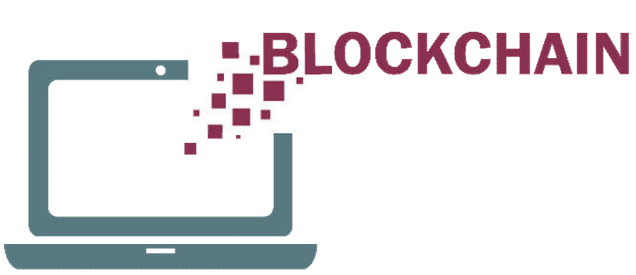
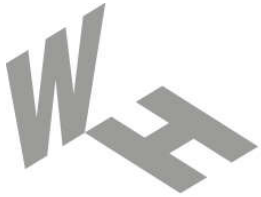




Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Trusted BlockChain Interfaces

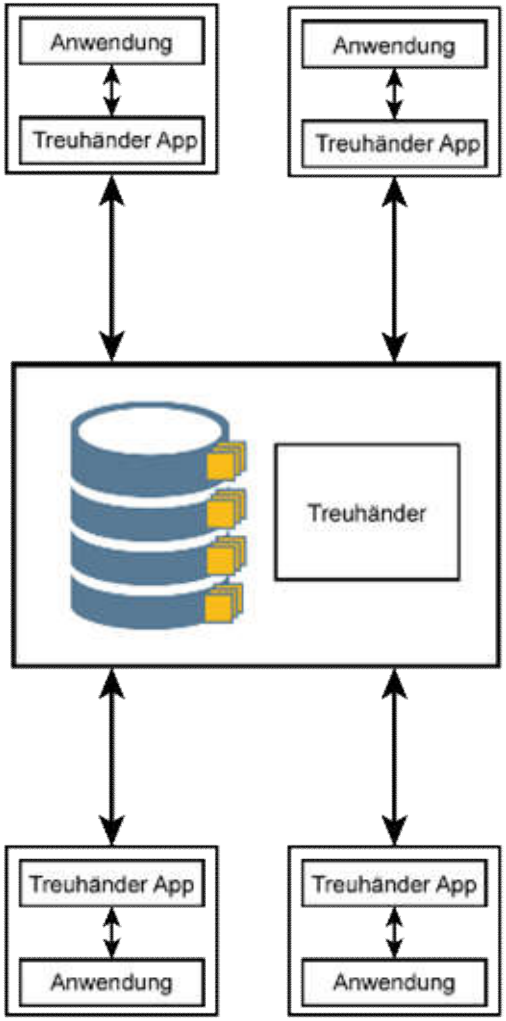
Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

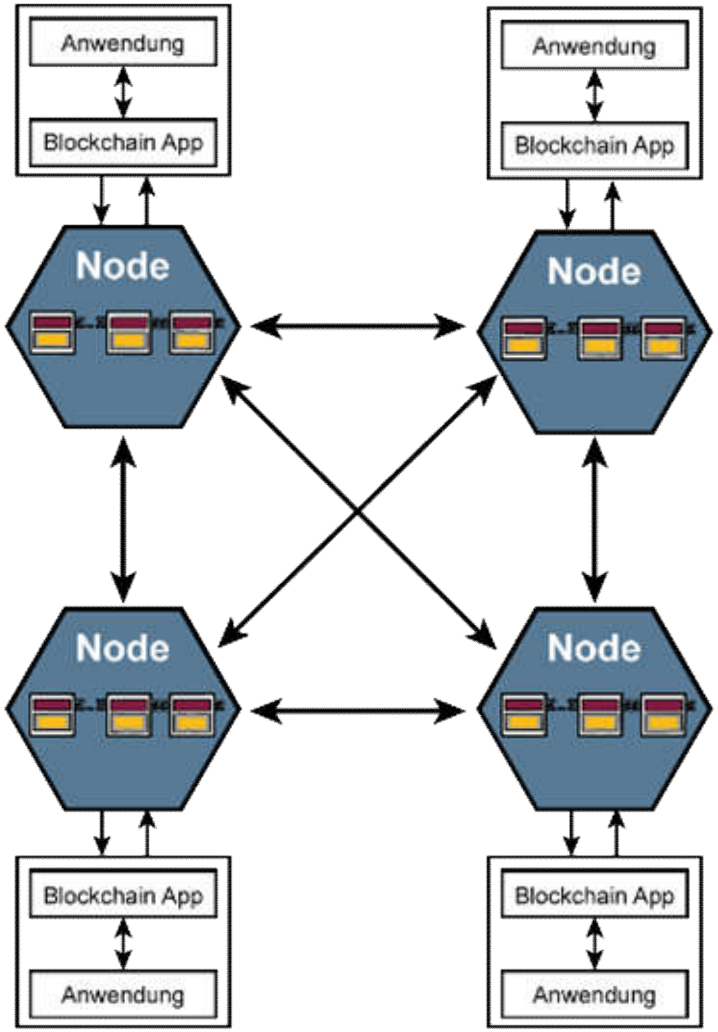
if(is)
internet-sicherheit.

BlockChain-Technologie
→ auf den Punkt gebracht

Transaktionsspeicher

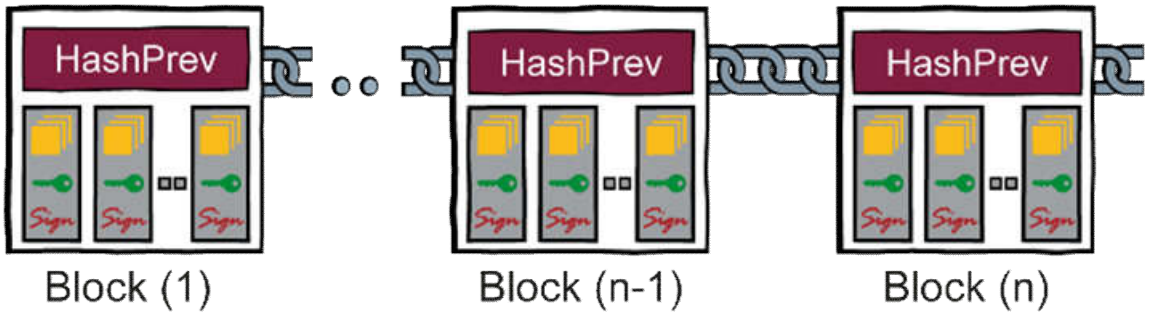


Zentrale Architektur



Dezentrale Architektur

BlockChain-Technology
→ Sicherheitseigenschaften

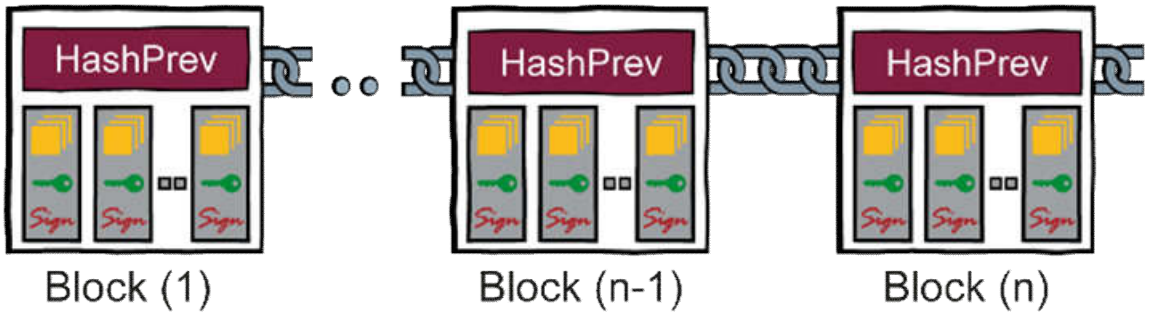


BlockChain

- ist eine **fälschungssichere**,
- **verteilte**, **redundante** Datenstruktur
- in der **Transaktionen** **in der Zeitfolge protokolliert**
- **nachvollziehbar**, **unveränderlich** und
- **ohne zentrale Instanz** abgebildet sind.

*(**Sicherheitseigenschaften** einer **BlockChain**)*

BlockChain-Technology
→ Datenstruktur einer BlockChain

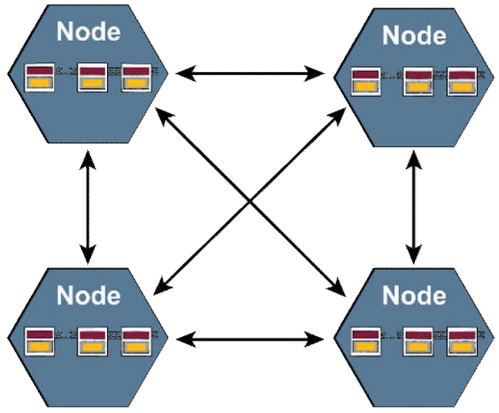


- Die **Daten** sind Transaktionsdaten mit Geldeinheiten, Zertifikaten, Produktionsdaten, Sensordaten, Source Code, ... digitale Werte

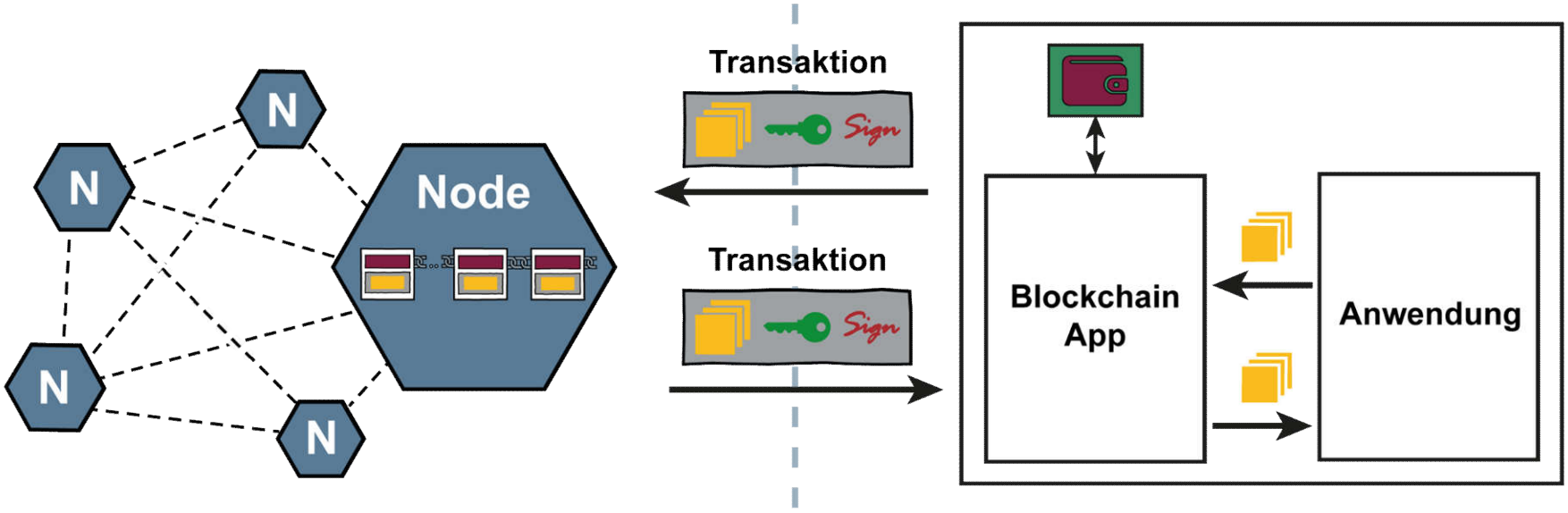
- **Transaktionen** mit **Daten** werden vom Teilnehmer erstellt und **sign**iert (Wallet/Schlüssel). Passende **Public Key** in der Transaktion. Verteilung

- **Block** *beinhaltet verknüpfte Transaktionen. Der Hashwert* **HashPrev** *sichert die Blockverkettung. Verteilte Validierung, Konsens.*

- Die **BlockChain** beinhaltet alle Blöcke (**Daten**). Auf jeder Node eines bestimmten Peer-to-Peer Netzwerkes ist eine Version der **BlockChain** gespeichert



BlockChain-Technologie
→ Infrastruktur und Anwendung

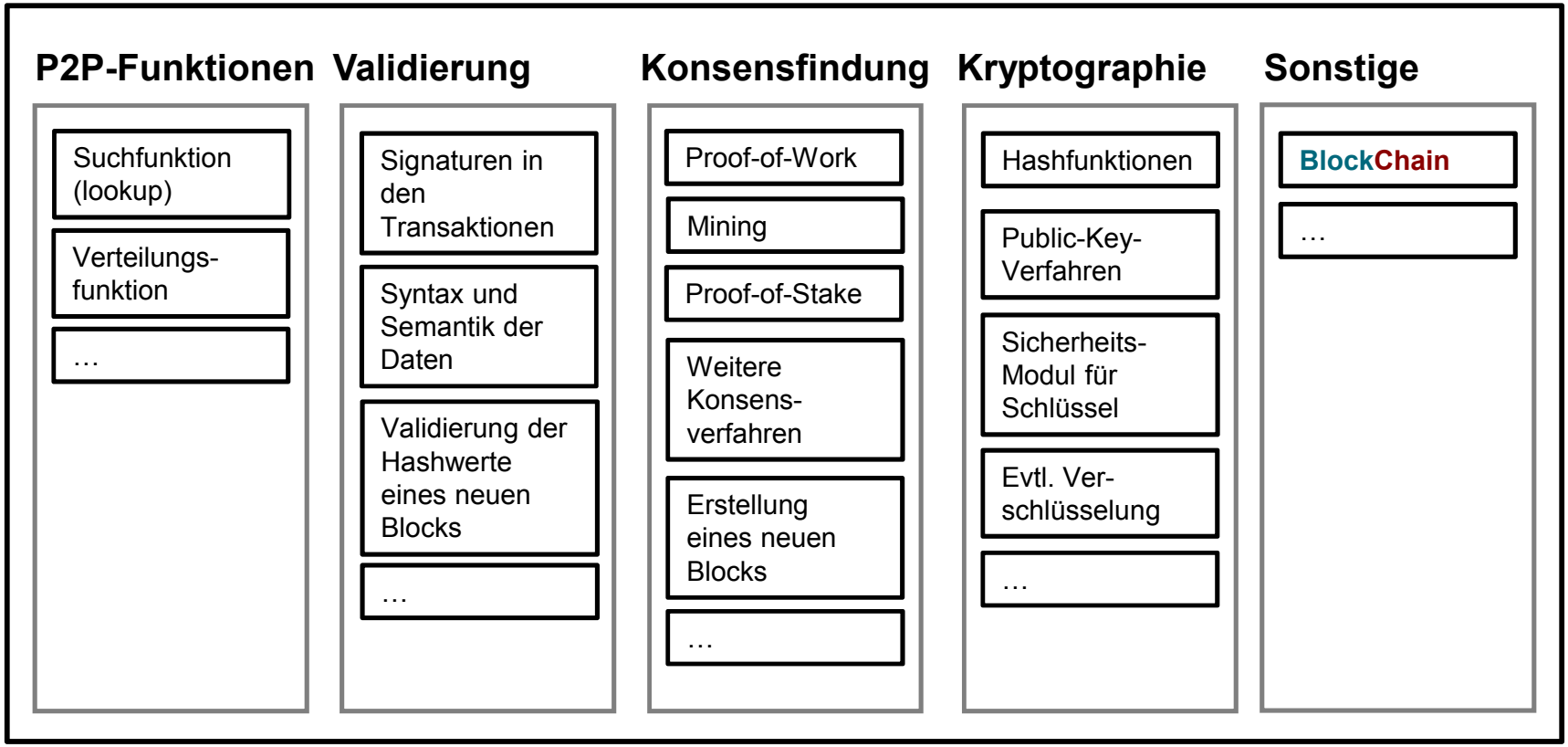


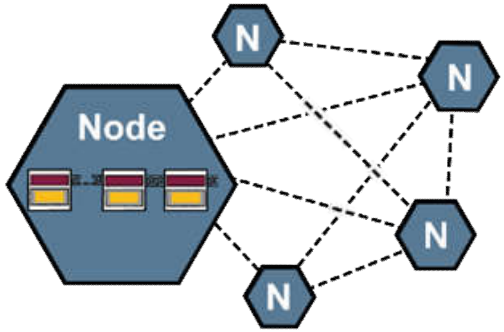
- **Die BlockChain-Infrastruktur**
  (Peer-to-Peer-Netzwerk, Nodes mit allen Kommunikations-, Sicherheits- und Vertrauensfunktionen, die **BlockChain** als Datenstruktur, …)

- **Die BlockChain-Anwendungen**
  (Blockchain-App, Wallet/Schlüssel, eigentliche Anwendung, …)

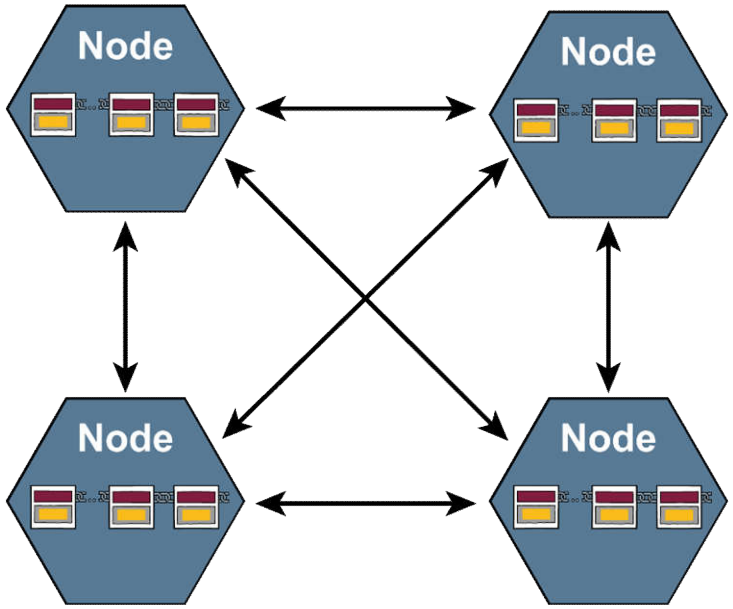
- Die **Transaktionen** als Schnittstelle dazwischen

BlockChain-Infrastruktur
→ Funktionen in einer Node





BlockChain-Infrastruktur
→ Eigenschaften: verteilt und redundant



Robustes Peer-to-Peer-Netzwerk

- **Skalierbarkeit / Ressourcenbedarf**
  - Bandbreite zwischen den Nodes
  - Speicherplatzkapazität auf der Node (Bitcoin BlockChain hat eine Größe von 160 G Byte)
  - Rechnerkapazität (CPU, RAM, …) einer Node
  - …
- **Zuverlässigkeit / Verfügbarkeit**
  - Anzahl der Nodes
  - Robust für die Verteilung von Transaktionen und neue Blöcke
  - Robust gegen DDoS-Angriffe
  - …

BlockChain-Infrastruktur

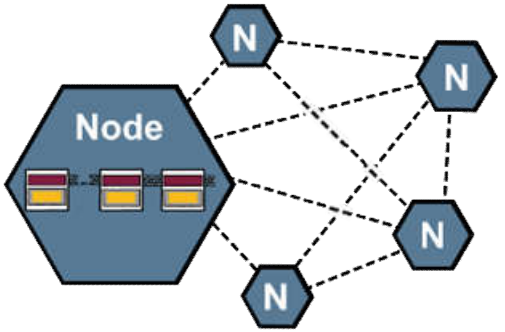
→ Eigenschaften: fälschungssicher/unveränderlich

Kryptographie-Agilität

- **Stand der Technik** (Technische Richtlinie: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“)
  - **Public-Key-Verfahren** (*Signierung / Verifizierung* von Transaktionen)
    → (*RSA - 3.000 bit*)
  - **Hashfunktionen** (*Adresserzeugung, HashPrev, Merkle Hash*)
    → (*SHA-3 - 256 bit*)

- **Risiko Quantencomputing** → Post-Quantum-Kryptoverfahren

- **Lebensdauer der BlockChain / Kryptographie**
  - Wechseln von kryptographischen Verfahren
    (z.B. alle 10 Jahre Organisation eines Hard Fork)

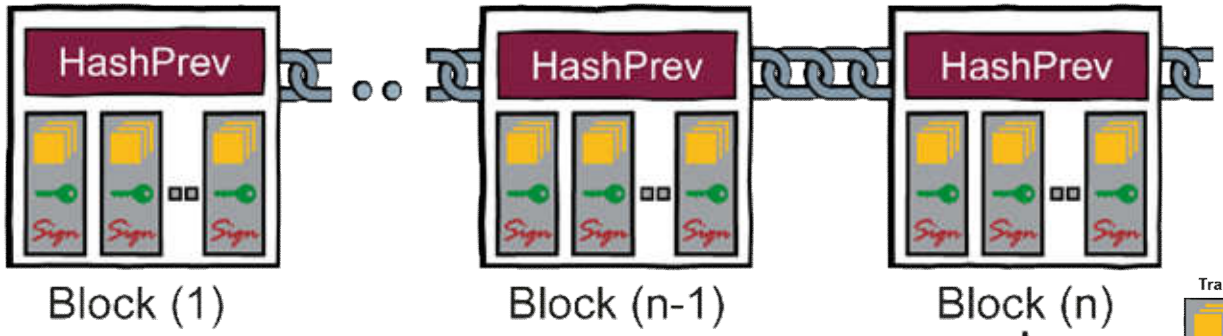


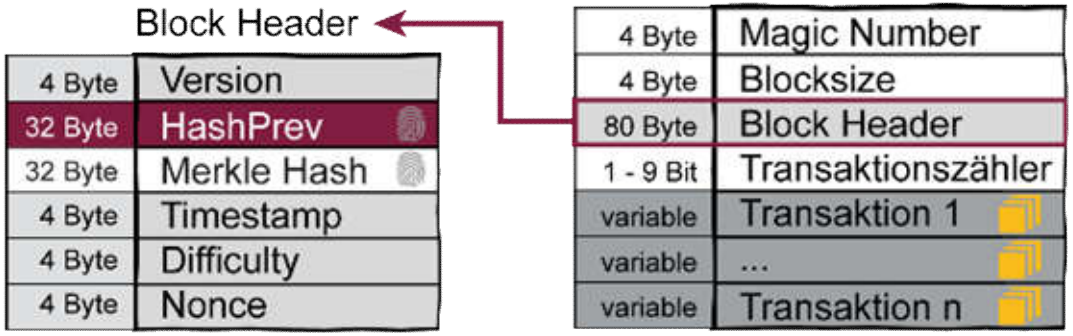
BlockChain-Infrastruktur

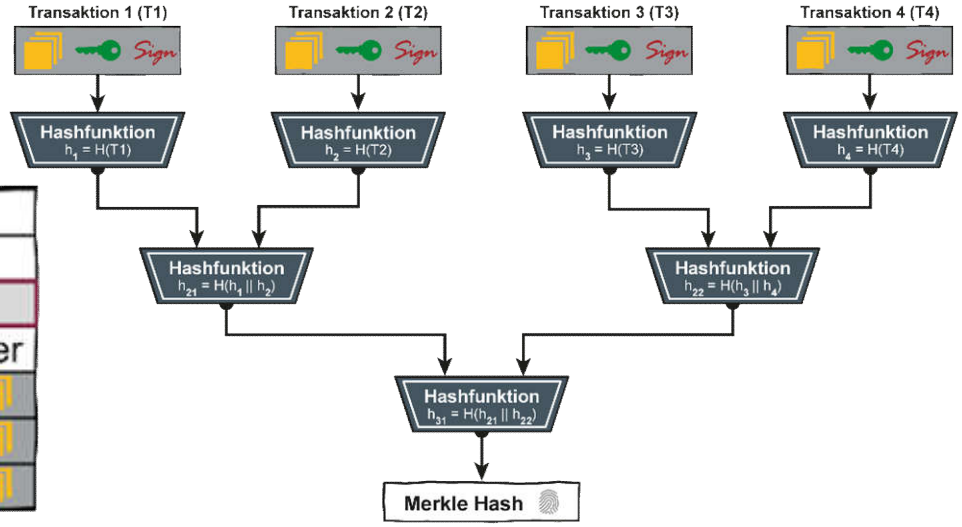
→ Eigenschaft: Zeitfolge protok./nachvollziehbar

internet-sicherheit.

Clevere Nutzung von Hashfunktionen





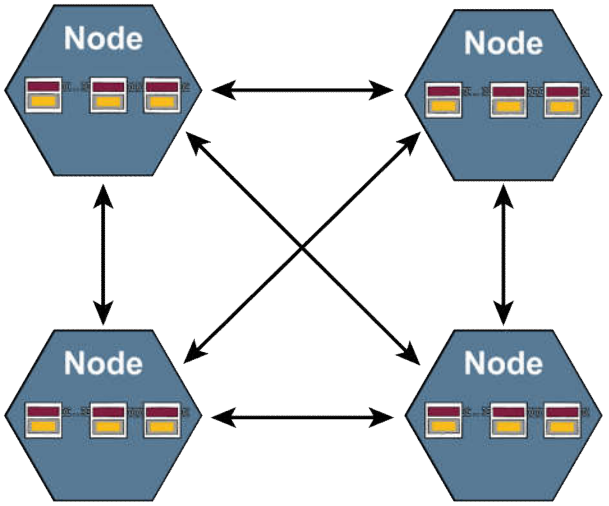


$$HashPrev_n = H\ (\ Block\text{-}Header_{n-1}\ )$$

Daten in der **BlockChain** können **nicht gelöscht** werden!

BlockChain-Infrastruktur
→ Eigenschaft: ohne zentrale Instanz

- Die **BlockChain**-Technologie bietet **"programmiertes Vertrauen"** mit Hilfe verschiedener IT-Sicherheits- und Vertrauensmechanismen.
- Alle IT-Sicherheits- und Vertrauensfunktionen sind inhärent als **"Security-by-Design"** in die **BlockChain**-Technologie integriert.



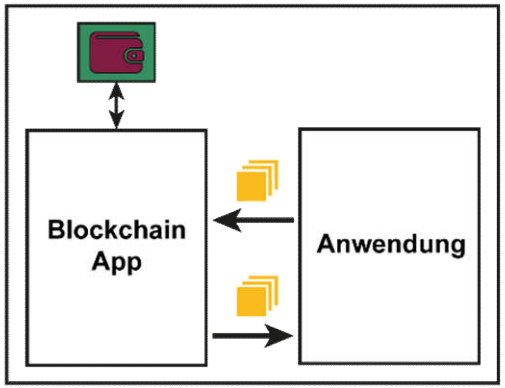
Vertrauenswürdigkeitsmechanismen

- **Verteilte Konsensfindungsverfahren**
  - Gewinnen einer Krypto-Aufgabe (Proof-of-Work)
  - Wichtig für die **BlockChain** (Proof-of-Stake)
- **Verteilte Validierung**
  - Echtheit der Transaktionen (Überprüfung der Hashwerte/Signatur)
  - Korrektheit der Blöcke (Überprüfung der Hashwerte/Konsens)
  - Syntax, Semantik, … (Schutz gegen Fremdnutzung)
- **Berechtigungsarchitektur**
  - Zugriff, Validierung, …
  - privat, öffentlich, …

BlockChain-Anwendung
→ Übersicht

- **Blockchain-App**
  - Daten von der Anwendung werden in Transaktionen vom **BlockChain-Teilnehmer (Wallet-Besitzer)** signiert und in der **BlockChain** verstetigt
  - Transaktionen werden verifiziert und die Daten von der Anwendung „verarbeitet“

- **Wallet**
  - Hardware-Sicherheitsmodule (USB-, NFC-Token, …) in denen die Schlüssel sicher gespeichert sind

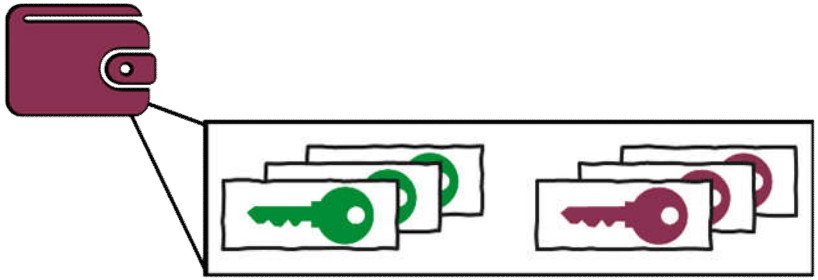


Teilnehmer

- **Anwendung**
  - Die eigentliche Anwendung nutzt die **BlockChain**-Technologie

BlockChain-Anwendung
→ Sicherheit der Schlüssel

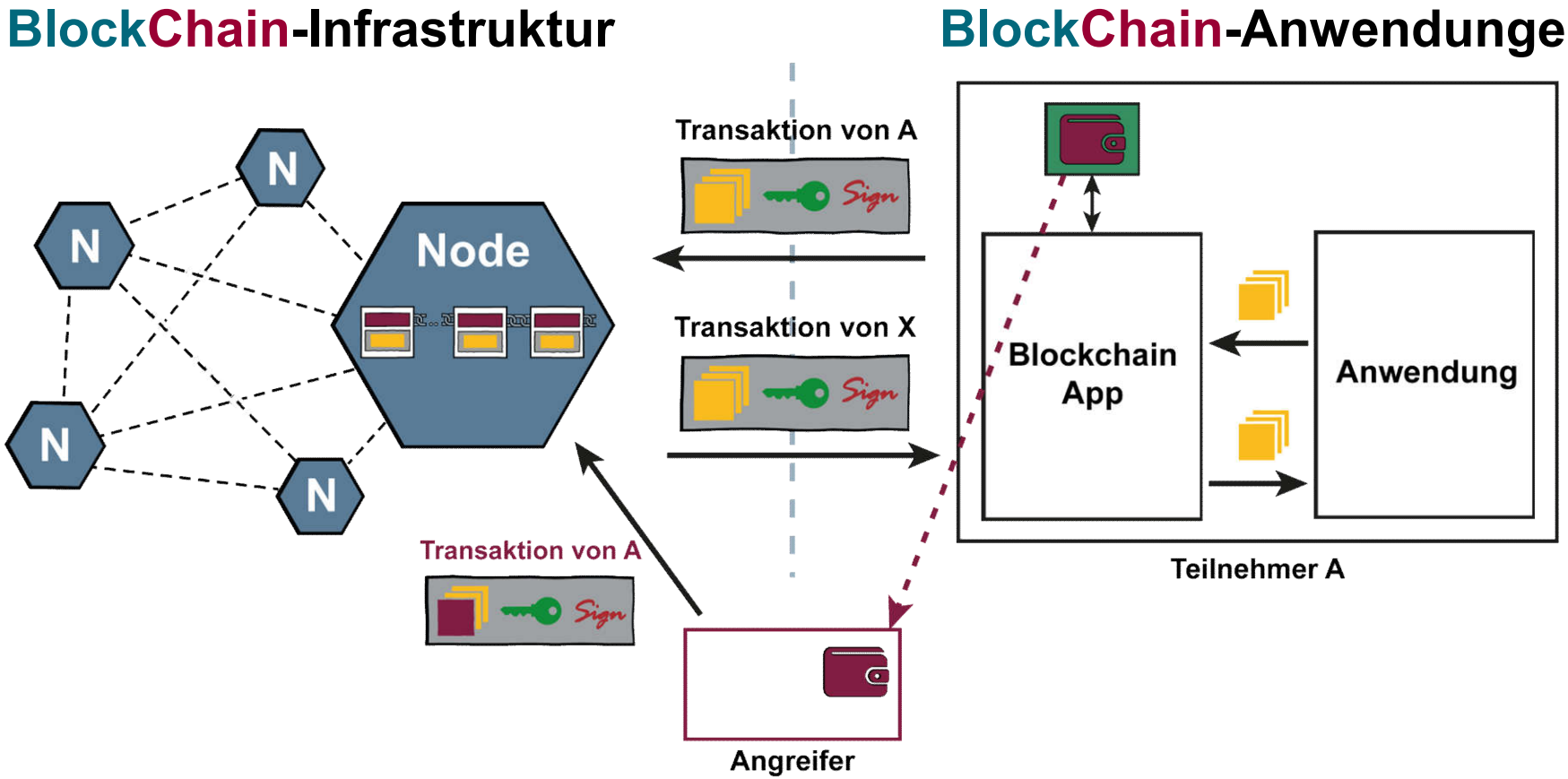
- Die Sicherheit der **BlockChain**-Technologie hängt auch von der **Geheimhaltung der privaten Schlüssel** der Public-Key-Verfahren ab (Wallet).



- **Gefahren** bei nicht ausreichendem Schutz des **privaten Schlüssels**
  - Der **private Rechner / IoT-Gerät** wird **gehackt** (Malware)
  - Die **Website** der Online Wallet (Service Node) wird **gehackt**
  - Ein nicht ausreichend gesichertes **Smartphone** wird **gestohlen** (Light N.)
  - Der **private Schlüssel** wird ***gestohlen*** oder ***unberechtigt genutzt***

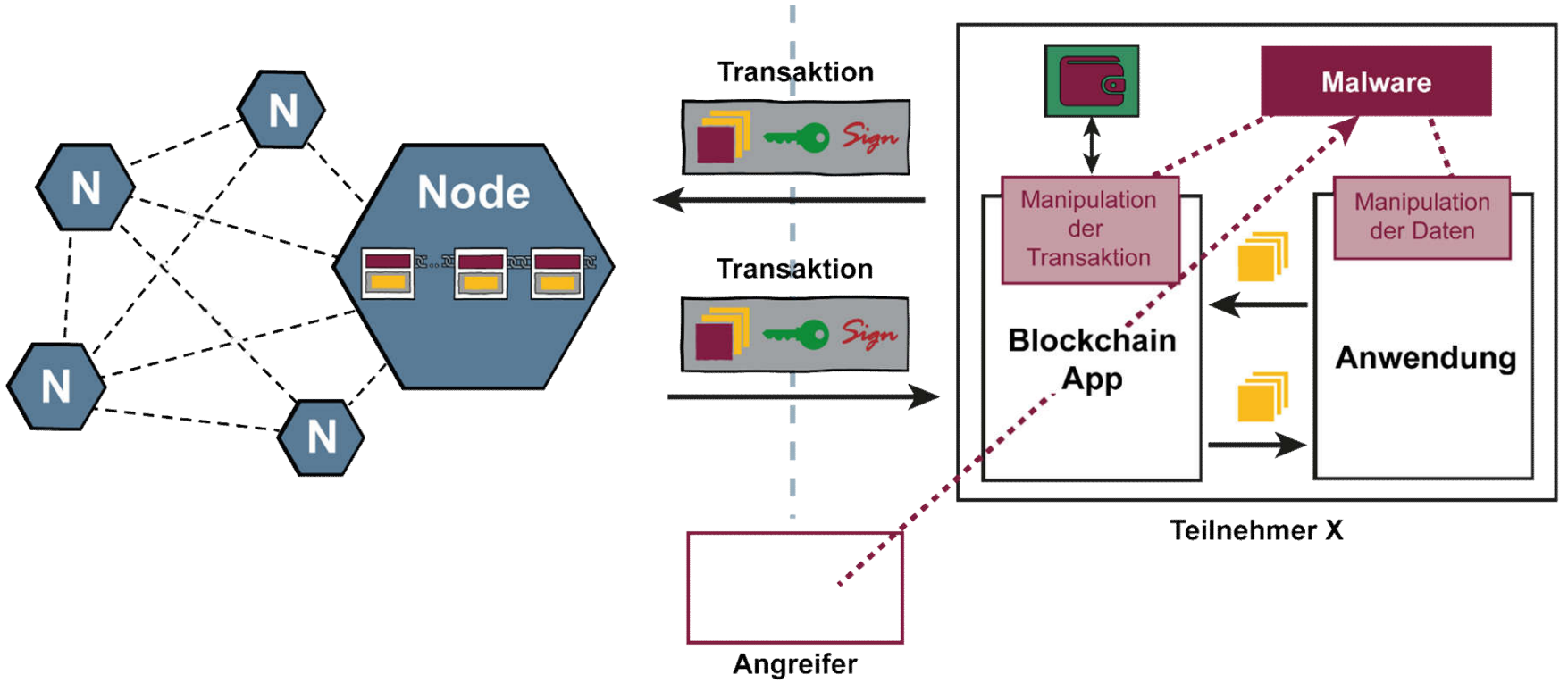
- Der Schutz des **privaten Schlüssels** sollte mit Hilfe von **Hardware-Security-Module** realisiert werden (Smartcards, Sec-Token, High-Level-Sicherheitsmodule) und **unberechtigte Nutzung muss aktiv verhindert werden**!

BlockChain-Anwendung
→ Manipulationen der Transaktionen



- Der Angreifer ***„besitzt“*** die **Wallet/Schlüssel** oder kann sie ***„unberechtigt nutzen“***
  - Damit kann er valide Transaktionen für den entsprechenden Teilnehmer A erstellen und die **BlockChain**-Anwendung manipulieren

BlockChain-Anwendung
→ Manipulationen der Daten

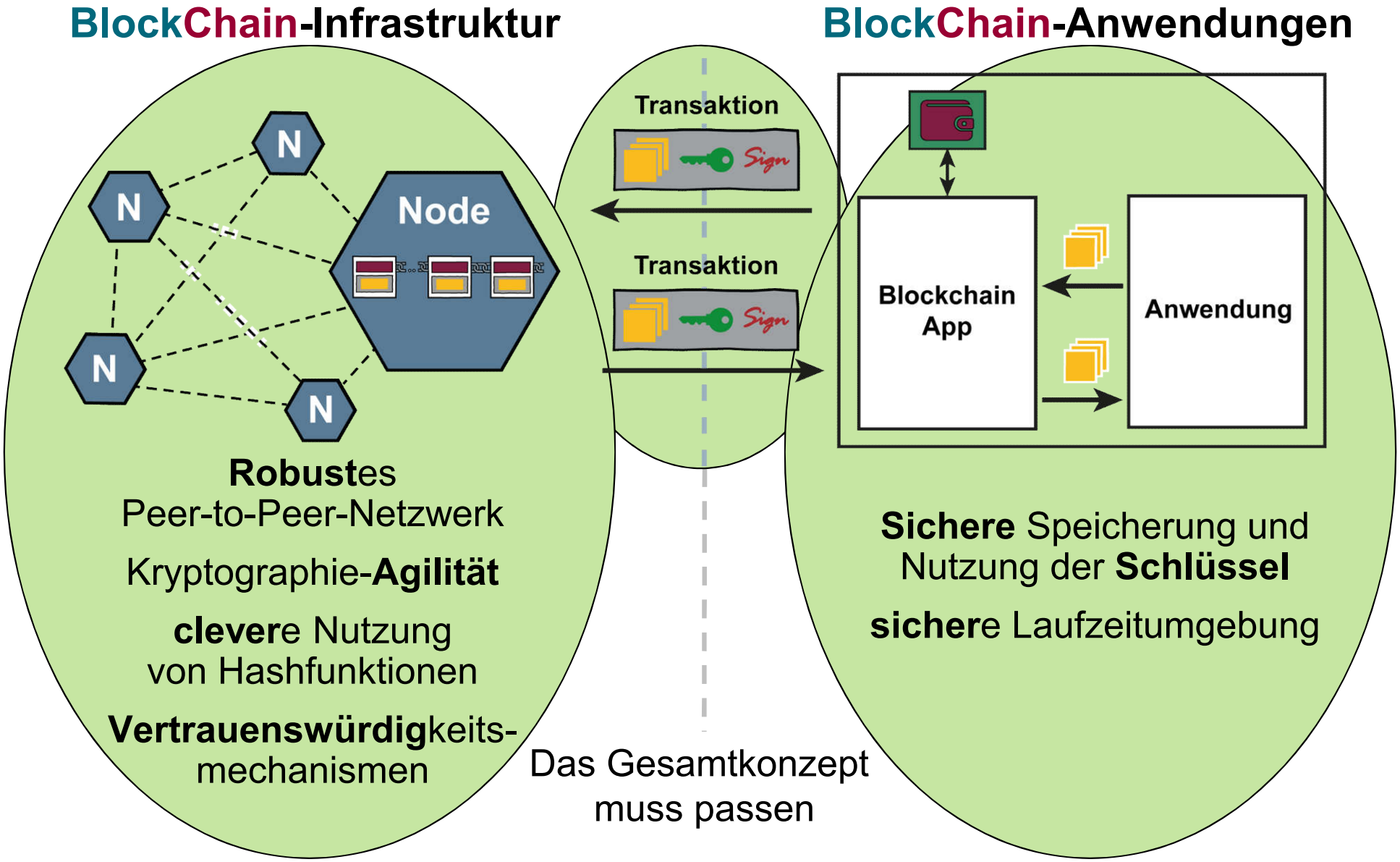


- Der Angreifer „betreibt“ auf dem IT-System des Teilnehmers X eine **Malware**
  - Damit kann der Angreifer die Daten der **BlockChain**-Anwendung manipulieren
  - Sowohl ausgehende und eingehende Transaktionen
  - Die Transaktionen sind im **BlockChain** sicher gespeichert

BlockChain-Anwendung
→ Vertrauenswürdig Laufzeitumgebung

- Wie kann die **Wallet angemessen geschützt** werden?
  - Hardwaresicherheitsmodul
  - Verhinderung der unberechtigten Nutzung (sichere Aktivierung)
  - …
- Wie kann ein **Malware-Angriff verhindert** werden?
  - Trusted Computing
  - Trusted Execution Environment
  - Sandboxing
  - …

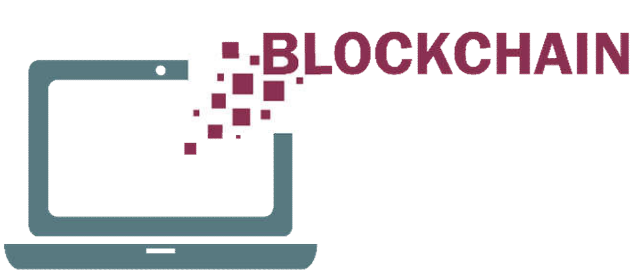
BlockChain-Technologie
→ Trusted BlockChain Interfaces



Trusted BlockChain Interfaces

BlockChain-Technologie
→ Zusammenfassung

- Die **BlockChain**-Technologie schafft eine Grundlage für verteilte, automatisierte und **vertrauenswürdige Zusammenarbeit**
- Die **BlockChain**-Technologie hat **"Security-by-Design"**
- Die **BlockChain-Infrastruktur** hat komplexe Kommunikations-, Sicherheits- und Vertrauenswürdigkeitsfunktionen, die im Einklang zueinander die notwendigen Sicherheits- und Vertrauenseigenschaften erbringen.
- Die **BlockChain-Anwendungen** ist dem „realen Leben“ ausgesetzt und muss für die **sicher Speicherung und Nutzung der Schlüssel** sowie für eine **manipulationsfreie Laufzeitumgebung** sorgen.
- Die Kombination beider Aspekte repräsentiert das **„Trusted BlockChain Interfaces“**



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Trusted BlockChain Interfaces

Mit BlockChain in die Zukunft!

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Anhang / Credits

Wir empfehlen

- **Kostenlose App securityNews**

- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/channel/UCEMkHjW9dHcWfek_En3xhjg
-
- **Cybärcast – Der IT-Sicherheit Podcast**
  https://podcast.internet-sicherheit.de/

- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/

Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

Google+
https://plus.google.com/107690471983651262369/posts

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/

Literatur

Artikel:

C. Kammler, N. Pohlmann: „Kryptografie wird Währung – Bitcoin: Geldverkehr ohne Banken“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 6/2013
https://norbert-pohlmann.com/app/uploads/2015/08/308-Kryptografie-wird-W%C3%A4hrung-Bitcoin-Geldverkehr-ohne-Banken-Prof-Norbert-Pohlmann.pdf

R. Palkovits, N. Pohlmann, I. Schwedt: „Blockchain-Technologie revolutioniert das digitale Business: Vertrauenswürdige Zusammenarbeit ohne zentrale Instanz“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 2/2017
https://norbert-pohlmann.com/app/uploads/2017/07/357-Blockchain-Technologie-revolutioniert-das-digitale-Business-Vertrauensw%C3%BCrdige-Zusammenarbeit-ohne-zentrale-Instanz-Prof.-Norbert-Pohlmann.pdf