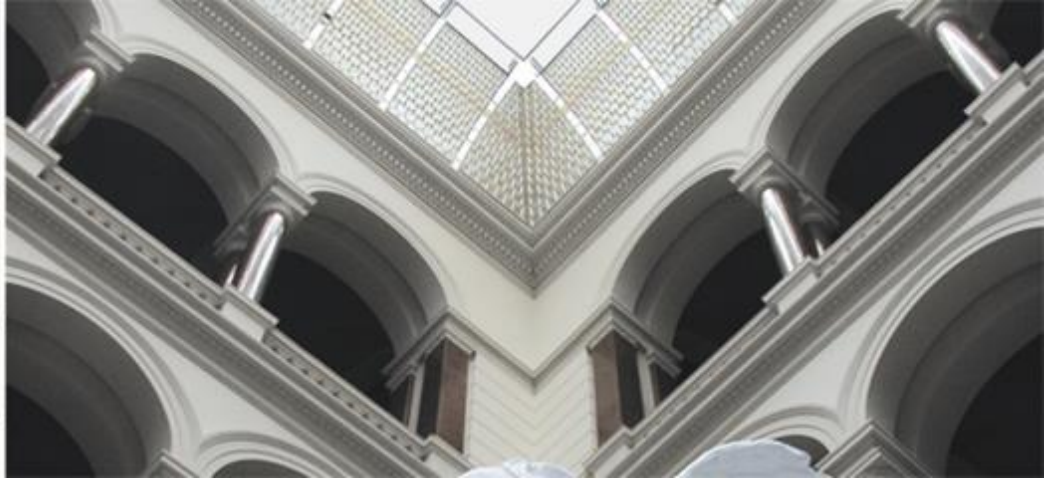
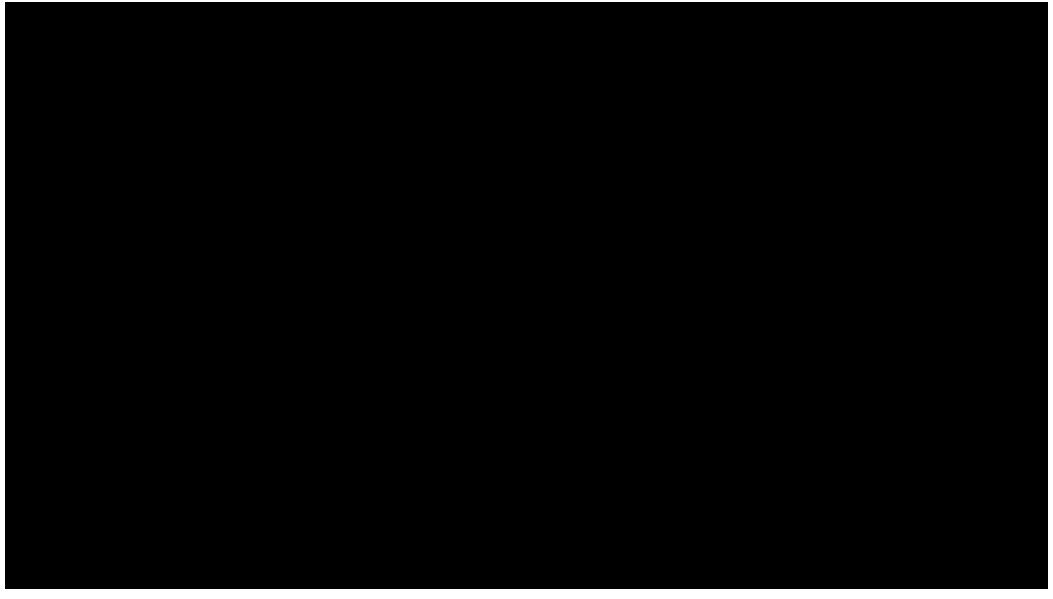


Blockchain and BPM

Guest Lecture in “Virtual Lecture Series on Business Process Management” @ Uni Würzburg

Prof. Dr. Ingo Weber | Chair for Software and Business Engineering
ingo.weber@tu-berlin.de | Twitter: @ingomweber

What is the Beef about Blockchain?



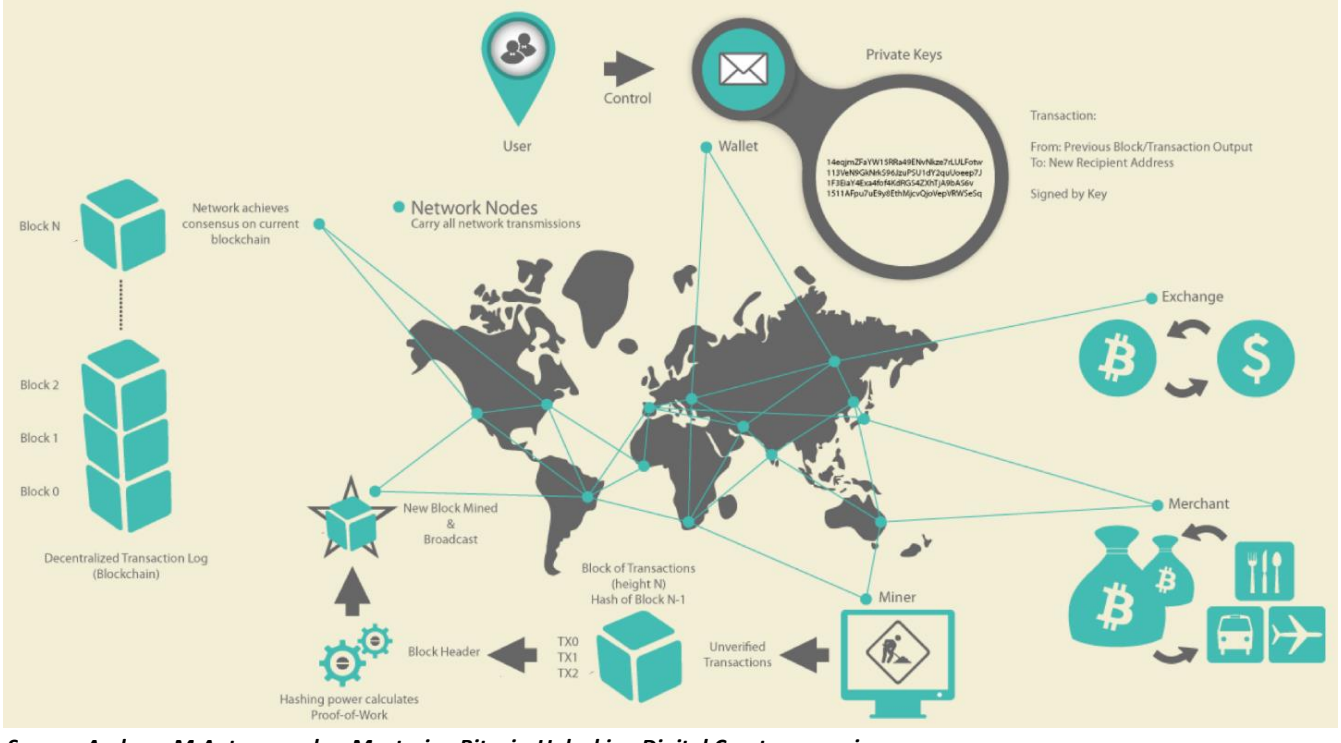
Video & reports:
https://www.data61.csiro.au/en/Our-Research/Focus-Areas/Distributed-Ledger-Technology-Blockchain

Bitcoin

First Cryptocurrency

Inventor: Satoshi Nakamoto (American? European? Denis Wright? Hal Finney?)

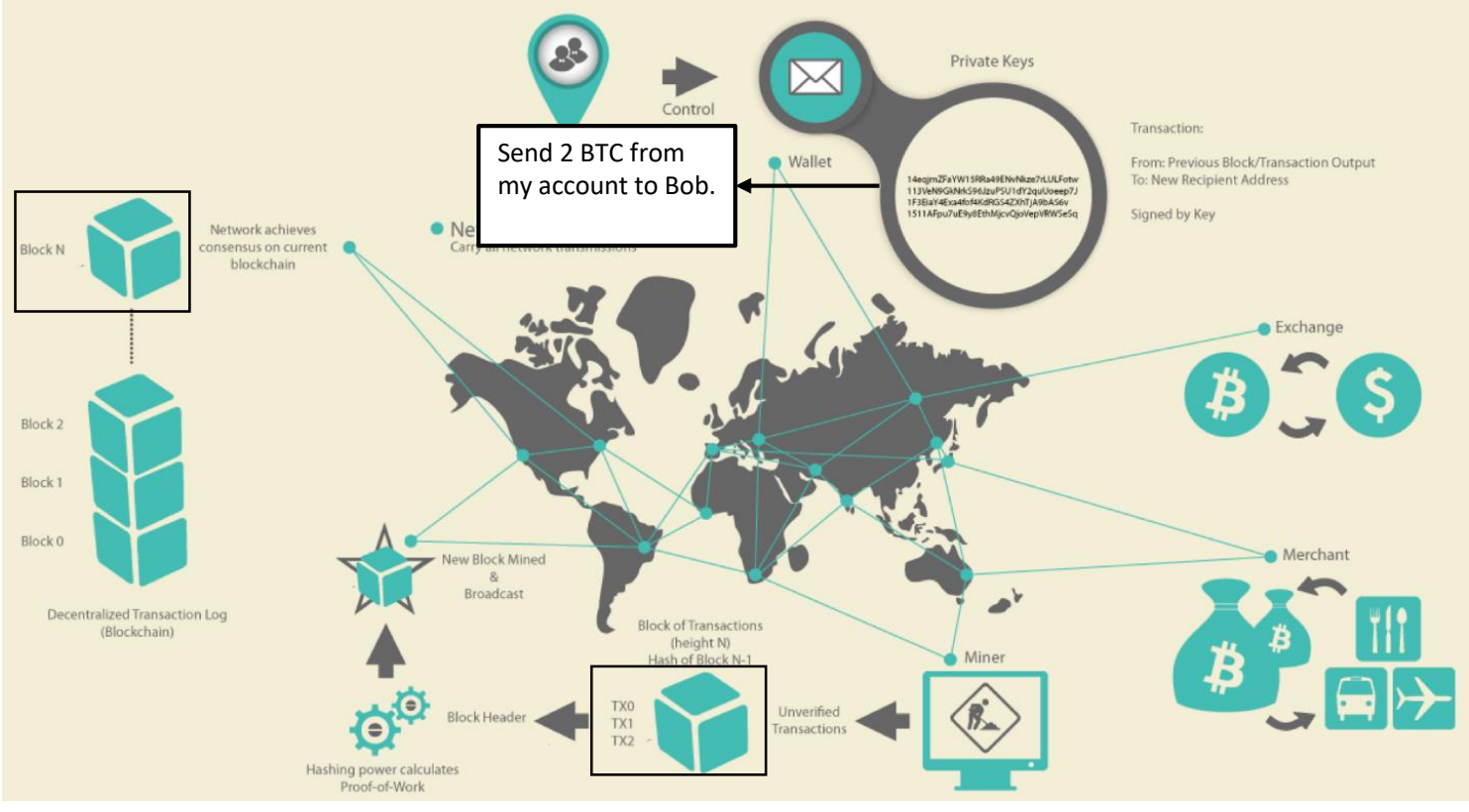
- A cryptocurrency operated on a p2p blockchain network
- 3 main types of participants
  - Users with wallets which contain keys to authenticate the transaction sent by the user using digital signature
  - Miners for producing blocks which store the validated transactions
  - Exchanges where users can trade bitcoin with other currencies



Source: Andreas M.Antonopoulos, Mastering Bitcoin-Unlocking Digital Cryptocurrencies

Bitcoin

Walkthrough



Users:

- create transactions,
- sign them, and
- announce them to network

Miners:

- receive transactions
- include them in a new block,
- (try to) append the new block to the data structure

When a transaction is part of the data structure, it has taken place (though it's a bit more complicated – probabilistic guarantees).

Blockchain 2nd gen – Smart Contracts

Technische Universität Berlin

- 1st gen blockchains: transactions are financial transfers

- Now Blockchain ledger can do that, and store/transact any kind of data

- Blockchain can deploy and execute programs: Smart Contracts
  - User-defined code, deployed on and executed by whole network
  - Can enact decisions on complex business conditions

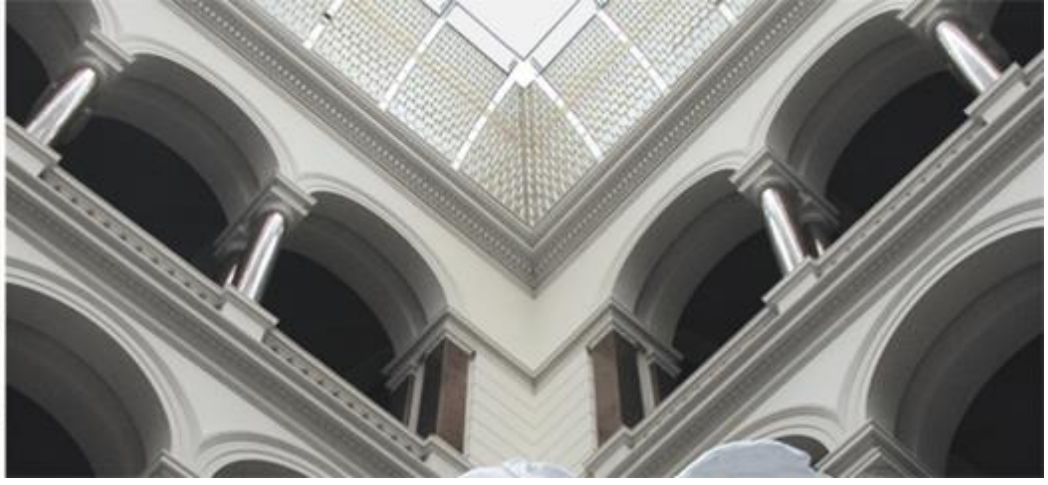
  - Can hold and transfer assets, managed by the contract itself
  - Ethereum: pay per assembler-level instruction

What is a Blockchain?

Visualization of a Blockchain: http://ethviewer.live

So what?

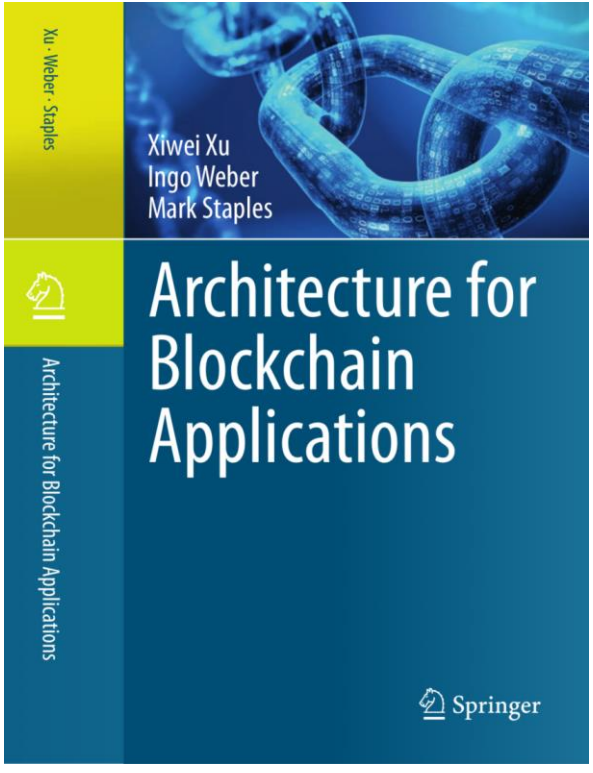
- Well, blockchains are exciting because they can be used as a new foundation for re-imagining systems:
  - a neutral infrastructure for processing transactions and executing programs
  - potentially interesting for innovation at **all touch-points** between organizations or individuals
  - ➢ **blockchain applications have the potential to disrupt the fabric of society, industry, and government**
- Blockchains can also be used as a technology platform to handle hard issues of data replication and system state synchronization with high integrity



Defining Blockchain

Technische Universität Berlin

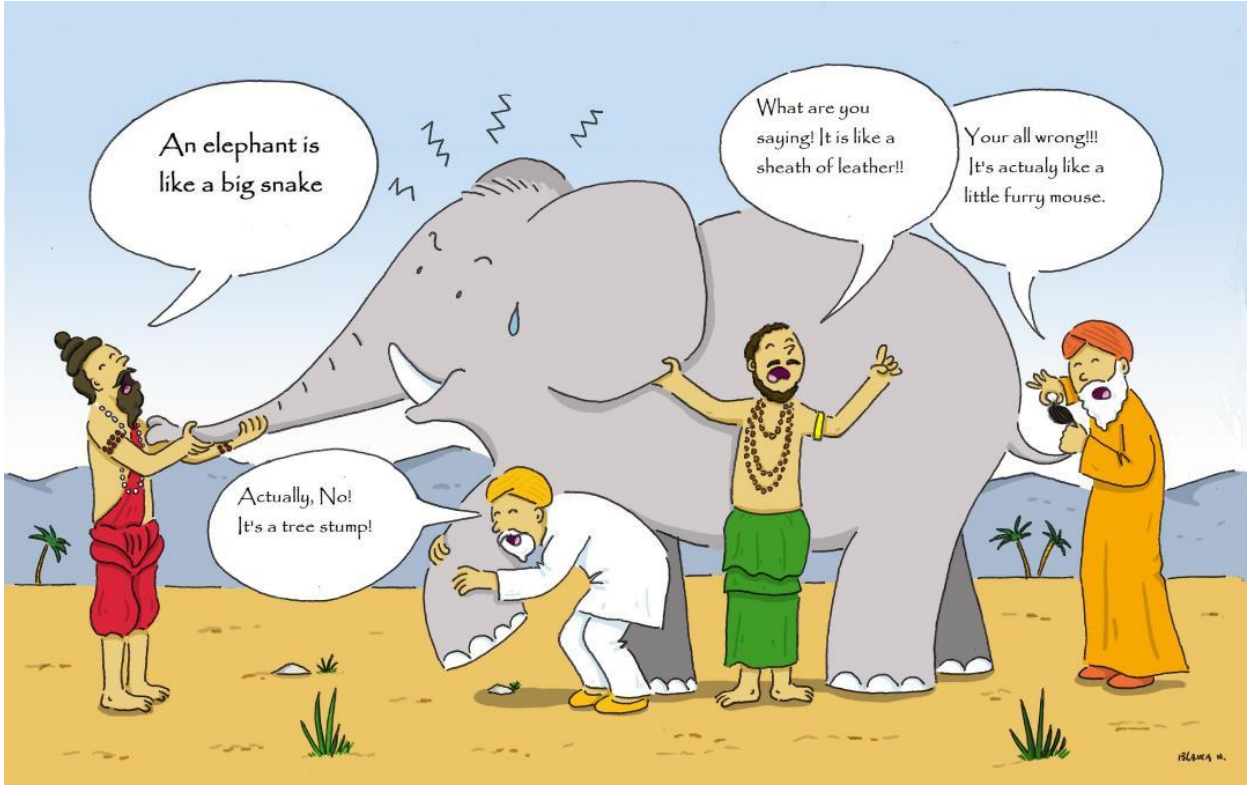
Book:
Architecture for Blockchain Applications



Xiwei Xu, Ingo Weber, Mark Staples. Architecture for Blockchain Applications. Springer, 2019.

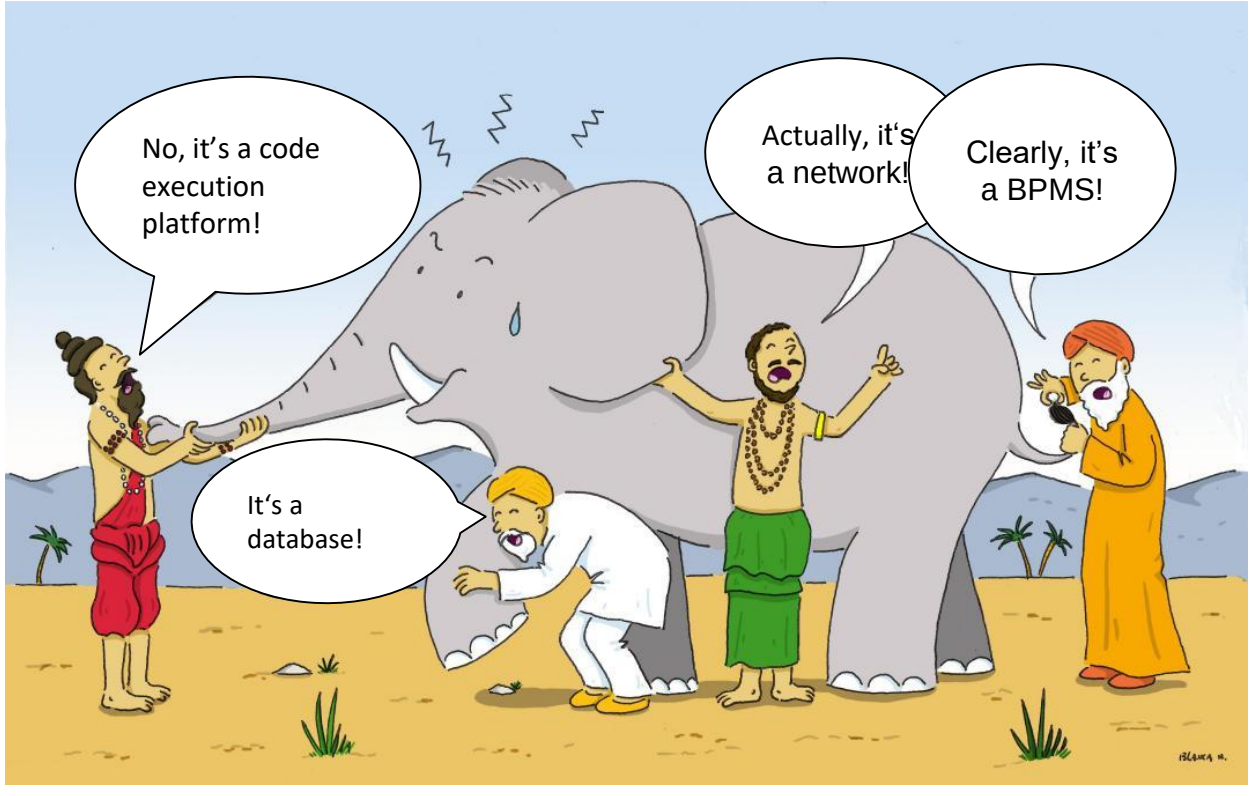
Includes definitions of blockchain (concept), DLT, smart contracts, etc.

What is a blockchain?



Parable of the blind men and the elephant, see e.g., https://wildequus.org/2014/05/07/sufi-story-blind-men-elephant/ (source of figure)

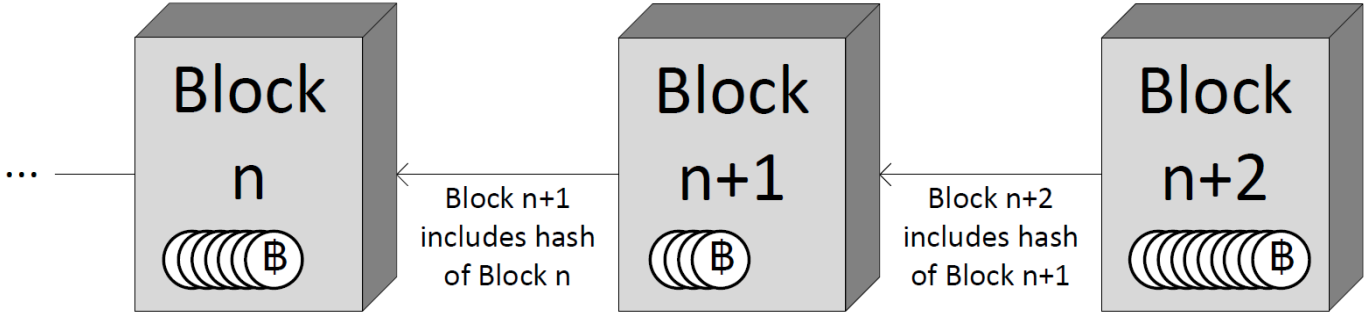
What is a blockchain?



Parable of the blind men and the elephant, see e.g., https://wildequus.org/2014/05/07/sufi-story-blind-men-elephant/ (source of figure)

Defining Blockchain (1)

- **Distributed Ledger**
  - An “append-only” transaction store distributed across machines *(immutability)*
  - A new transaction might reverse a previous transaction, but both remain part of the ledger
- **Blockchain**
  - A distributed ledger structured into a linked list of blocks
  - Each block contains an ordered set of transactions
  - Use cryptographic hashes to secure the link from a block to its predecessor



Defining Blockchain (2)

Technische Universität Berlin

- A **Blockchain System** consists of
  - A blockchain network of nodes
  - A blockchain data structure
    - For the ledger replicated across the blockchain network
    - Full nodes hold a full replica of the ledger
  - A network protocol
    - Defines rights, responsibilities, and means of communication, verification, validation, and consensus across the nodes in the blockchain network
    - Includes ensuring authorisation and authentication of new transactions, mechanisms for appending new blocks, incentive mechanisms

Defining Blockchain (3)

Technische Universität Berlin

- A **Public Blockchain** is a blockchain system with the following characteristics:
  - Has an open network
    - Nodes can join and leave without requiring permission from anyone
  - All full nodes can verify new transactions and blocks
  - Incentive mechanism to ensure the correct operation
    - Valid transactions are processed and included in the ledger and invalid transactions are rejected
- A **Blockchain Platform** is the technology needed to operate a blockchain
  - Blockchain client software for processing nodes
  - The local data store
  - Alternative clients to access the blockchain network

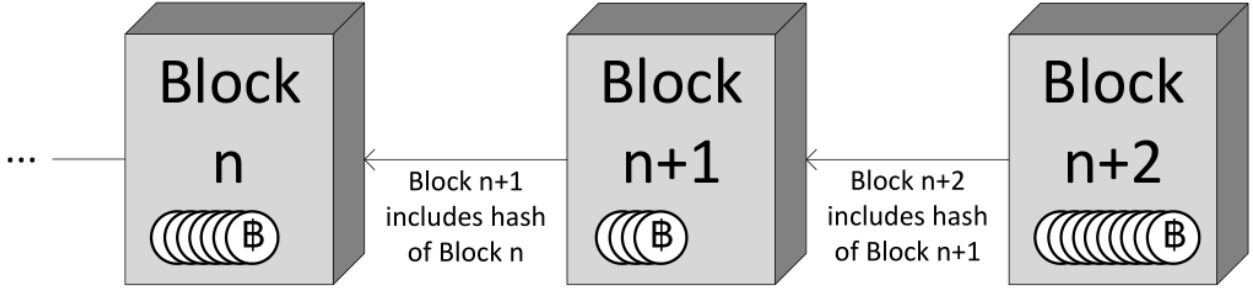
Decentralised Applications and Smart Contracts

Technische Universität Berlin

- **Smart contracts**
  - Programs deployed as data and executed in transactions on the blockchain
  - Blockchain can be a computational platform (more than a simple distributed database)
  - Code is deterministic and immutable once deployed
  - Can invoke other smart contracts
  - Can hold and transfer digital assets
- **Decentralized applications** or **dapps**
  - Main functionality is implemented through smart contracts
  - Backend is executed in a decentralized environment
  - Frontend can be hosted as a web site on a centralized server
    - Interact with its backend through an API
  - Could use decentralized data storage such as IPFS
  - "State of the dapps" is a directory recorded on blockchain: https://www.stateofthedapps.com/

Blockchain defined (1/4)
Verbatim from the Book

- **Definition 1 (Distributed Ledger).** A Distributed Ledger is an *append-only store of transactions* which is distributed across many machines.
- **Definition 2 (Blockchain (Concept)).** A Blockchain is a *distributed ledger* that is structured into a *linked list of blocks*. Each block contains an ordered set of transactions. Typical solutions use cryptographic hashes to secure the link from a block to its predecessor.



Blockchain defined (2/4)
Verbatim from the Book

Technische Universität Berlin

- **Definition 3 (Blockchain System).** A Blockchain System consists of:
  - a *blockchain network* of machines, also called *nodes*;
  - a *blockchain data structure*, for the ledger that is replicated across the blockchain network. Nodes that hold a full replica of this ledger are referred to as *full nodes*;
  - a network *protocol* that defines rights, responsibilities, and means of communication, verification, validation, and consensus across the nodes in the network. This includes ensuring *authorization and authentication* of new transactions, mechanisms for appending new blocks, incentive mechanisms (if needed), and similar aspects.

Blockchain defined (3/4)
Verbatim from the Book

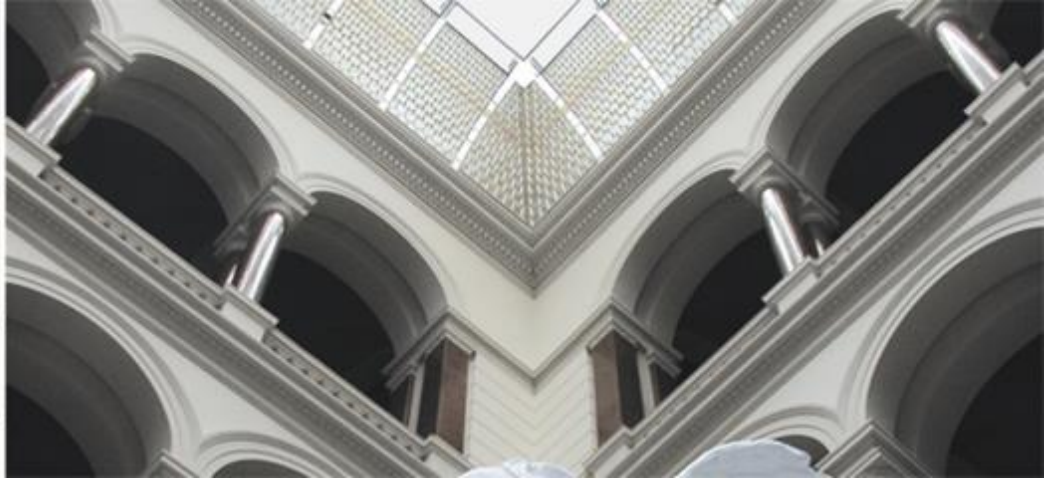
Technische Universität Berlin

- **Definition 4 (Public Blockchain).** A Public Blockchain is a *blockchain system* that has the following characteristics:
  - it has an *open network* where nodes can join and leave as they please without requiring permission from anyone;
  - all full nodes in the network can *verify each new piece of data* added to the data structure, including blocks, transactions, and effects of transactions; and
  - its protocol includes an *incentive mechanism* that aims to ensure the correct operation of the blockchain system including that valid transactions are processed and included in the ledger, and that invalid transactions are rejected.

Blockchain defined (4/4)
Verbatim from the Book

Technische Universität Berlin

- **Definition 5 (Blockchain Platform).** A blockchain platform is the *technology needed to operate a blockchain*. This comprises the blockchain client software for processing nodes, the local data store for nodes, and any alternative clients to access the blockchain network.
- **Definition 6 (Smart Contract).** Smart contracts are *programs* deployed as data in the blockchain ledger, and executed in transactions on the blockchain. Smart contracts can *hold and transfer digital assets* managed by the blockchain, and can invoke other smart contracts stored on the blockchain. Smart contract code is *deterministic and immutable* once deployed.
- **Definition 7 (dapp).** A decentralized application or dapp is a software system that is designed to provide its main functionality through smart contracts.

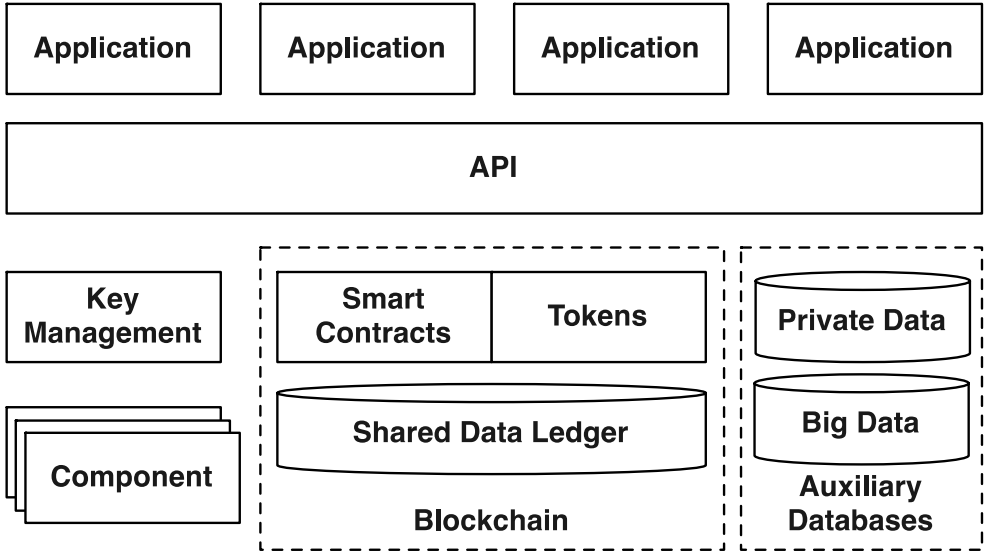


Overview: Blockchain Applications and Architecture

Technische Universität Berlin

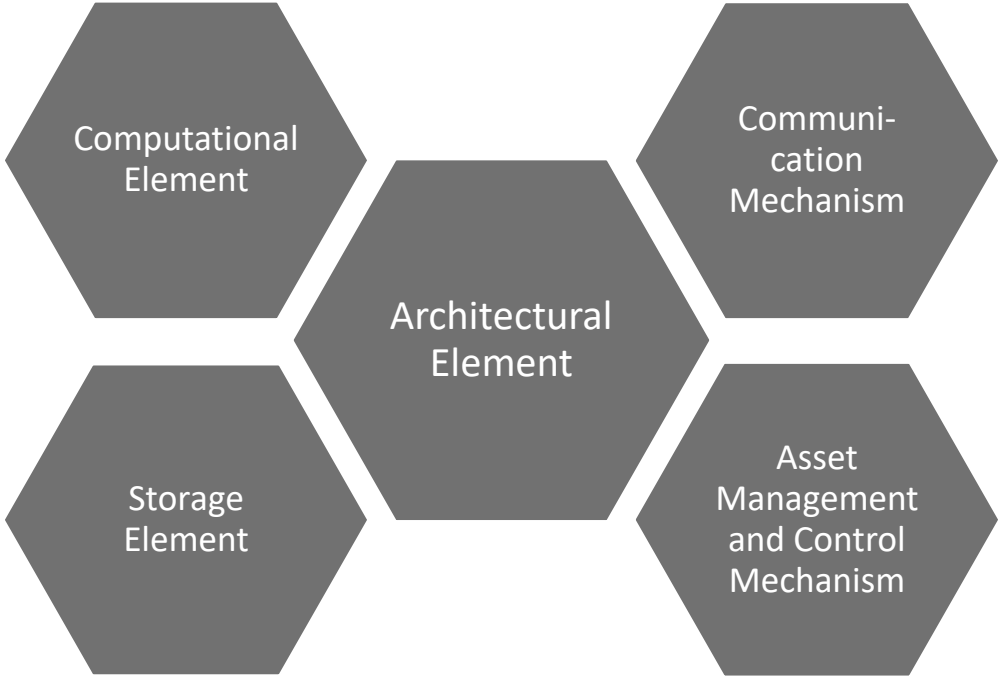
Context: Blockchain Applications

- Blockchain can be a component of a big software system
- Communicate with other components within the software system



Functions blockchain can provide in an application architecture

- Blockchain as…

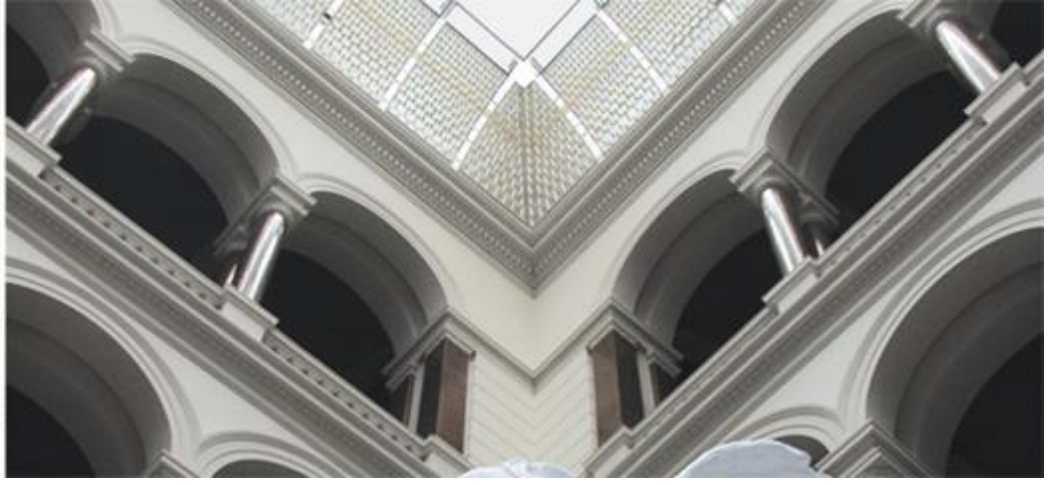


Non-Functional Trade-Offs

- Compared to conventional database & script engines, blockchains have:
  - (-) Confidentiality, Privacy
  - (+) Integrity, Non-repudiation
  - (+ read/ - write) Availability

  } Security: combination of CIA properties

  - (-) Modifiability
  - (-) Throughput / Scalability / Big Data
  - (+ read/ - write) Latency



BPM: Process Execution on Blockchain

Technische Universität Berlin

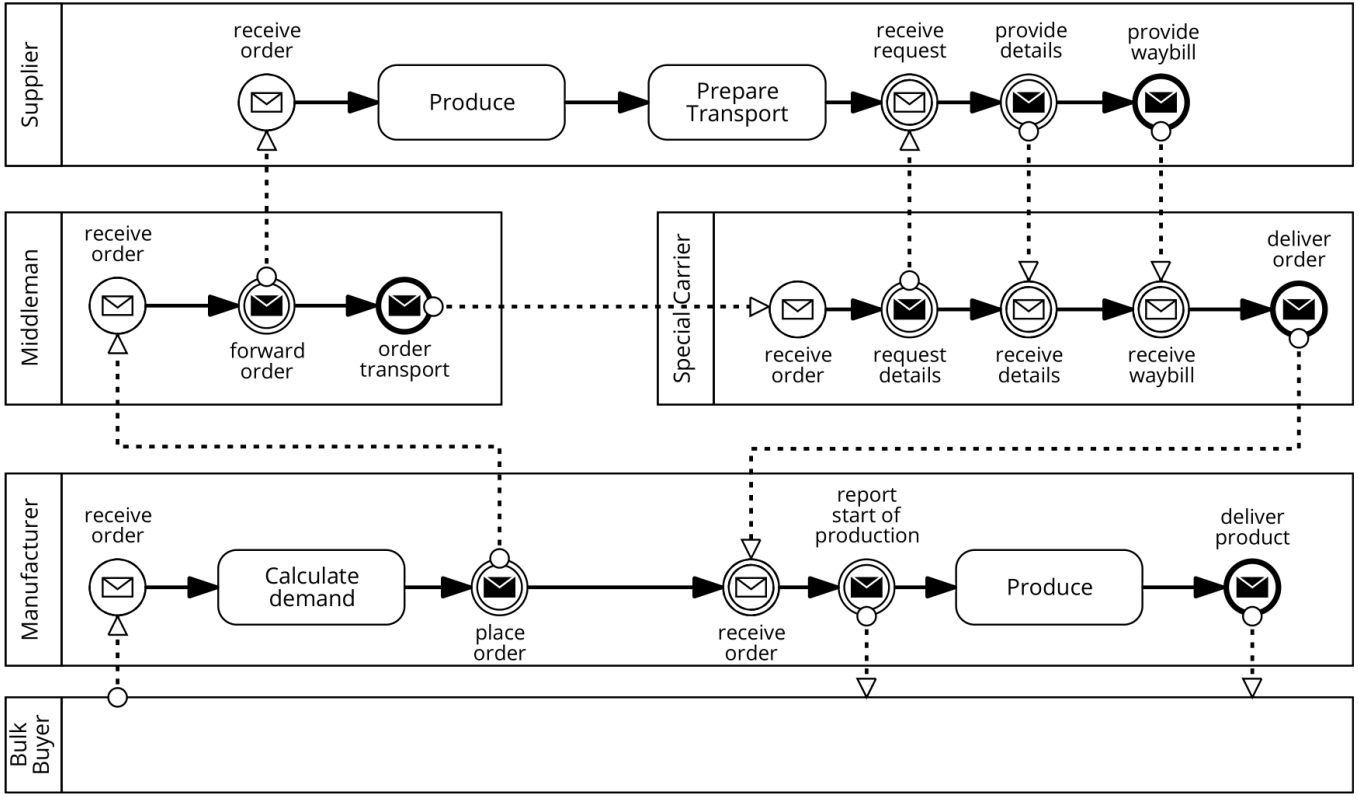
Business Processes on Blockchain – Motivation

- Integration of business processes across organizations: a key driver of productivity gains
- Collaborative process execution
  - Doable when there is trust – supply chains can be tightly integrated
  - Problematic when involved organizations have a **lack of trust** in each other
    → if 3+ parties should collaborate, where to execute the process that ties them together?
    - Can any participant be trusted with operating an authoritative database?
- Cross-organizational processes: by now a common use case for blockchain applications

Motivation: Example

Issues:

- Knowing the status, tracking correct execution
- Handling payments
- Resolving conflicts



Approach (Weber 2016) in a Nutshell

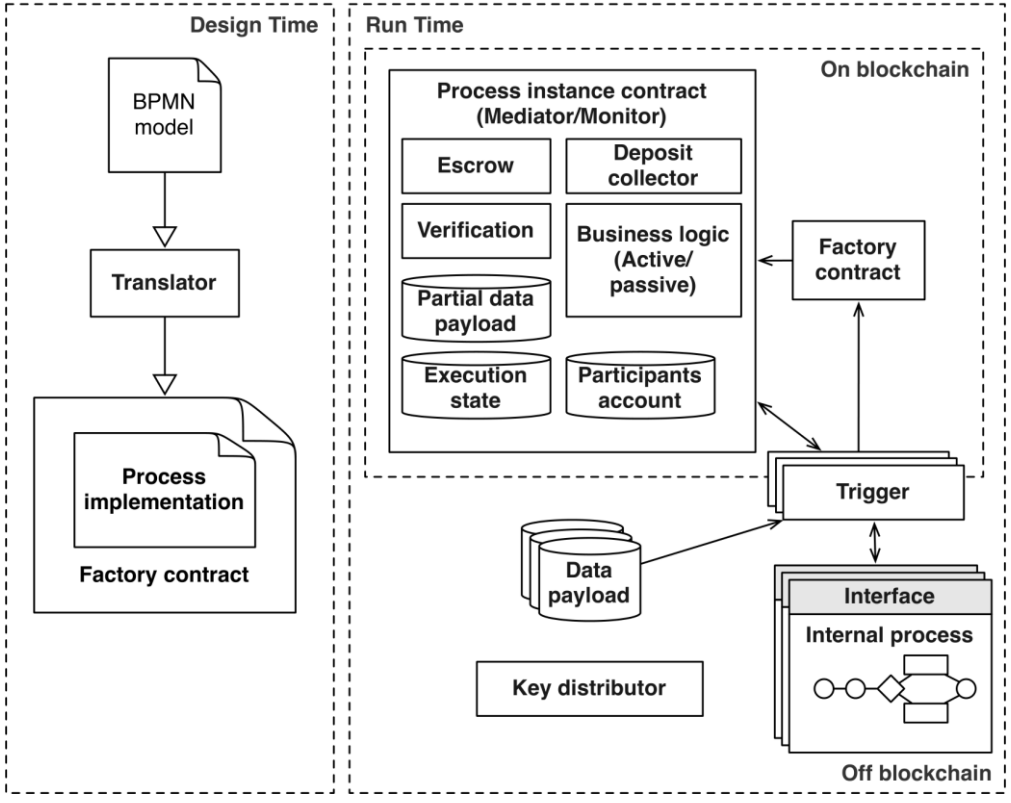
- Goal: execute collaborative business processes as smart contracts
  - Translate (enriched) BPMN process models to smart contract code → Model-driven engineering (MDE)
  - Triggers act as bridge between Enterprise world and blockchain
  - Smart contract provides:
    - Independent, global process monitoring
    - Process enforcement: messages are only accepted if they are expected, given the state of the process, and only if sent from the participant playing the respective role
    - Automatic payments & escrow
    - Data transformation
    - Encryption

Advantages of MDE vs. coding in the blockchain context

Technische Universität Berlin

- Code generation can implement best practices and well-tested building blocks
  - Code can adhere to blockchain “standards” (like ERC-20, ERC-721, …)
- Improved productivity, especially for novices in a particular technology
  - However: someone should understand the code and review it
- Models can be independent of specific blockchain technologies or platforms
  - Avoid lock-in to specific blockchain technologies
- Models are often easier to understand than code – particularly useful in communicating with business partners about smart contracts
  - Facilitates building trust
  - Domain experts can understand how their ideas are represented in the system
- With my former team at Data61, we used MDE in all blockchain industry projects, in 2/3rds of the cases also process models

Architecture

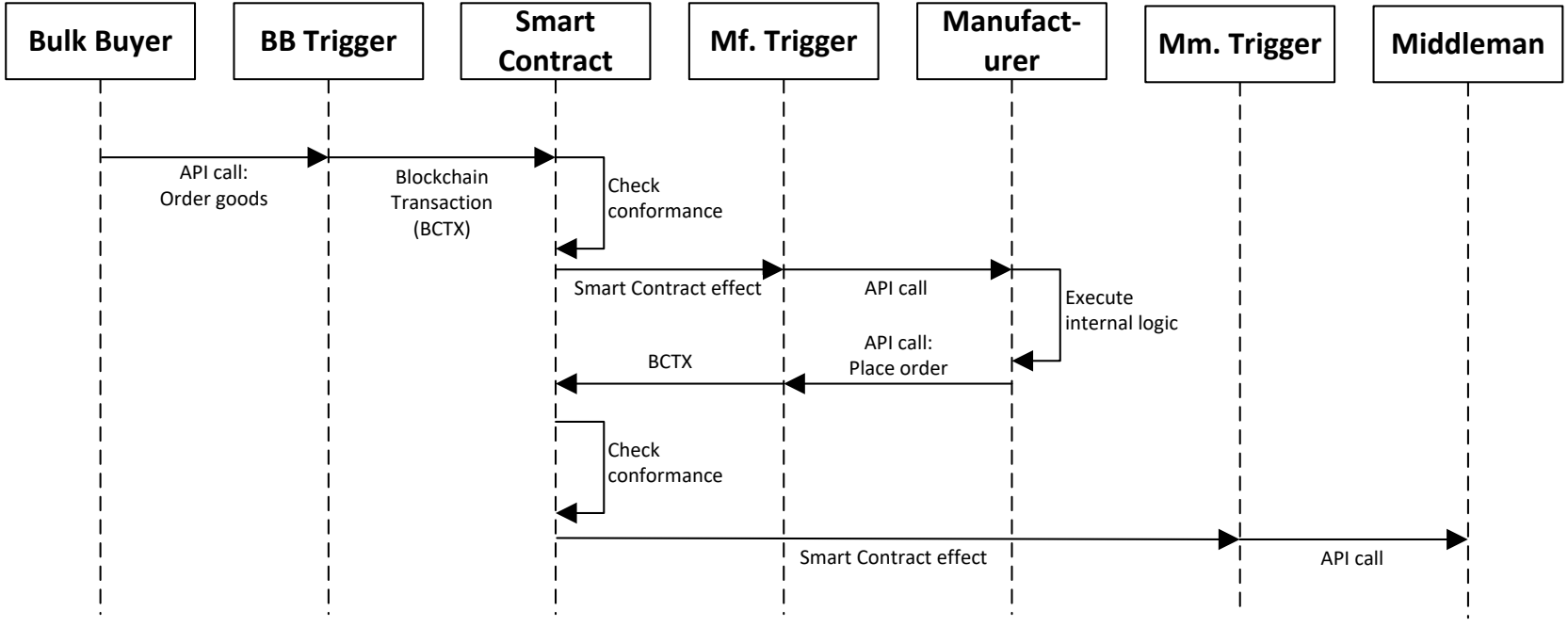


Runtime

- Instantiation:
  - New *instance contract* per process instance
  - Assign blockchain accounts to roles during initialization
  - Exchange keys and create secret key for the instance
- Messaging:
  - Instead of sending direct WS calls: send through triggers & smart contract
  - Instance contract handles:
    - Global monitoring
    - Process enforcement (conformance checking)
    - Automated payments
    - Data transformation

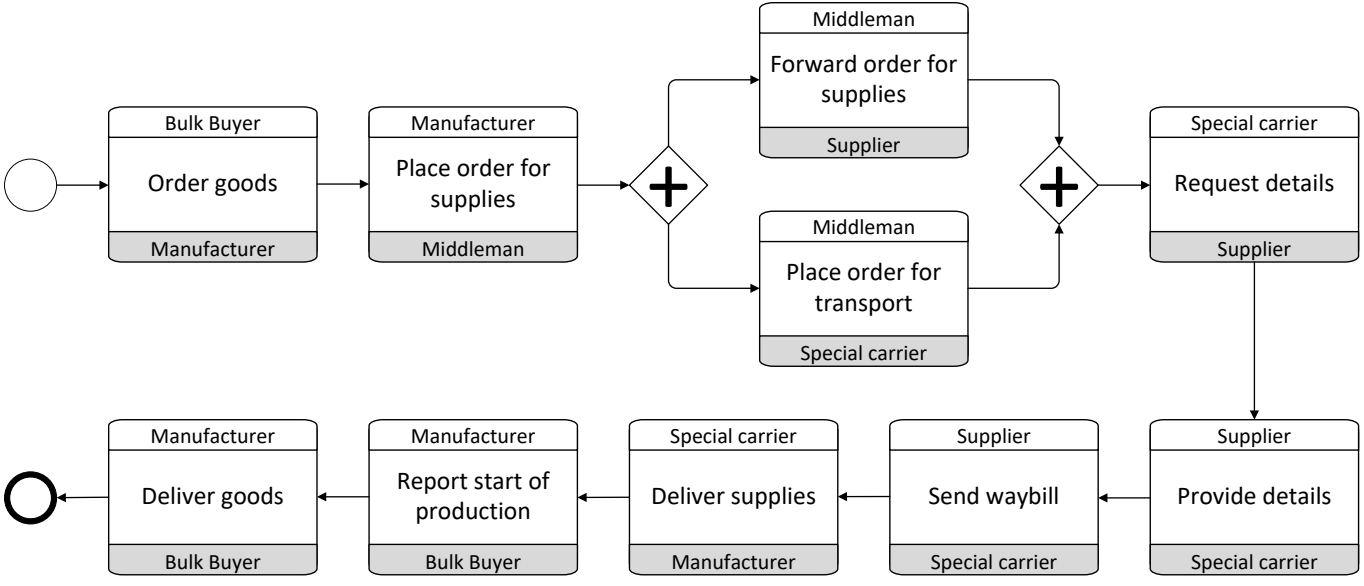
Runtime

- Instantiation:
  - New *instance contract* per process instance



Translator

- Translate subset of BPMN elements to *Solidity*
  - BPMN Choreography diagrams or regular BPMN models with lanes



Caterpillar Design Principle: Models with a Single Pool

- Model the collaborative process as if it were an intra-organizational business process executed on top of a traditional BPMS
  - In other words, the collaborative process is modelled as if all the parties shared the same process execution infrastructure (the blockchain)

→Model as a single-pool BPMN Process Diagram

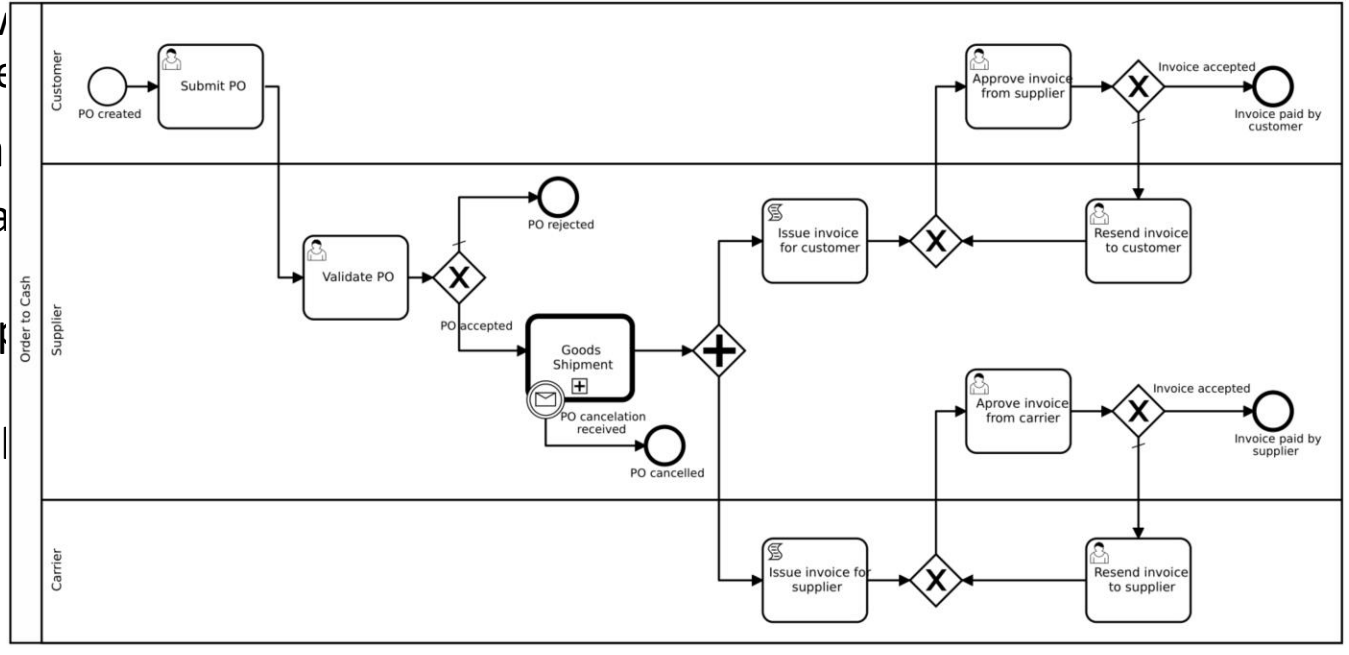
  - not a collaborative process or a choreography where parties communicate via messages
  - Each independent party in the process is represented as a lane
  - Hand-offs between parties are simply represented via sequence flows that go from one lane to another (and not via messages).

Caterpillar Design Principle: Models with a Single Pool

- Model the collaborative process as if it were an intra-organizational business process executed on top of a traditional BPMS
  - In other w
    shared the

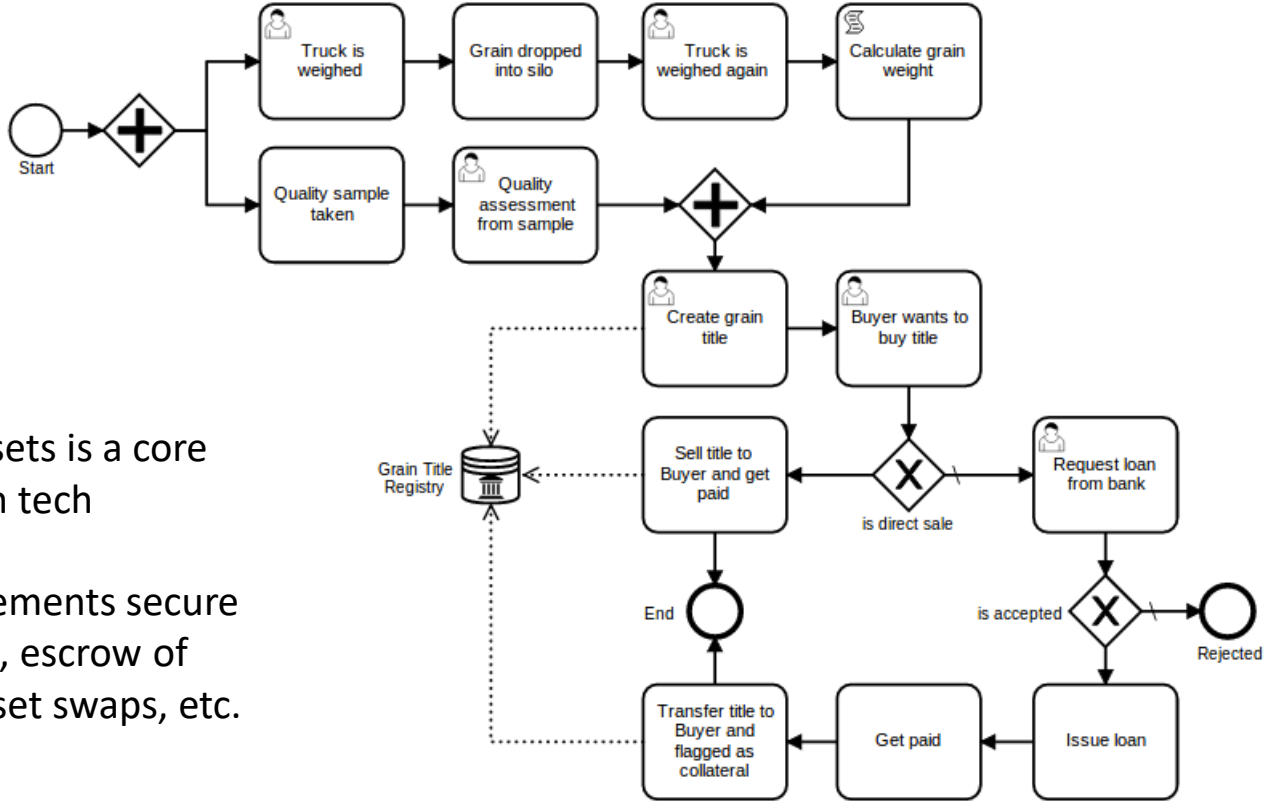
→Model as a

  - not a colla
    messages
  - Each indep
  - Hand-offs
    from one



Combining process and data/token models

Technische Universität Berlin

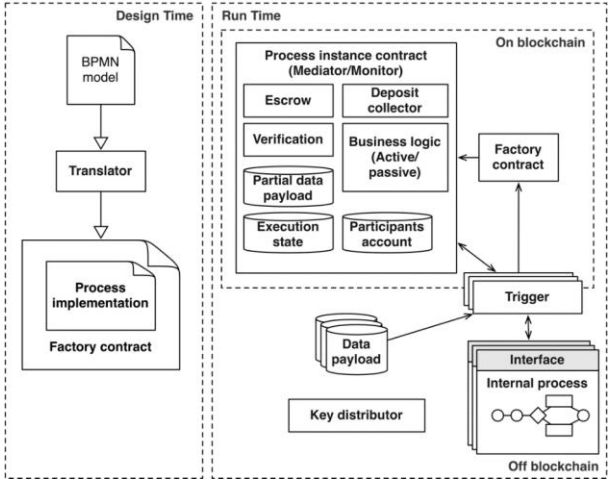


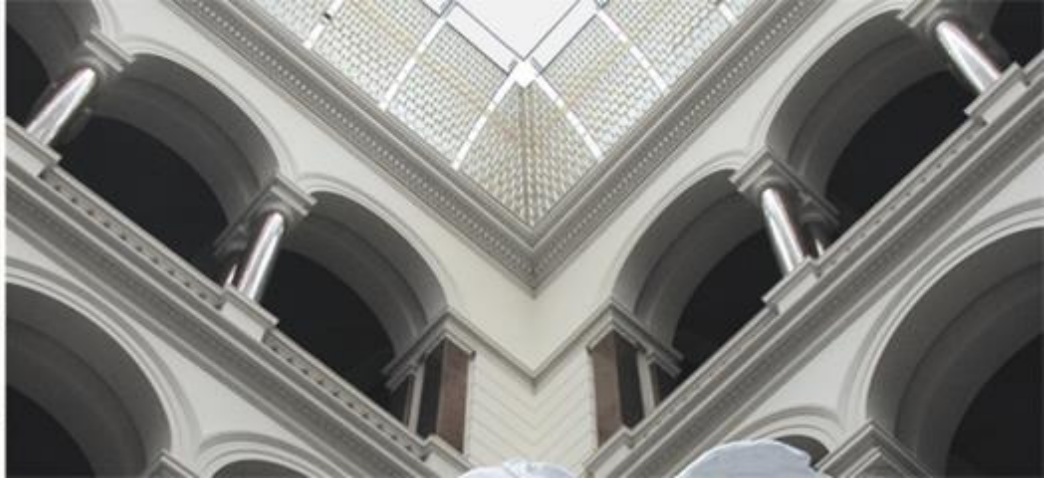
Managing (virtual) assets is a core strength of Blockchain tech

Generated code implements secure methods for payment, escrow of money and assets, asset swaps, etc.

BPM & Model-driven Engineering

- Business Process Execution & Analysis
  - **Untrusted business process monitoring and execution using blockchain**, I. Weber, X. Xu, R. Riveret et al., BPM 2016
  - **Optimized Execution of Business Processes on Blockchain**, L. García-Bañuelos, A. Ponomarev, M. Dumas, I. Weber, BPM 2017
  - **Caterpillar: A blockchain-based business process management system,** O. López-Pintado, L. García-Bañuelos, M. Dumas, I. Weber, BPM 2017 Demo
  - **Runtime verification for business processes utilizing the Bitcoin blockchain,** C. Prybila, S. Schulte, C. Hochreiner, I. Weber, FGCS 2018
  - **Dynamic role binding in blockchain-based collaborative business processes,** O. López-Pintado, M. Dumas, L. García-Bañuelos, I. Weber CAISE 2019
  - **Interpreted execution of business process models on blockchain.** O. López-Pintado, M. Dumas, L. García-Bañuelos, I. Weber. EDOC 2019
  - **Modeling and enforcing blockchain-based choreographies.** J. Ladleif, M. Weske, I. Weber. BPM 2019
  - **Mining blockchain processes: Extracting process mining data from blockchain applications.** C. Klinkmüller, A. Ponomarev, A.B. Tran, I. Weber, and Wil van der Aalst. BPM Blockchain Forum 2019 - Best Paper Award
- Data / Asset Modeling
  - **Regerator: a Registry Generator for Blockchain,** A. B. Tran, X. Xu, I. Weber, CAISE 2017 Demo
- Combined Asset & Process Modeling
  - **Lorikeet: A Model-Driven Engineering Tool for Blockchain-Based Business Process Execution and Asset Management** A. B. Tran, Q. Lu, I. Weber, BPM 2018 Demo
  - Integrated model-driven engineering of blockchain applications for business processes and asset management. Q. Lu, A. B. Tran, I. Weber et al. SPE journal, October 2020. In press, accepted.





Thank you for your attention

Blockchain and BPM

Guest Lecture in “Virtual Lecture Series on Business Process Management” @ Uni Würzburg

Prof. Dr. Ingo Weber | Chair for Software and Business Engineering

ingo.weber@tu-berlin.de | Twitter: @ingomweber