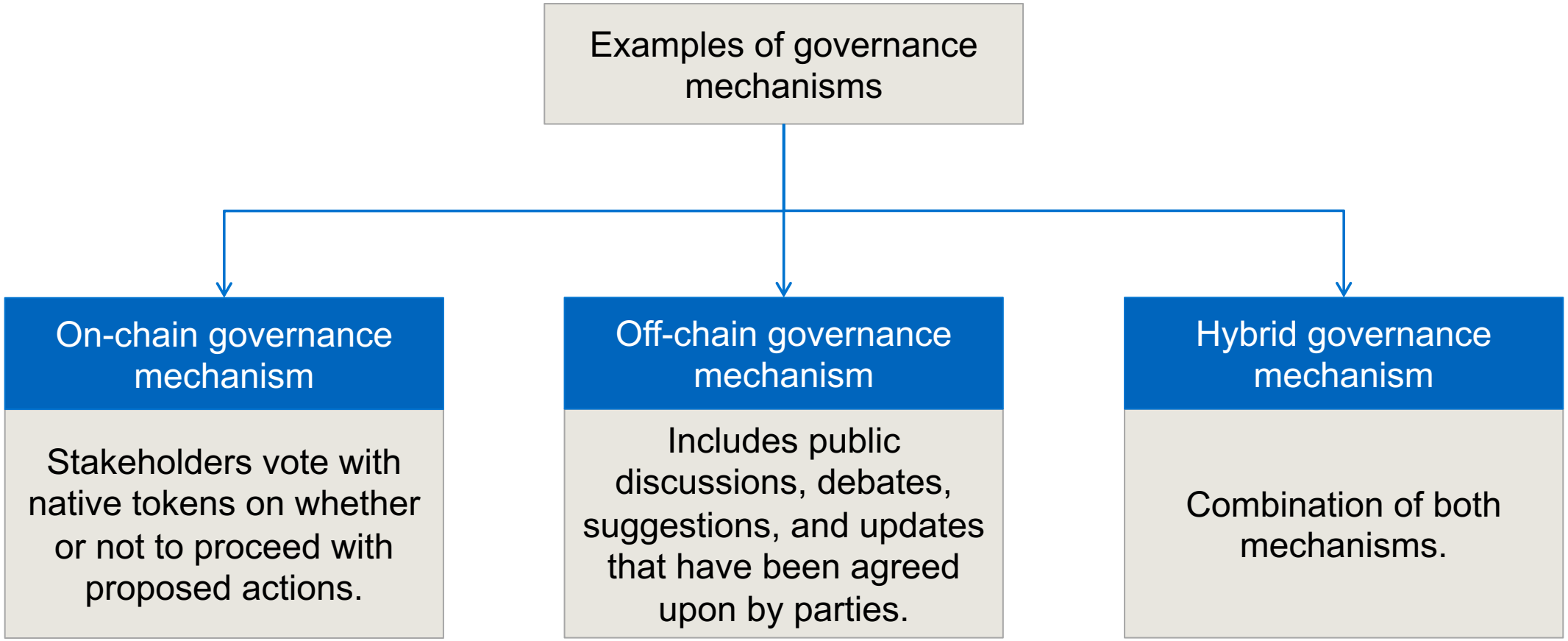
!

Blockchain Governance

- Ecosystem
- Applications
- Infrastructure

Governance in Blockchain-based Systems

- In blockchain-based systems, there is a lack of clarity on how the technology is/will be governed. Governance is the process by which a set of transaction and block verification rules are decided upon, implemented, and enforced, such that individuals adopt these rules for the verification of transactions.



Blockchains are a Team Sport

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

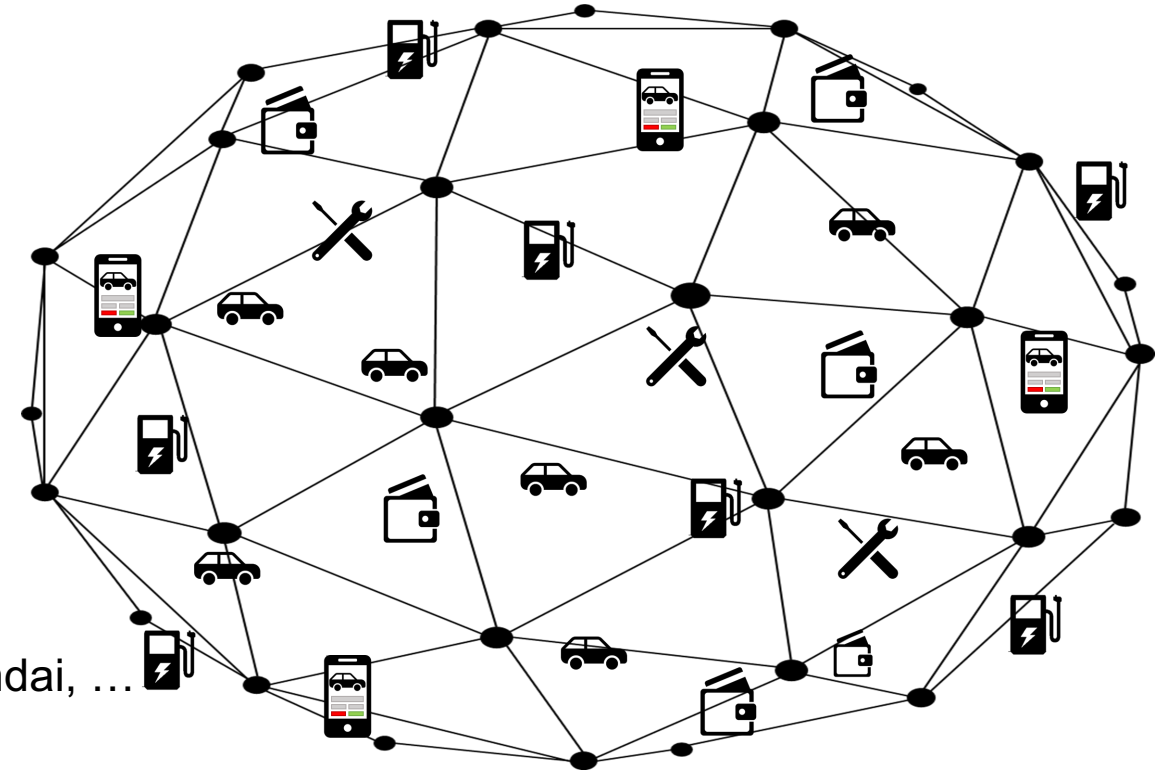
Banking: R3 Consortium (2014)

- 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, …

Connect, Understand, Design, Do, Learn: Blockchain Bayern (1/2019)

- Staatsministerium für Digitales, IHK München, Bayern Innovativ, >150 Members

Blockchain-based Architectures

Summary

Characteristics
- Focus on the precise, algorithmic descriptions of the rights and obligations of the contracting parties based on a shared state
- Trackability of all transactions
- Use of cryptographic methods
- Domain-specific languages
- Decentralized peer-to-peer execution environment

Drawbacks
- High execution costs
- Increased organizational and legal complexity
- Paradigm shifting for the development of new business models

Problems they do not address
- Correctness of input information
- Enforceability of rights outside the execution platform
- Correctness of the code

Our Current Projects on Blockchain-based Systems Engineering

Development projects

- Identity Issuance, Assurance, and Management in Decentralized Systems
- Chip Card Solutions, DRK: Securing blood products with RFID and blockchain-technologies
- Noumena Digital AG: Language Engineering for Smart Contracts
- Tr8cy: Peer2Peer Trade Financing Platform
- TUM: Digital university certificates
- Privacy Preservation in Data Marketplaces
- Enforcement of Cross-Organizational Workflows
- GAIA-X: Cross-company exchange of simulation data for highly automated driving functions

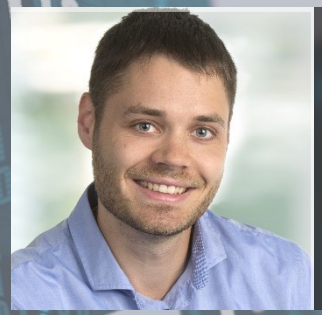
Education and consulting

- Lecture Blockchain-based Systems Engineering (you are here ;))
- Certified Blockchain & Distributed Ledger Technology Manager at TUM Executive Education
- GS1 Cologne: Blockchain Governance (Pallet exchange platform)
- Permissionless Blockchain-based platforms
- Blockchain Hackathons (IBM, TU Munich, Ethereum, …)
- Bavarian Ministries (Justice, Finance, Social)
- Associations (IHK, Münchner Kreis, **Blockchain Bayern**, …)

More information about research activities at TUM around blockchain:
https://www.blockchain.tum.de

BLOCKCHAIN
Bayern e.V.

Florian
Matthes
1. Vorstand



Alexander
Bogensperger

Julia
Christiansen

Maximilian
Irlbeck
2. Vorstand

Maximilian
Forster

Ulrich
Gallersdörfer

Christoph
Möslein
Schatzmeister

Franziska
Neuberger

Andreas
Zeiselmair