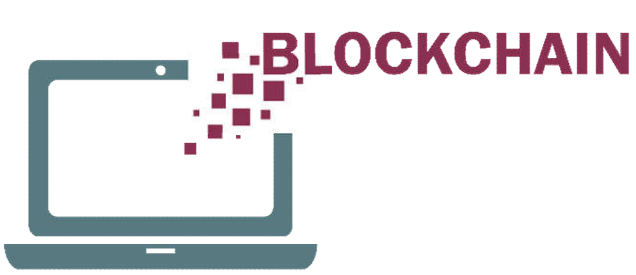
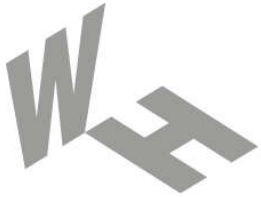




Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

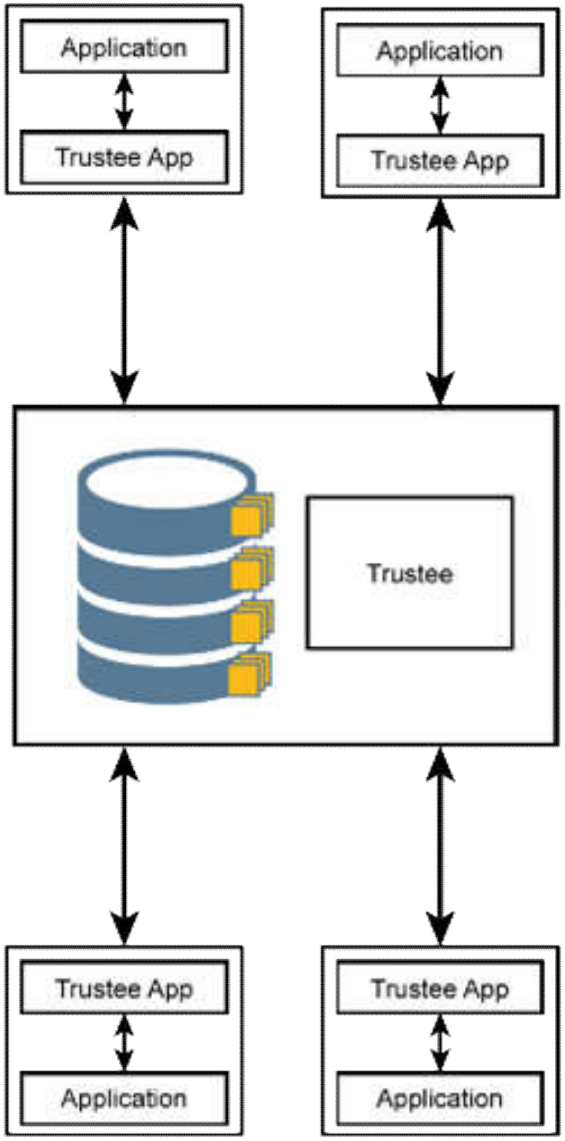
Blockchain Security

Prof. Dr. (TU NN)
Norbert Pohlmann

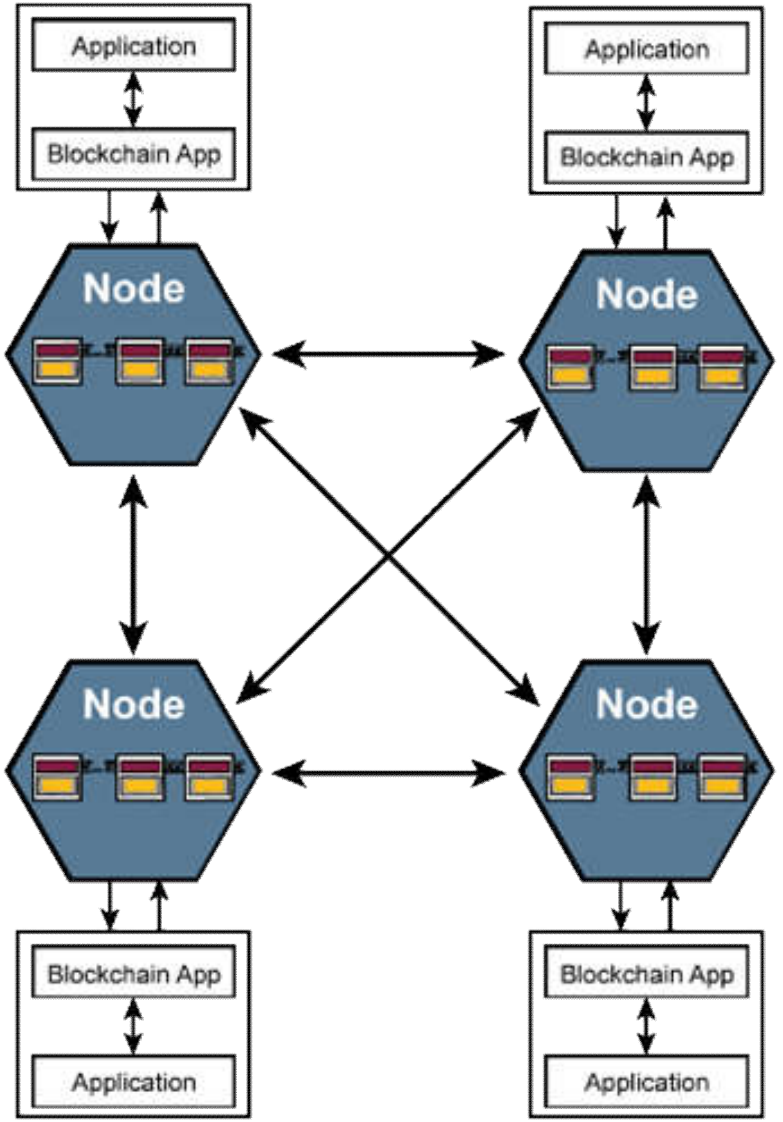
Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

BlockChain-Technology
→ in a nutshell



Centralized Architecture



Decentralized Architecture

BlockChain Concept
→ Different perspectives

- For a **computer scientist**, the **BlockChain** is a simple data structure, the data chained as "blocks" and redundantly managed in a distributed network by nodes.

  The alternative could be a conventional database, which is continuously replicated by all participants.

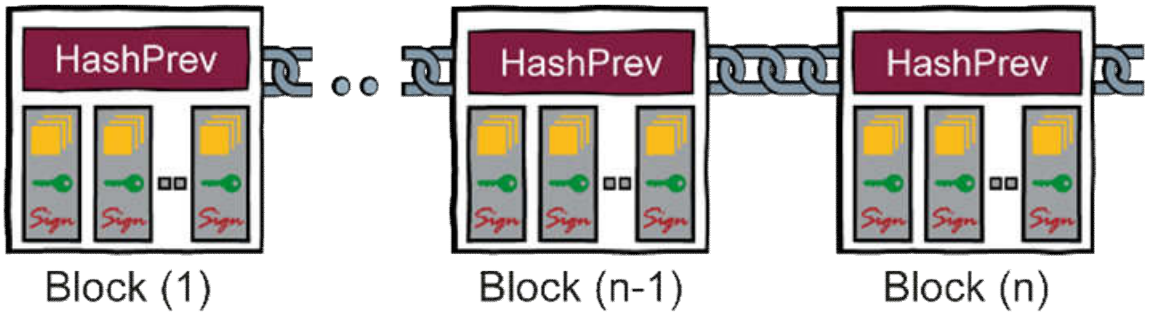
- For the **IT security experts**, the **BlockChain** has the advantage that the **data** can be stored in individual "blocks" **tamper-proof**, which means that the participants in the **BlockChain** will be able to check
  → the authenticity,
  → the origin and
  → the integrity of the stored data.

  The alternative could be a PKI system.

- For the **application designer**, using **BlockChain** technology means **trusted and automated collaboration between different organizations**.

  The alternative could be a costly trustee.

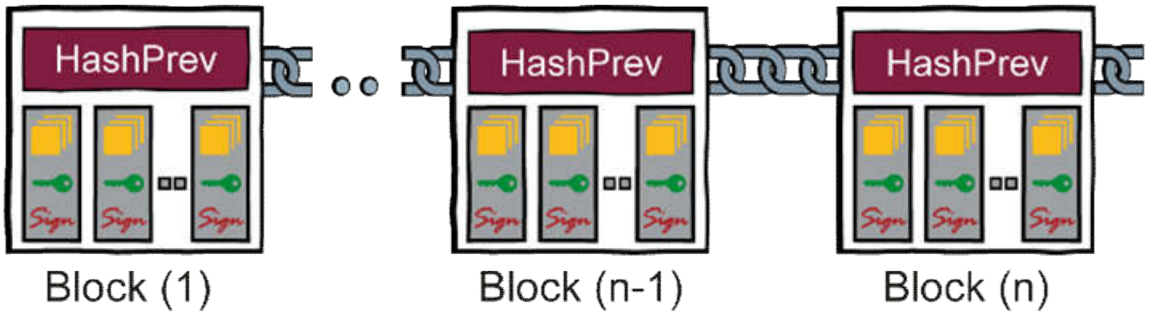
BlockChain-Technology
→ als ein Collaboration-Tool



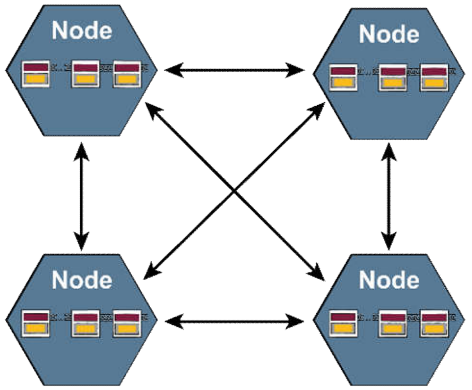
BlockChain

- is a **tamper-proof**,
- **distributed**, **redundant** **data structure**
- in which transactions are **logged in chronological order**
- **traceable**, **unmodifiable** and
- **offers trust** **without a central entity**.

BlockChain-Technology
→ Data structure of the Blockchain



- **The data can be coins, certificates, sensor data, source code, ... or more generally: any kind of digital assets**
- **Transactions with the data are created and signed by the BlockChain participants. The matching public key is also stored in the transactions**
- *A* **block** *combines several transactions that are hashed together. The hash value* **HashPrev** *ensures block chaining*
- The **BlockChain** contains all blocks (**data**). On each node of the corresponding peer-to-peer network, a version of the **BlockChain** is stored



BlockChain-Technology
→ Property: tamper-proof/unmodifiable

- **Transactions are signed** with the help of the digital signature by the **BlockChain** participants
- Transactions are **hashed together** in a block and the hash value **HashPrev ensures block chaining** for the **BlockChain**
- **For this property we need a crypto agility**
  - We have to use always “State of the Art” crypto (Technical Guideline: "Cryptographic Methods: Recommendations and Key Lengths")
    - Public-key method (*RSA - 3.000 bit*)
    - Hash functions (*SHA-3 - 256 bit*)
  - **Quantum Computing Risk** → Post-Quantum Crypto method
  - Important question: Lifetime of the **BlockChain** / cryptography
    - Switching cryptographic methods (for example every 10 years organizing a hard fork)

BlockChain-Technology
→ Property: distributed/redundant

- On each node of the corresponding peer-to-peer network, a version of the **BlockChain** is stored

- **For this property we need a robust peer-to-peer network**

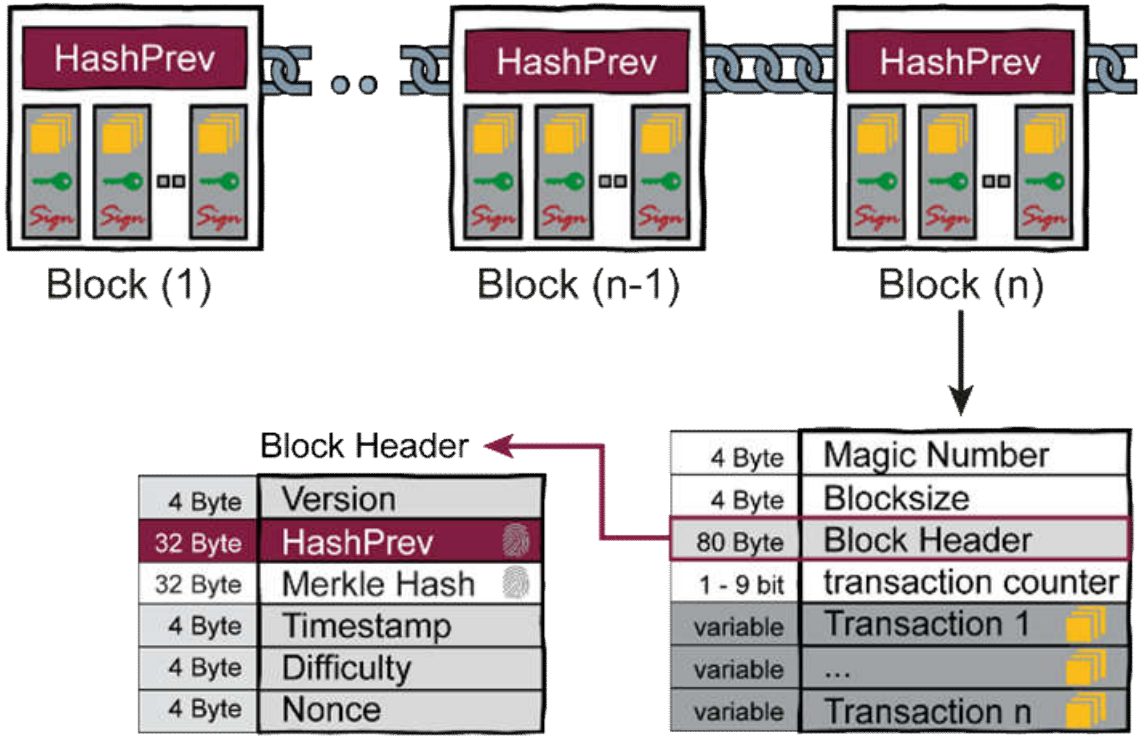
  - ***Scalability / resource requirements***
    - Bandwidth between the nodes
    - Storage capacity on the node (bitcoin **BlockChain** has a size of more than 160 G byte)
    - Computer (CPU, RAM, …) capacity of a node
    - ...

  - ***Reliability / Availability***
    - Necessary number of nodes
    - Robust distribution function for transactions and new blocks
    - Robust against DDoS attacks
    - ...

BlockChain-Technology
→ Property: logged in chronological order

- With the help of the hash value **HashPrev** **block chaining** is ensures

- **For this property we need additionally**
  - A clever use of the hash functions (transactions, block chaining)
  - distributed trust services

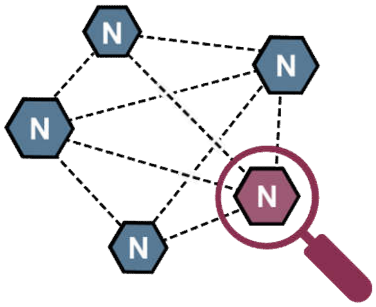


$$HashPrev_n = H (Block\text{-}Header_{n-1})$$

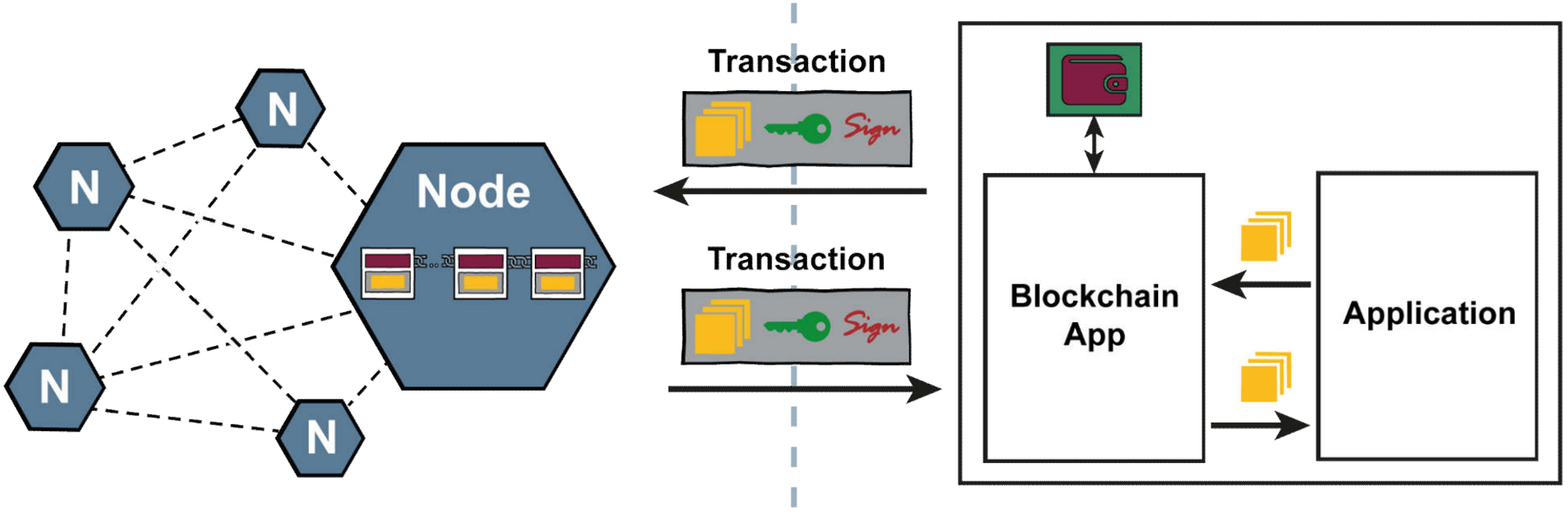
BlockChain-Technology
→ Property: trused without a central entity

- The **BlockChain** technology provides "programmed trust" with the various IT security and trust mechanisms.
- All IT security and trust features are inherently integrated as **security-by-design** in the **BlockChain** technology.

- **For this property we need distributed trust services**
  - The right design for a suitable **BlockChain** architecture with appropriate “Distributed Consensus” and distributed validation mechanisms
    - Distributed Consensus: Proof-of-Work, Proof-of-Stake, …
    - (Distributed) Validation: Hash, signature, syntax, semantic, …
    - **BlockChain** architecture: public, private, … permissionless, permissioned, …



BlockChain-Technology
→ Infrastructure and Application

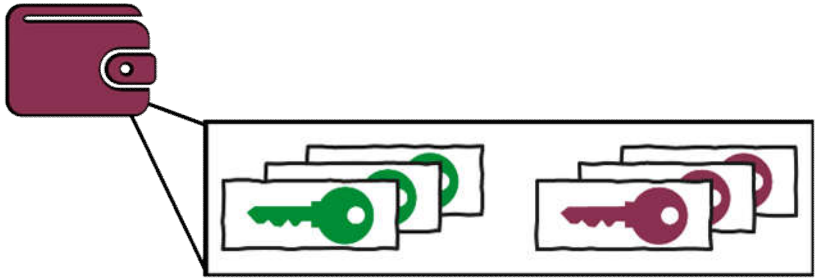


BlockChain Infrastructure **BlockChain Application**

- The **BlockChain Infrastructure** (peer-to-peer network, Nodes with all communication, security and trust functions, the data structure **BlockChain**, ...)
- The **BlockChain Application** (Blockchain App, wallet / keys / security module, Application, ...)
- The **transactions** as an interface in between infrastructure and application

BlockChain-Application
→ Security of the keys

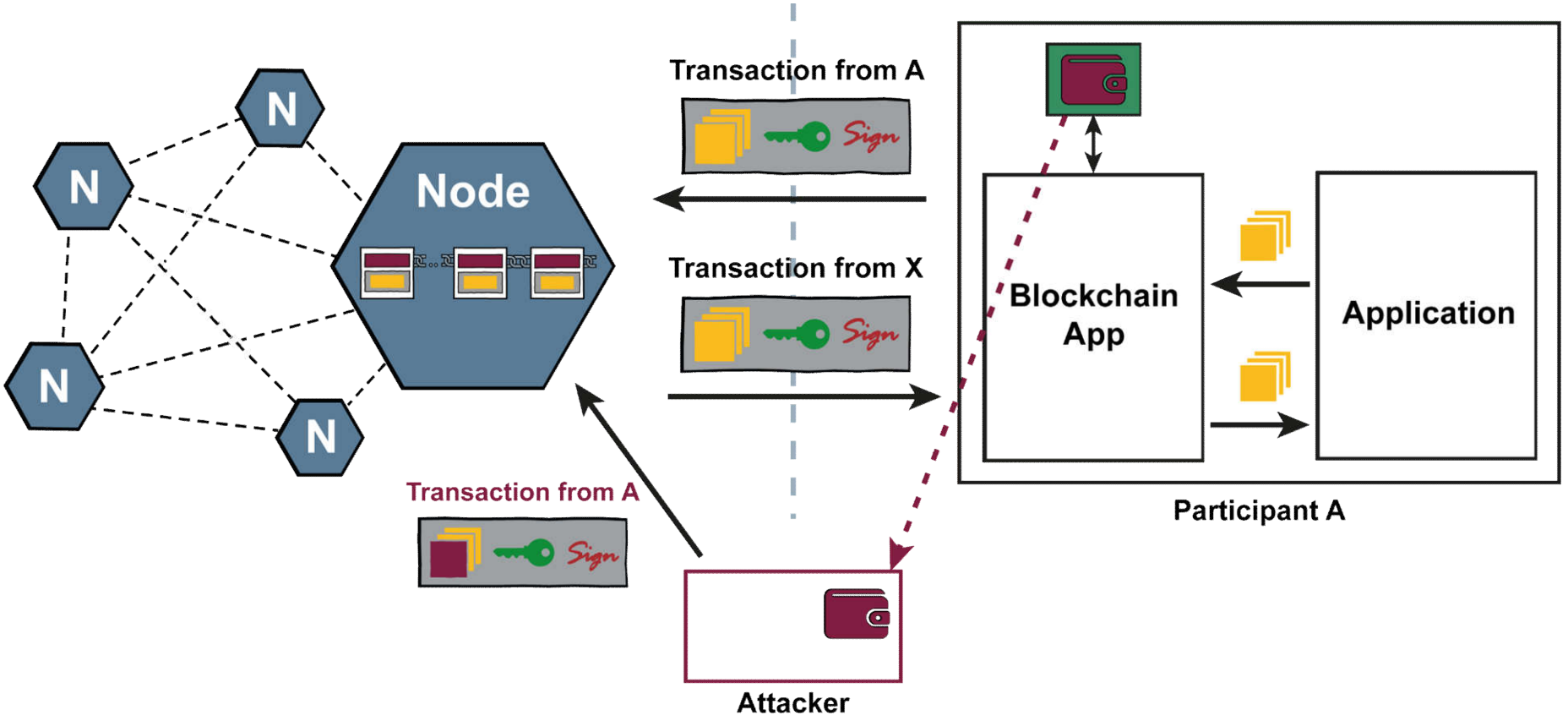
- The security of the **BlockChain** technology also depends **on the secrecy of the private keys** of the public-key method (Wallet).



- **Dangers** of inadequate protection of the private key
  - The private computer / IoT device is hacked (malware)
  - The website of the Online Wallet (Service Node) is hacked
  - An insufficiently secured smartphone is stolen (Light Node)
  - The **private key is stolen** or is **used without authorization**

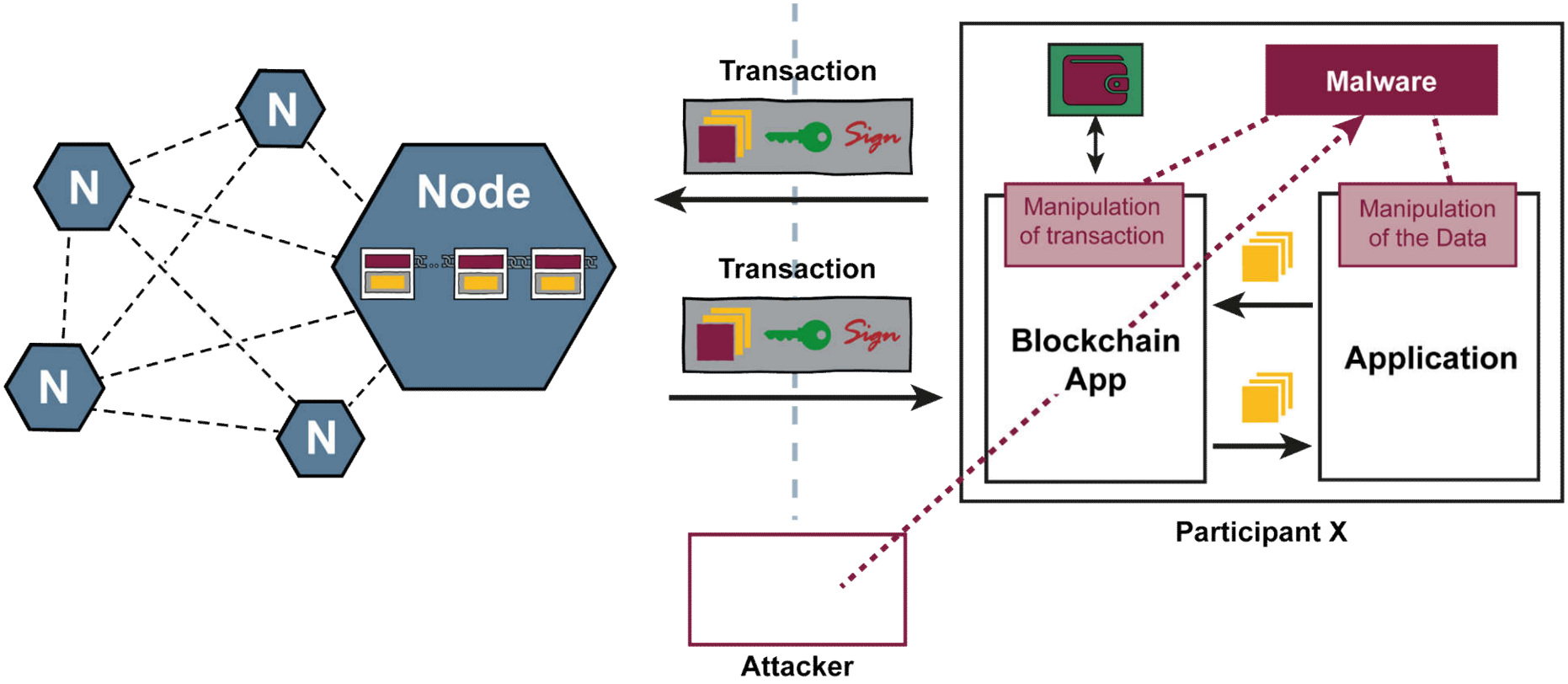
- The protection of the private key should be realized with the help of **hardware security modules** (smart cards, security tokens, high-level security modules) - and unauthorized use must be actively prevented!

BlockChain-Application
→ Manipulation of transaction



- The attacker **"owns"** the wallet/key or can **"use it without authorization"**
  - This allows the attacker to create valid transactions for the corresponding participant A and manipulate the **BlockChain** application

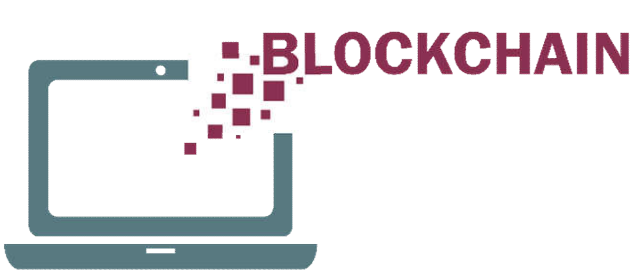
BlockChain-Application
→ Manipulation of the data

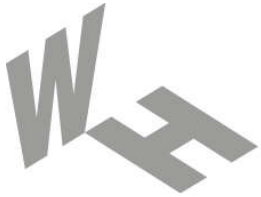


- The attacker "runs" **malware** on the participant's IT system
  - This allows the attacker to manipulate the data of the **BlockChain** application
  - Both, outgoing and incoming transactions
  - The transactions are securely stored in the **BlockChain**

Blockchain Security
→ Summary

- **We need a robust peer-to-peer network**
  - Adequate resources, robust distribution function, …
- **We need a crypto agility**
  - Only use of “State of the Art” crypto, concept for switching crypto, …
- **We need distributed trust services**
  - Appropriate **BlockChain** architecture, distributed consensus, distributed validation mechanisms, …
- **We must protect the Wallet against theft and unauthorized use**
  - hardware security modules, unauthorized use prevention, …
- **We need to protect the BlockChain applications for malware attack**
  - Trusted Computing, Sandboxing, …





Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Blockchain Security

With secure BlockChain into the future!

Prof. Dr. (TU NN)
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.