A High-Performance Solution for Data Security and Traceability in Civil Production and Value Networks through Blockchain

Erik Neumann[1], Kilian Armin Nölscher[2], Gordon Lemme[2], Adrian Singer[2]

[1] Faculty Applied Computer Sciences and Biosciences University of Applied Sciences Mittweida
[2] Department Digitalization in Production Fraunhofer IWU

Contact email: **neumann3@hs-mittweida.de**

safeURchain

IARIA

Presenter

Erik Neumann

- Works as a blockchain developer in the project “safe-UR-chain” at the Blockchain Competence Center Mittweida
- Is studying in the Blockchain & Distributed Ledger Technologies (DLT) program toward a M. Sc. at the University of Applied Sciences Mittweida
- Research interests: consensus algorithms, distributed computing, blockchain

Introduction

- Cybercrime is becoming more frequent [1]
- Value chains are increasingly interconnected and production data is stored digitally
- Cyberattacks on value chains pose a threat to the civil infrastructure
- The project “safe-UR-chain” [2] explores a blockchain-based solution to combat data manipulation

Introduction

Motivation

- Confidentiality, integrity, and availability are basic protection objectives for digital communication
- Current solutions allow for confidentiality (e.g., by encryption) and availability (e.g., through cloud solutions), but not usually for integrity (i.e., ensuring that stored data is correct)
- Blockchain networks can provide this missing property by storing data in a distributed linked list
- If the stored data also is signed, it can be irrefutably linked to a source

Introduction

Motivation

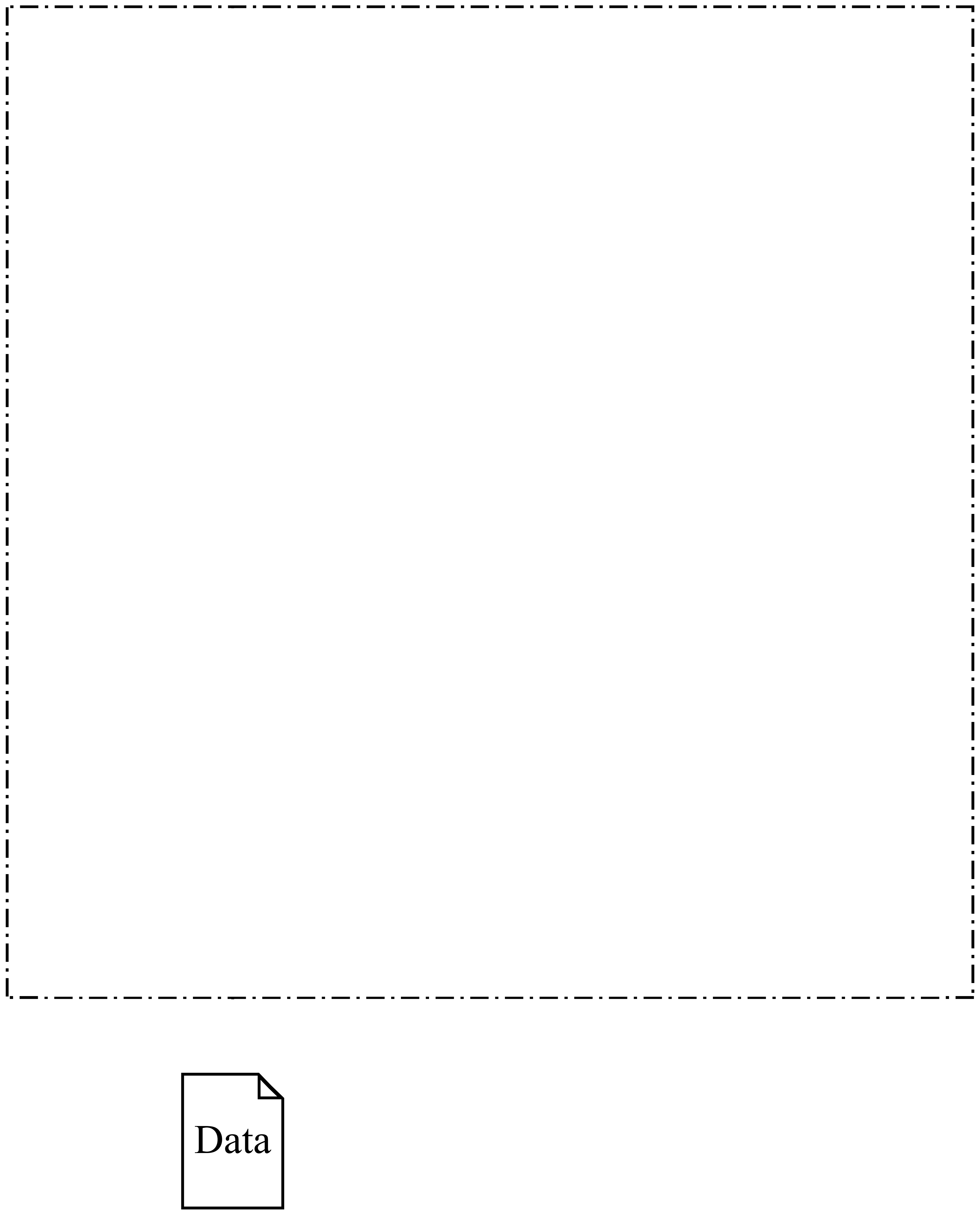
- Public blockchain networks provide a high level of security, but low bandwidth
- Private blockchain networks can provide higher bandwidth, but due to the lower number of participants, a relatively lower level of security
- “safe-UR-chain” aims to provide a traceable and tamper-proof data storage for companies in a value chain by entangling private blockchain networks

Architectural Overview

- To add records into the system, data is
  1. Collected
  2. Distributed
  3. Included into the blockchain
  4. “Countersiged” by the other networks
- This process is distributed over multiple layers within the system

Architectural Overview
Nodes

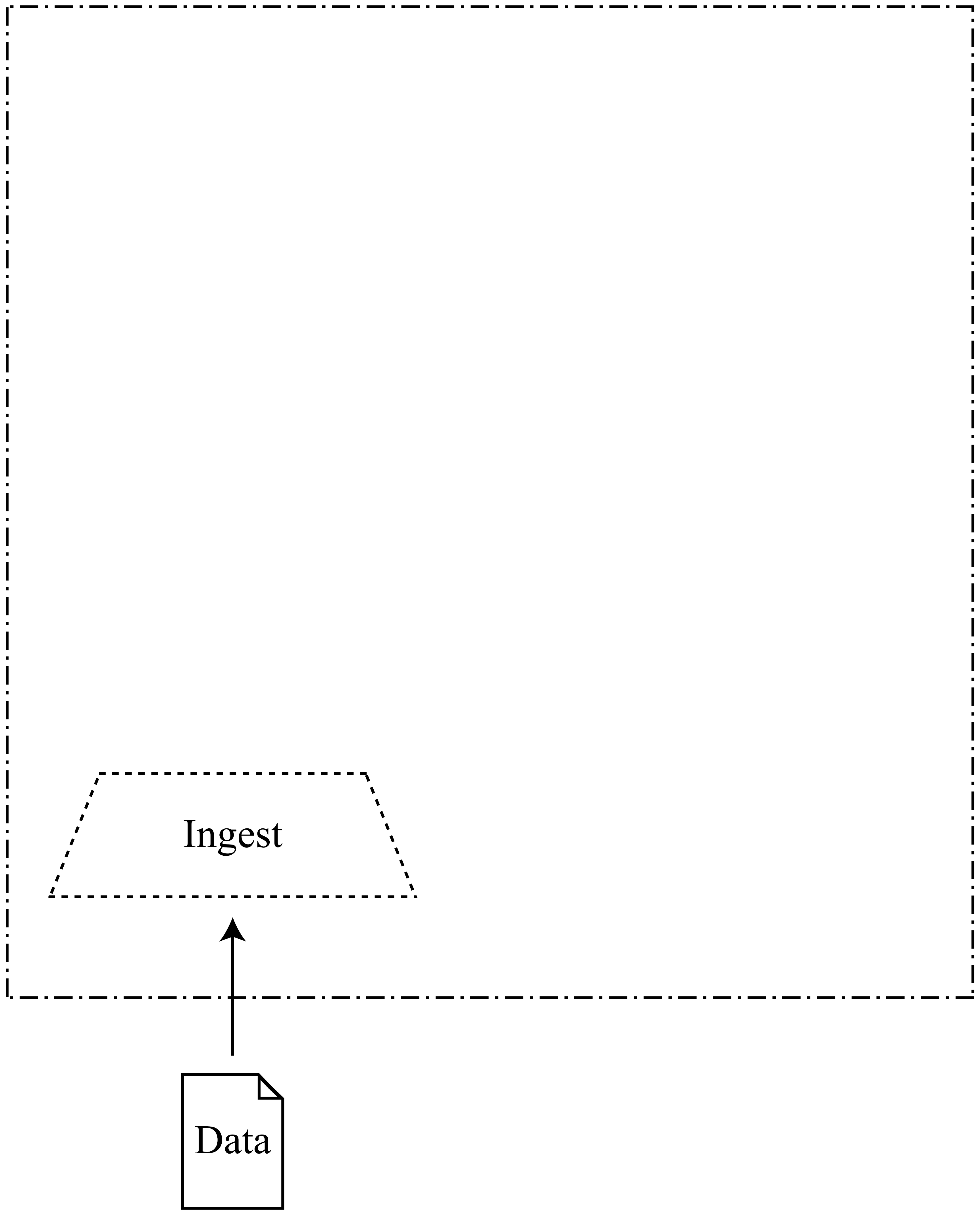
- Nodes form the backbone of local blockchain networks
- They consist of multiple modules



Architectual Overview

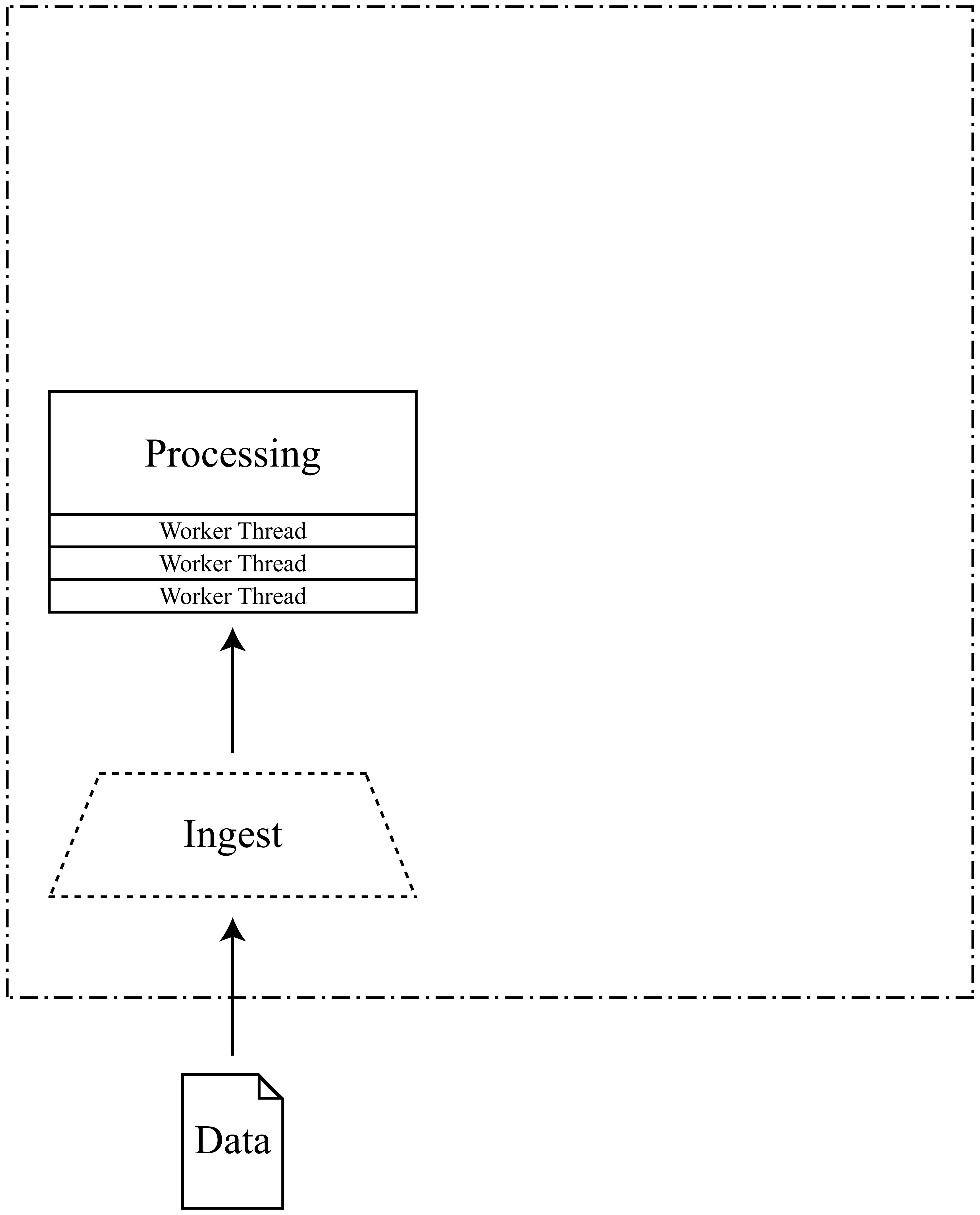
Nodes

- **Ingest** module
  - Provides a generic interface for feeding data into the system
  - Can consume data from files, the network, serial communication, etc.
  - Ingested data is signed and broadcast as "transactions"



Architectural Overview
Nodes

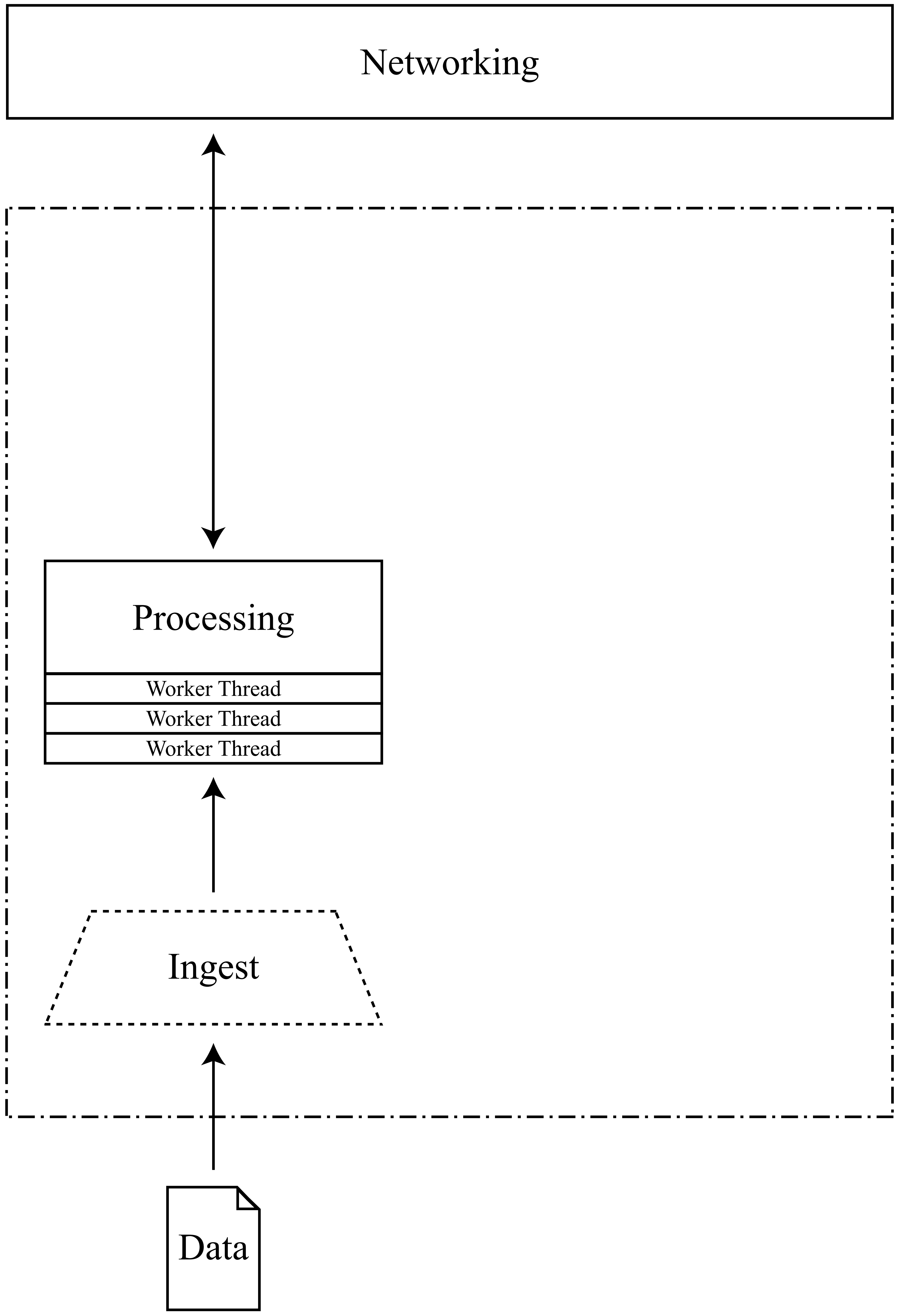
- **Processing** module
  - Processes internal tasks via a configurable amount of worker-threads
  - Passes data between the other modules
  - Queues outgoing network messages
  - Processes incoming network messages



Architectural Overview

Nodes

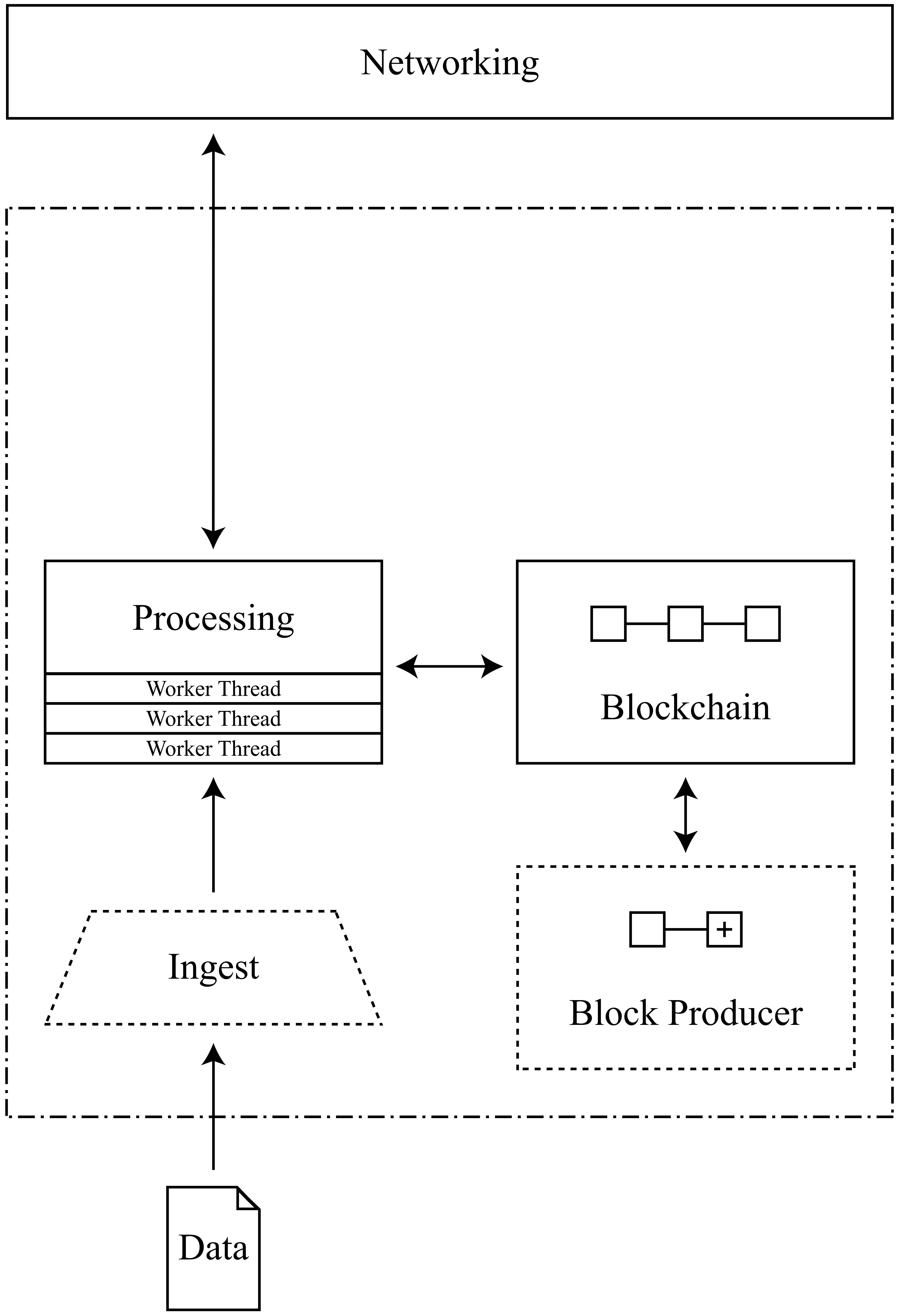
- **Networking** module
  - Maintains a list of other nodes on the network
  - Sends and receives network messages



Architectual Overview

Nodes

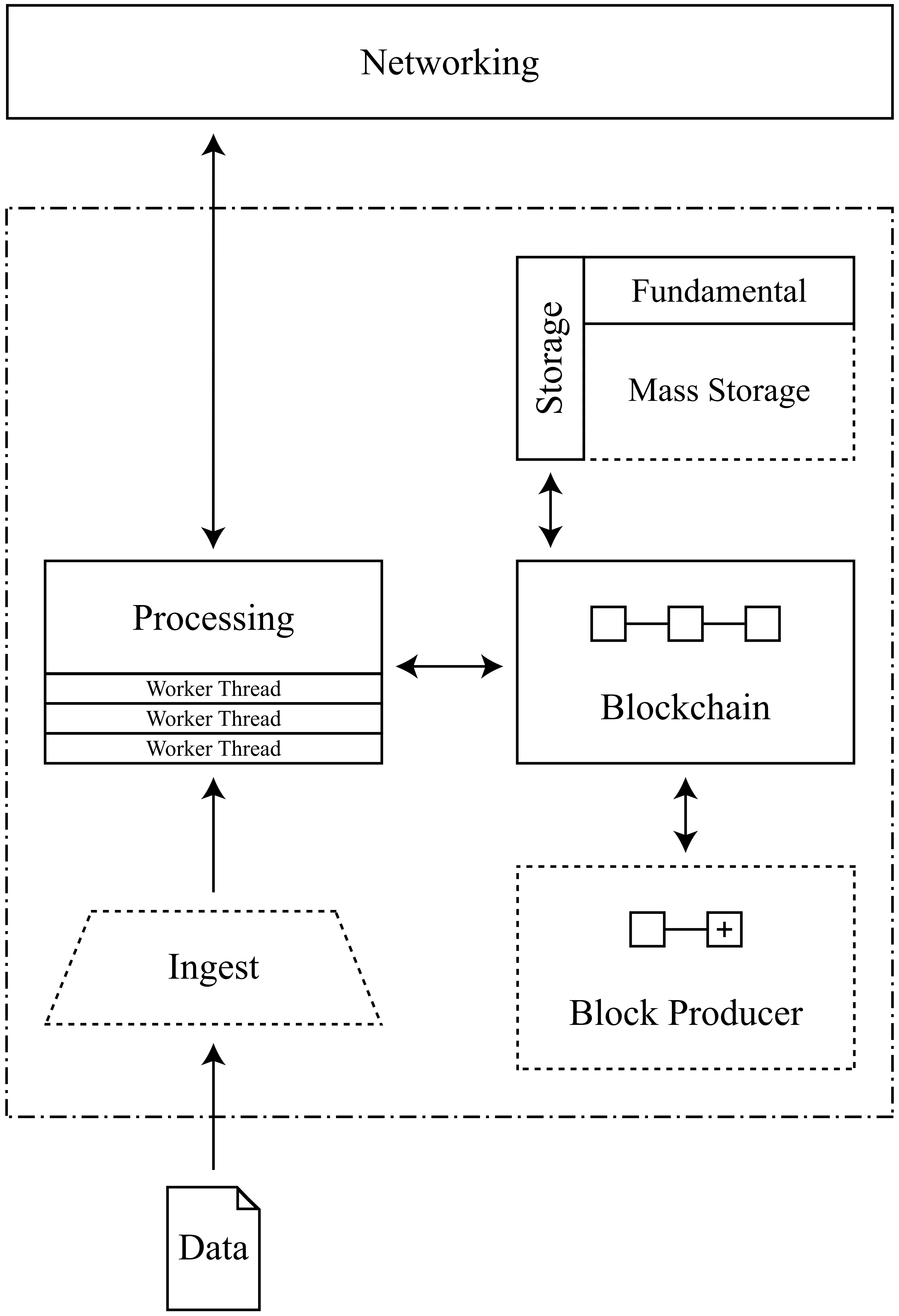
- **Blockchain & Block Producer** modules
  - Transactions are bundled into blocks
  - Blocks are created according to the rules of a consensus mechanism
  - New Blocks are appended to the blockchain



Architectural Overview

Nodes

- **Storage** module
  - Blocks can be stored with all associated data or partial data
  - This is done to save disk space
  - The stored data is determined by a configurable filter



Architectural Overview

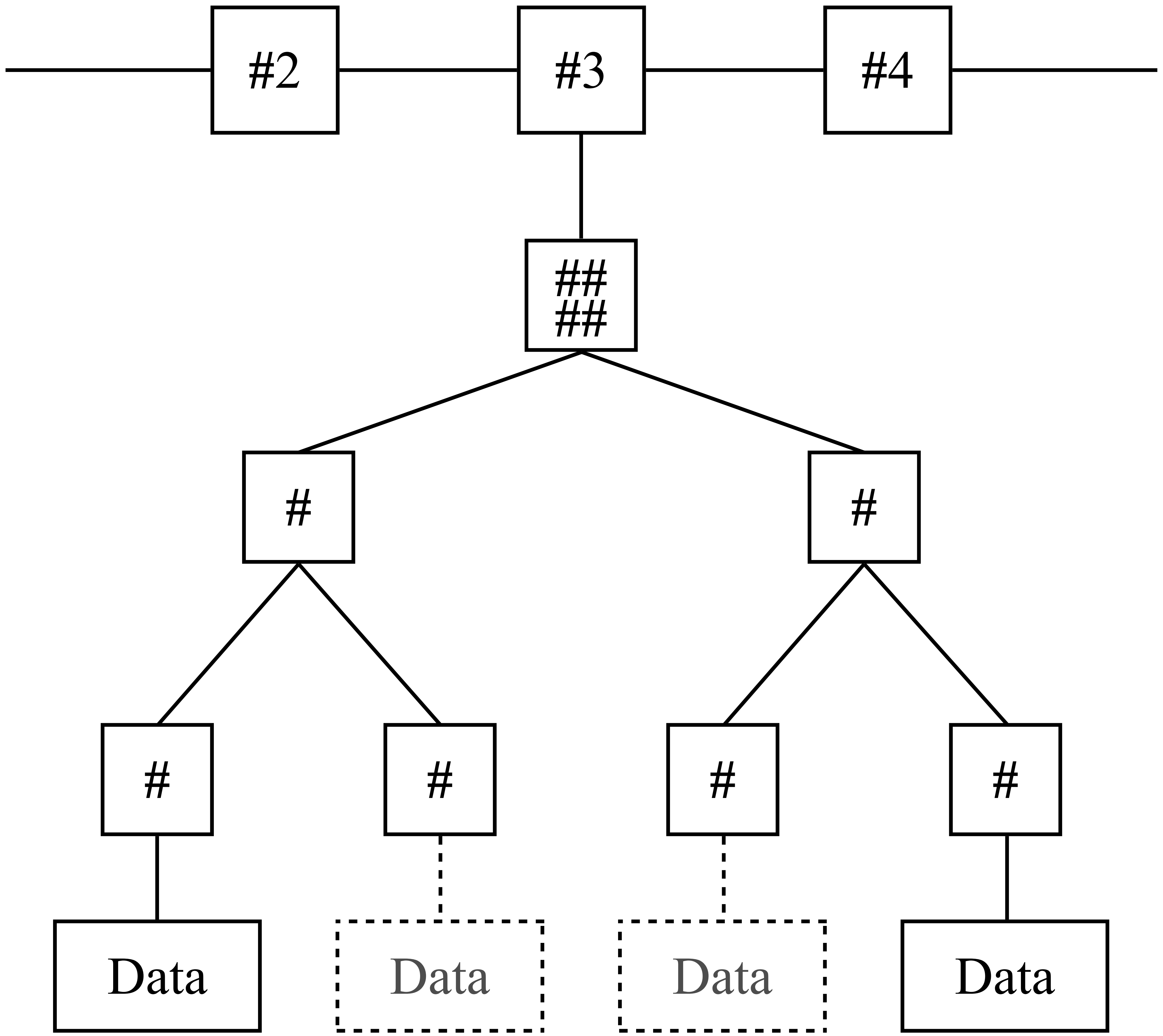
Nodes

- By selectively disabling some modules, different node types can be created
- These types differ in their hardware requirements
- The **Block Producer** module can be disabled to reduce CPU requirements
- The **Storage** module can be configured to store only essential data and therefore reduce disk space requirements
- By configuring nodes in this way, companies can tailor their local blockchain networks to their needs/resources

Architectural Overview

Blockchain

- Data is stored in a block via a Merkle Tree [8]
- The root-hash of this tree is stored within the block header
- Hash values are used as proxies for data
- Data can be left out without changing the root-hash
- Blocks with partial partial retain their hash

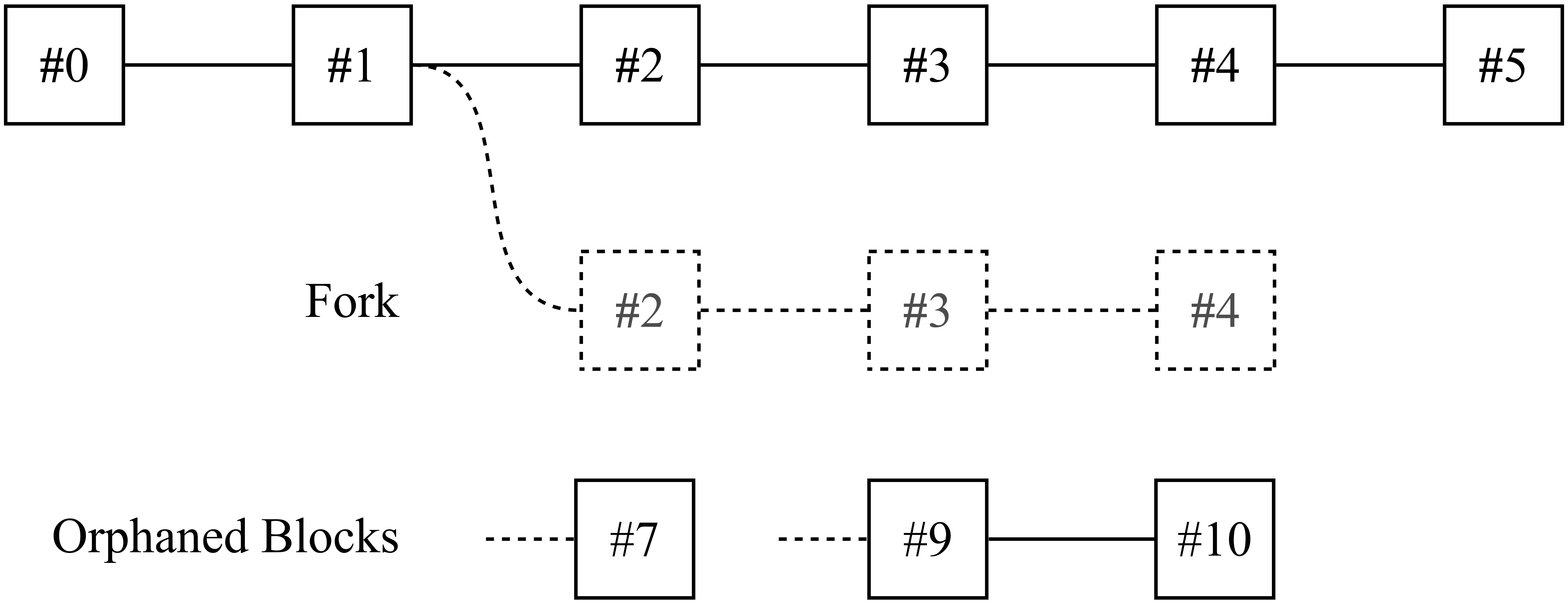


Architectural Overview
Blockchain

- Blocks are stored in a tree like data structure
- This structure uses the rules of the consensus protocol to determine the canonical chain
- If blocks arrive before their predecessor (orphaned blocks), they are stored until they can be appended

Architectural Overview

Blockchain



Architectural Overview
Local Network

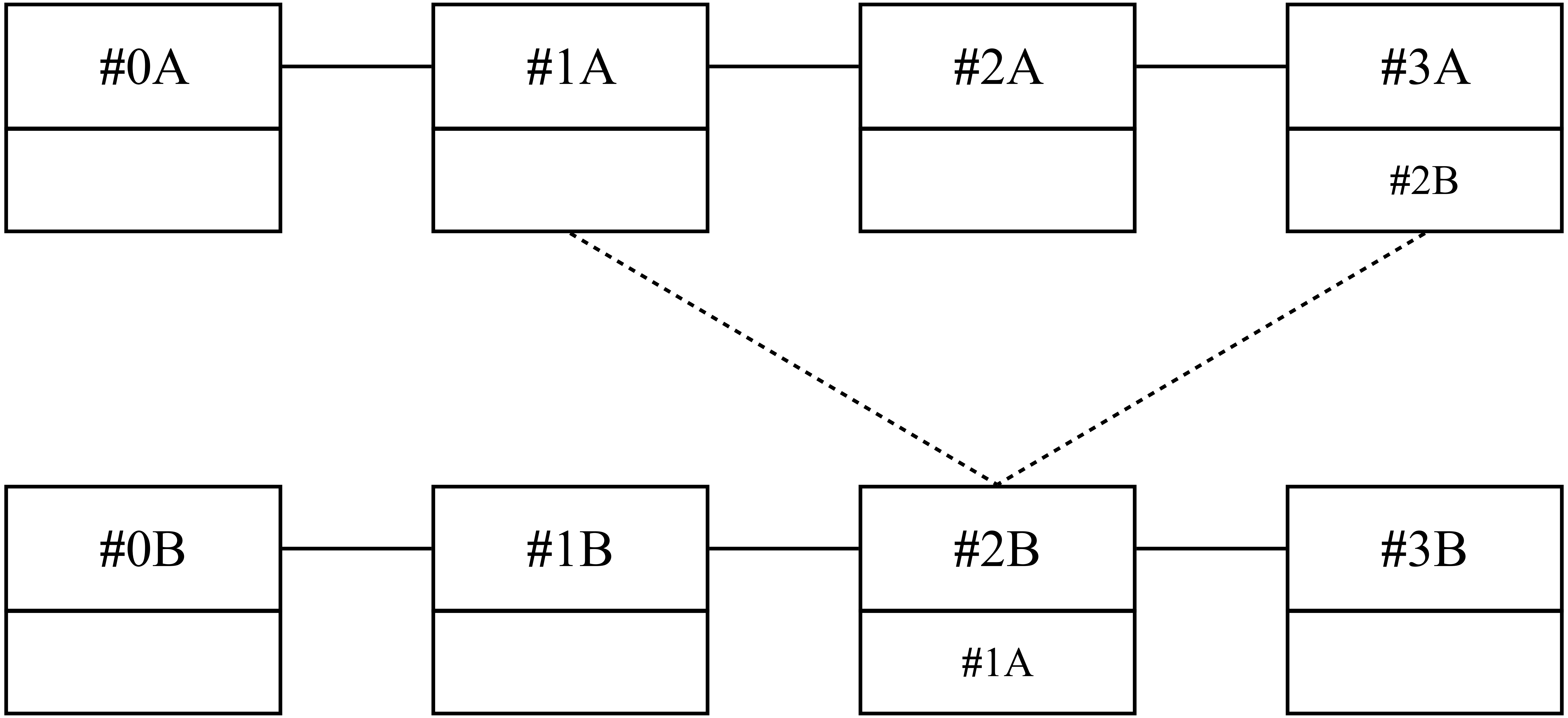
- Blockchain Nodes communicate via a peer-to-peer network
- This network automatically bootstraps by using known nodes that have a high availability within the network
- The network has self-repairing capabilities
- A flooding protocol [7] ensures message delivery without the need for complicated routing

Architectural Overview
Global Network

- Local networks exchange block-hashes via an HTTPs message broker
- The hashes are included in the blockchains of the other networks
- This eliminates the possibility of retroactive changes to a participant's blockchain
- Messages sent via the broker are network-to-network encrypted

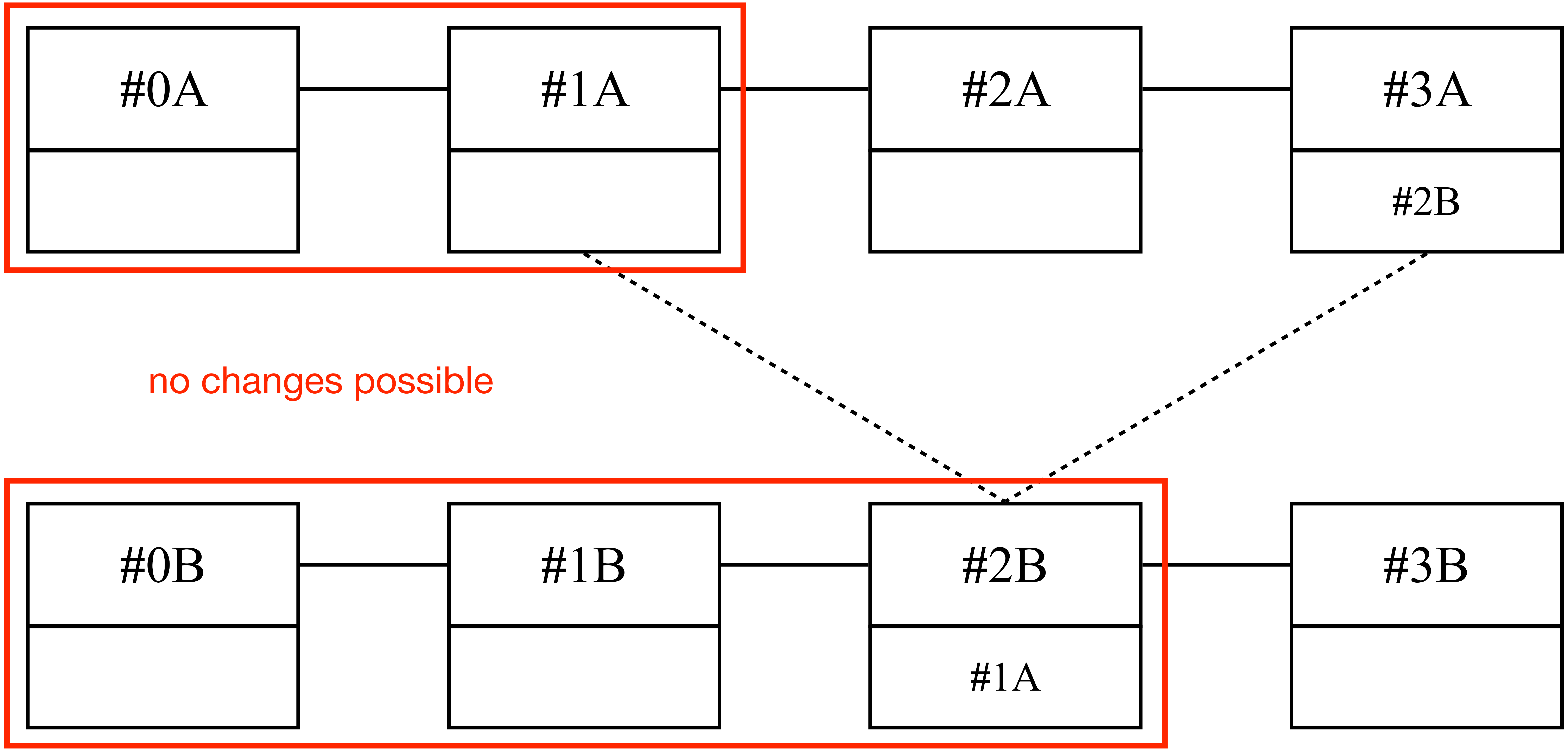
Architectural Overview

Global Network



Architectural Overview

Global Network



Example Scenario

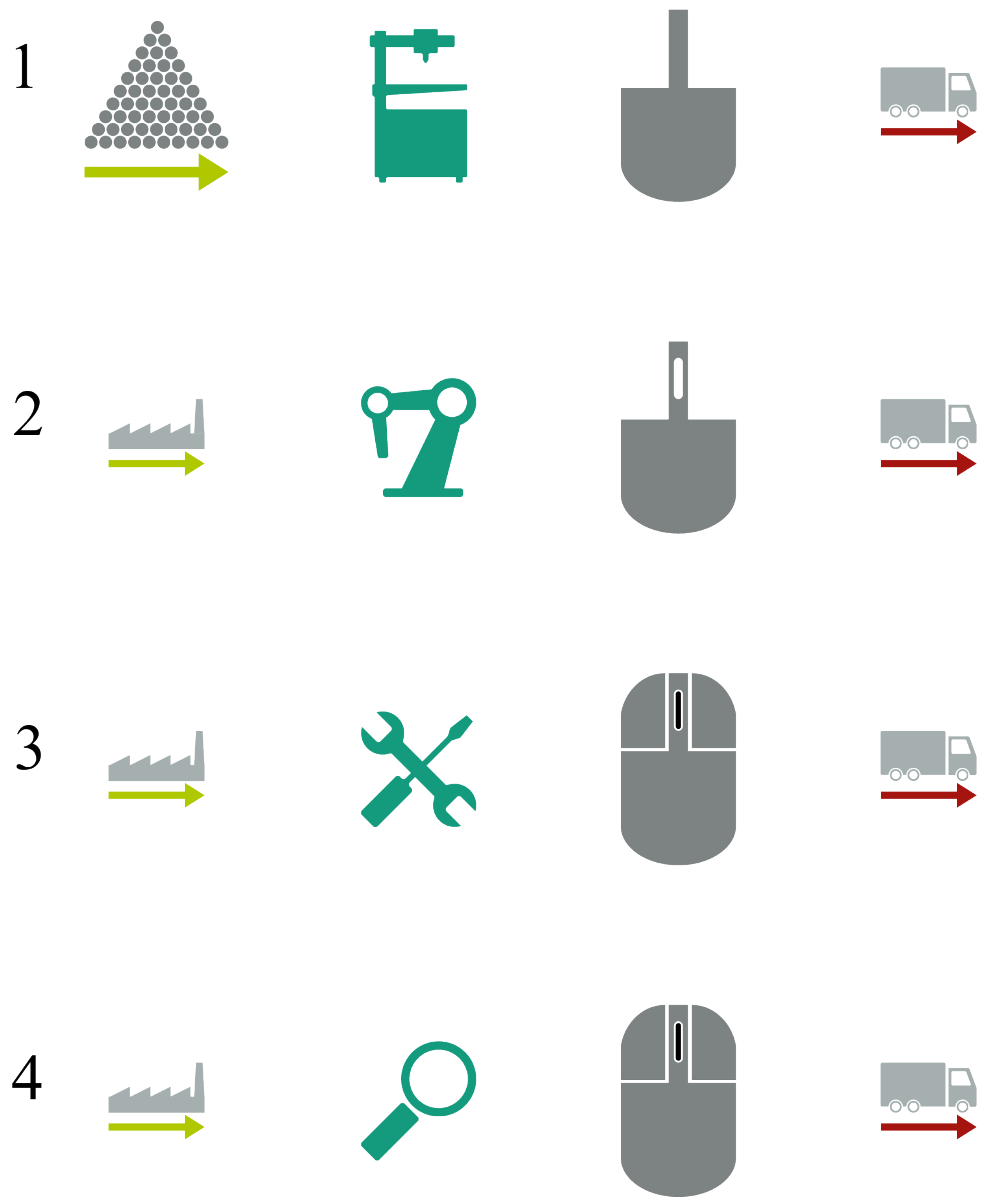
- A four-step example scenario was set up to simulate real-world data flows

  1. Raw material is turned into a semi-finished product

  2. The product is further processed

  3. The product is assembled using supplier components

  4. The product goes through quality control



Example Scenario

- All steps are associated with an identifier-code that is applied to the product
- The real-world version of the scenario was modeled using 3D-printed parts with an Automated Guided Vehicle (AGV) for transport between steps
- The blockchain network for the scenario used a main node with 32 GB of RAM and multiple nodes for data ingestion with 8 GB of RAM
- All nodes were equipped with SSD storage and used Ubuntu 20.4 LTS as their operating system
- Data was collected via OPC UA [9]

Evaluation
Proceeding

- Main questions:
  - Do packets get lost, especially during high transaction loads?
  - What is the effect of varying the payload of a transaction?
  - How big is the latency between transaction and block creation?

Evaluation

Proceeding

- The experiment was conducted with a block time of 15 seconds and ran for 44 blocks (11 minutes)
- Several test runs with different transaction sizes were carried out
- The data generated by the machines was also stored locally to facilitate the detection of possible packet losses
- The blockchain was reset between test runs

Evaluation

Results

- Up to 100 transactions per second could be processed
- No packet loss could be observed
- The payload size did not affect the throughput
- The transaction latency was at least 15 seconds (one block)
- When few transactions with large payloads were generated, they were included within one block
- When many transactions with small payloads were generated, they were included within two blocks

Conclusion

- Blockchain technology has significant potential in industries relying on sensitive data processing (e.g., aerospace, medical, and automotive)
- With this technology, faulty or manipulated product data can be detected
- The described system provides a flexible, high-throughput blockchain solution for tamper-proof and transparent data storage
- The system combines the high performance of a private blockchain with the high trustworthiness of a public one

Future Work

- A procedure to authenticate domain-specific data across locations and to distribute it in a tamper-proof manner
- A system extension for the exchange of data in horizontal value chains
- A detailed investigation of possible attack vectors on the system

Acknowledgement

The project is funded by the German Federal Ministry of Education and Research within the framework of the announcement “Civil Security - Critical Structures and Processes in Production and Logistics” under the funding codes 13N15150 to 13N15153.

References

- [1] R. Klatt, “Danger from cyber attacks has increased sharply in Germany.” [Online]. Available from: https://www.forschung-undwissen.de/nachrichten/oekonomie/gefahr-durch-cyberangriffe-hat- indeutschland-stark-zugenommen-13375090, June 2021.
- [2] Fraunhofer IWU, “safe-UR-chain Webpage.” [Online]. Available from: https://safe-ur-chain.de, August 2021.
- [3] G.Lemme,D.Lemme,K.A.No¨lscher,andS.Ihlenfeldt,“Towardssafe service ecosystems for production for value networks and manufacturing monitoring,” in Journal of Machine Engineering, Vol. 20 No. 1, March 2020, pp. 4–5.
- [4] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.” [On- line]. Available from: https://bitcoin.org/bitcoin.pdf August 2021.
- [5] “An Introduction to Hyperledger.” [Online]. Available from: https://www.hyperledger.org/wp-content/uploads/2018/07/HL Whitepap er IntroductiontoHyperledger.pdf August 2021.
- [6] G.Lemme,K.A.No¨lscher,E.Bei,C.Hermeling,andS.Ihlenfeldt,“Se- cure data storage and service automation for cyber physical production systems through distributed ledger technologies,” in Journal of Machine Engineering, Vol. 21 No. 1, March 2021, p. 4.
- [7] A. S. Tanenbaum and D. J. Wetherall, “Computer Networks (5th ed.),” Pearson Education, 2010, p. 368.
- [8] R.Merkle,“ProtocolsforPublicKeyCryptosystems,”IEEESymposium on Security and Privacy, 1980, pp. 125–127.
- [9] OPC Foundation, “OPC 10000-1: OPC Unified Architecture - Part 1: Overview and Concepts.” [Online]. Available from: https://opcfoundation.org/about/opc-technologies/opc-ua/, July 2021.