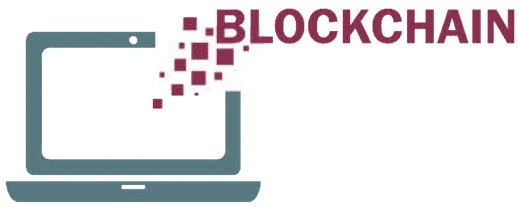


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

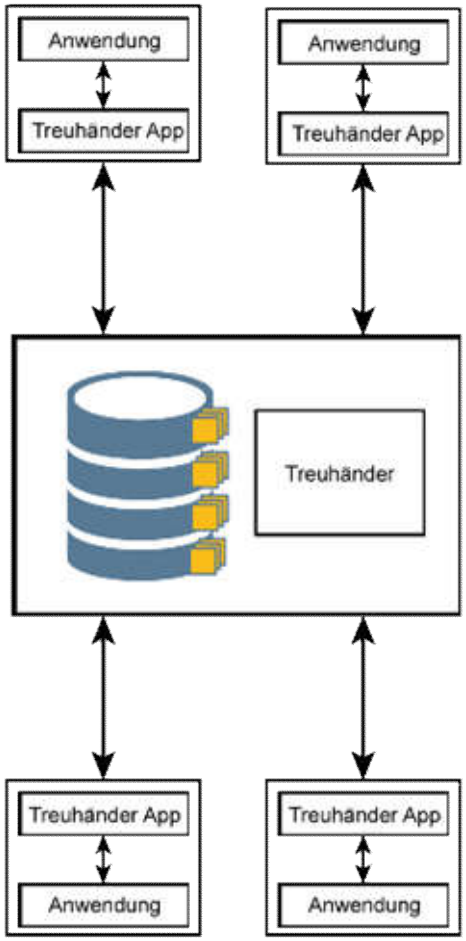
Blockchain-Technologie als Tool für Industrial Security

Prof. Dr. (TU NN)
Norbert Pohlmann

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

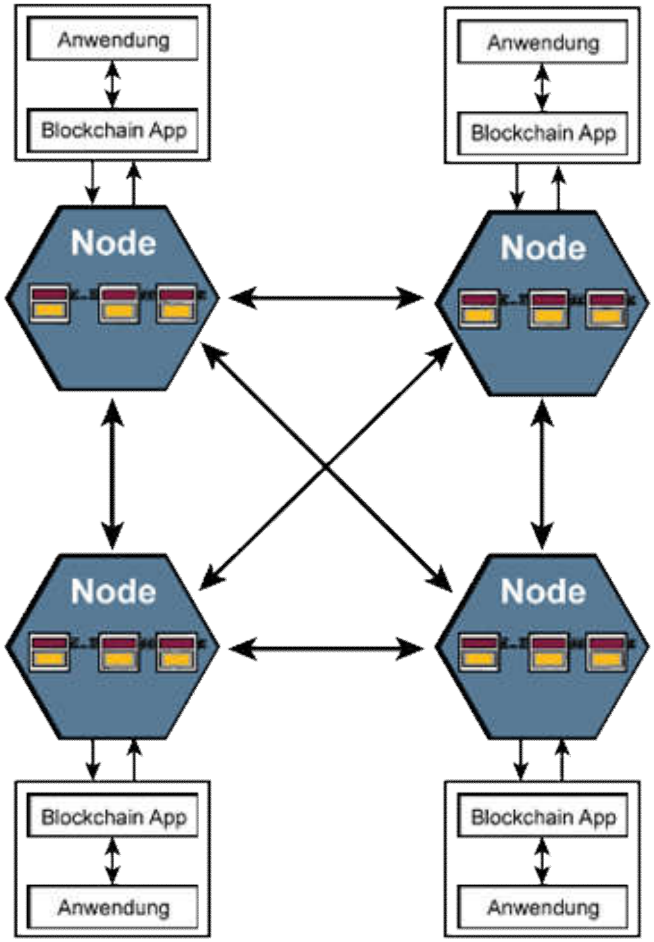
if(is) internet-sicherheit.

BlockChain-Technologie
auf den Punkt gebracht



Zentrale Architektur

Transaktionsspeicher



Dezentrale Architektur

BlockChain Konzept
Unterschiedliche Sichtweisen

- Für einen **Informatiker** ist die **BlockChain** eine **einfache Datenstruktur**, die Daten sind in einzelnen „Blöcken“ verkettet und in einem ***verteilten Netz*** **redundant** (mehrfach) verwaltet.

  Die Alternative wäre z.B. eine konventionelle Datenbank, die von allen Teilnehmern fortlaufend repliziert wird.

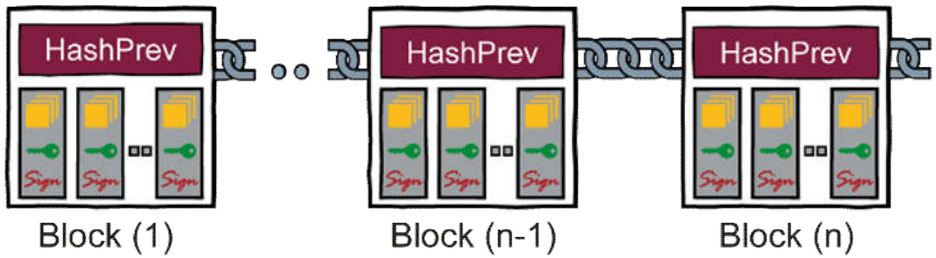
- Für die **IT-Sicherheitsexperten** hat die **BlockChain** den Vorteil, dass die **Daten** in den einzelnen „Blöcken“ **manipulationssicher gespeichert** werden können, das heißt, die Teilnehmer an der **BlockChain** sind in der Lage,
  → die **Echtheit**,
  → den **Ursprung** und
  → die **Unversehrtheit der gespeicherten Daten** zu überprüfen.

  Die Alternative wäre z.B. ein PKI-System.

- Für den **Anwendungsdesigner** bedeutet die Nutzung der **BlockChain**-Technologie eine **vertrauenswürdige und automatisierte Zusammenarbeit zwischen verschiedenen Organisationen**.

  Die Alternative wäre z.B. ein kostenintensiver Treuhänder.

BlockChain-Technology
Sicherheitseigenschaften

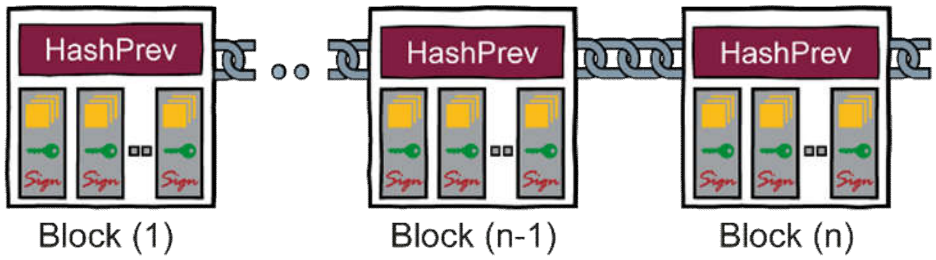


BlockChain

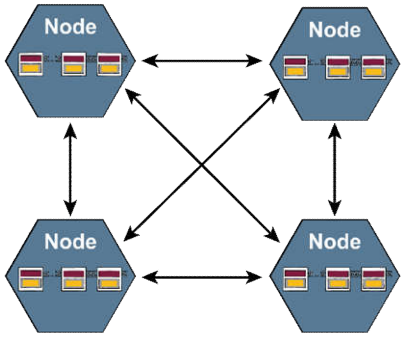
- ist eine **fälschungssichere**,
- **verteilte**, **redundante** Datenstruktur
- in der **Transaktionen in der Zeitfolge protokolliert**
- **nachvollziehbar**, **unveränderlich** und
- **ohne zentrale Instanz** abgebildet sind.

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

BlockChain-Technology
Datenstruktur einer BlockChain

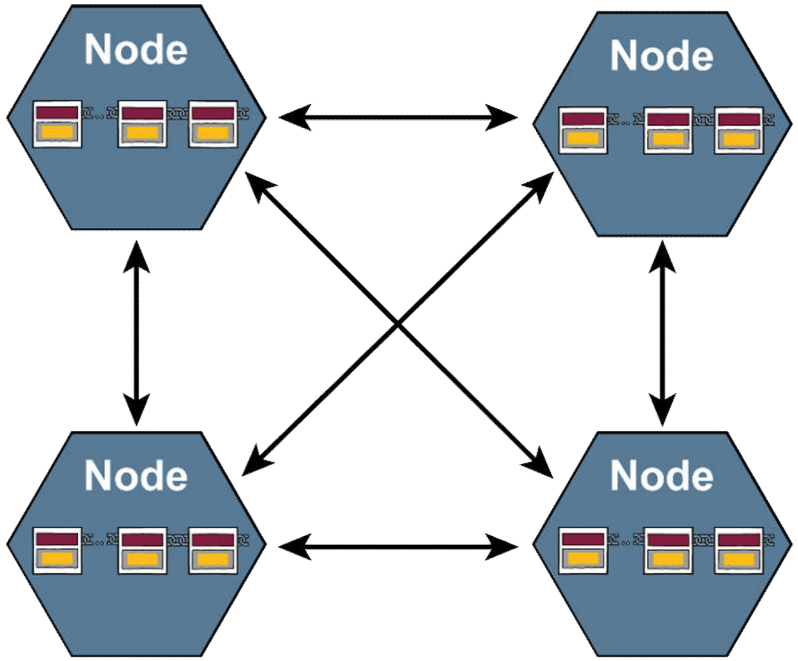


- Die **Daten** sind Transaktionsdaten mit Geldeinheiten, Zertifikaten, Produktionsdaten, Sensordaten, Source Code, ... digitale Werte
- **Transaktionen** mit **Daten** werden vom Teilnehmer erstellt und **sign**iert (Wallet/Schlüssel). Passende **Public Key** in der Transaktion. Verteilung
- **Block** *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-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
  - …

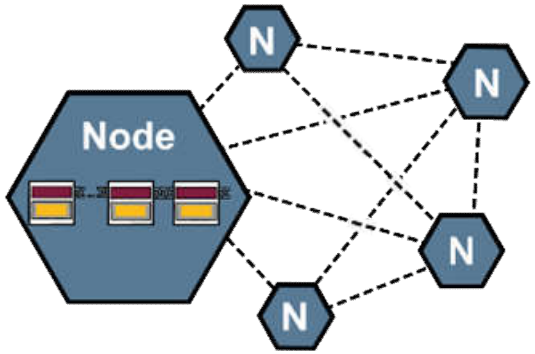
BlockChain-Infrastruktur
Eigenschaften: fälschungssicher/unveränderlich

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

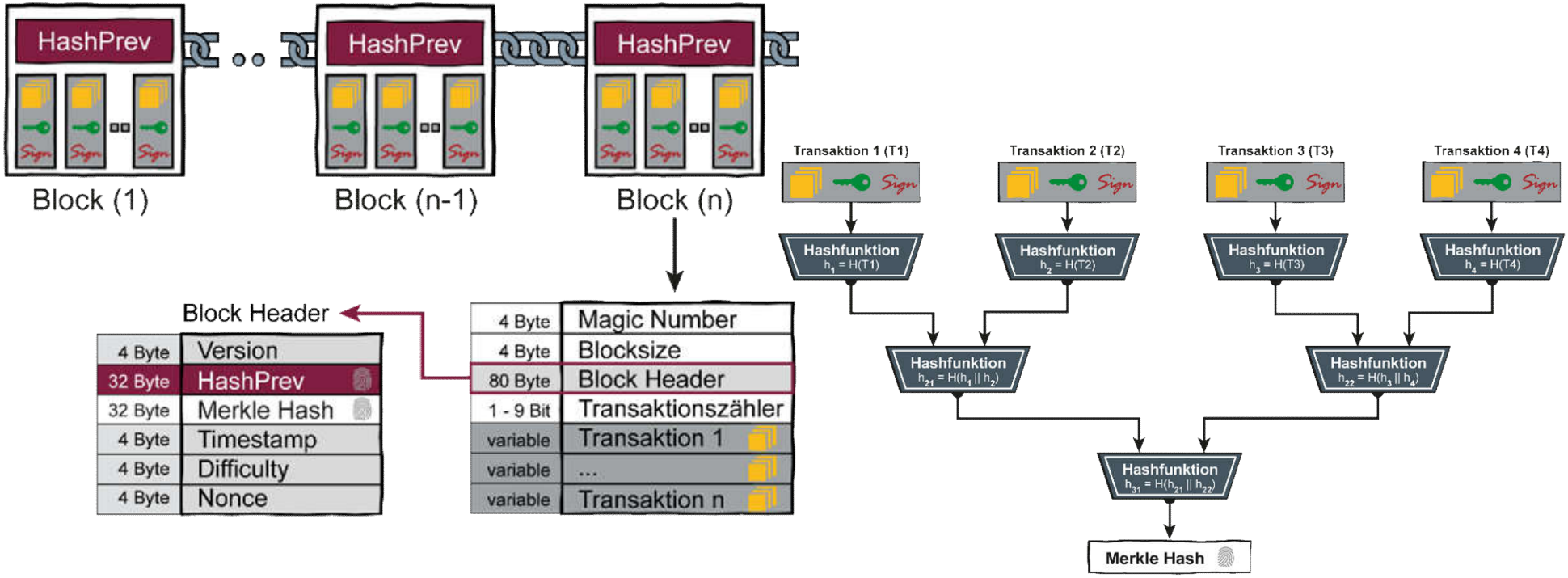
- **Lebensdauer der BlockChain / Kryptographie**
  - Wechseln von kryptographischen Verfahren
    (z.B. alle 10 Jahre Organisation eines Hard Fork)



BlockChain-Infrastruktur

Eigenschaft: Zeitfolge protokolliert/nachvollziehbar

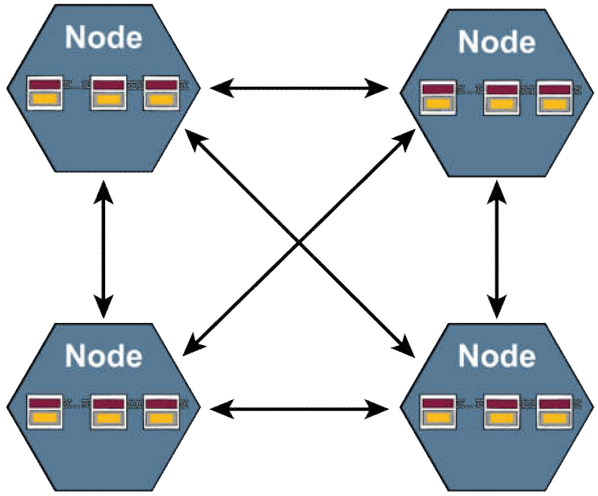
Clevere Nutzung von Hashfunktionen



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

BlockChain-Infrastruktur
Eigenschaft: ohne zentrale Instanz

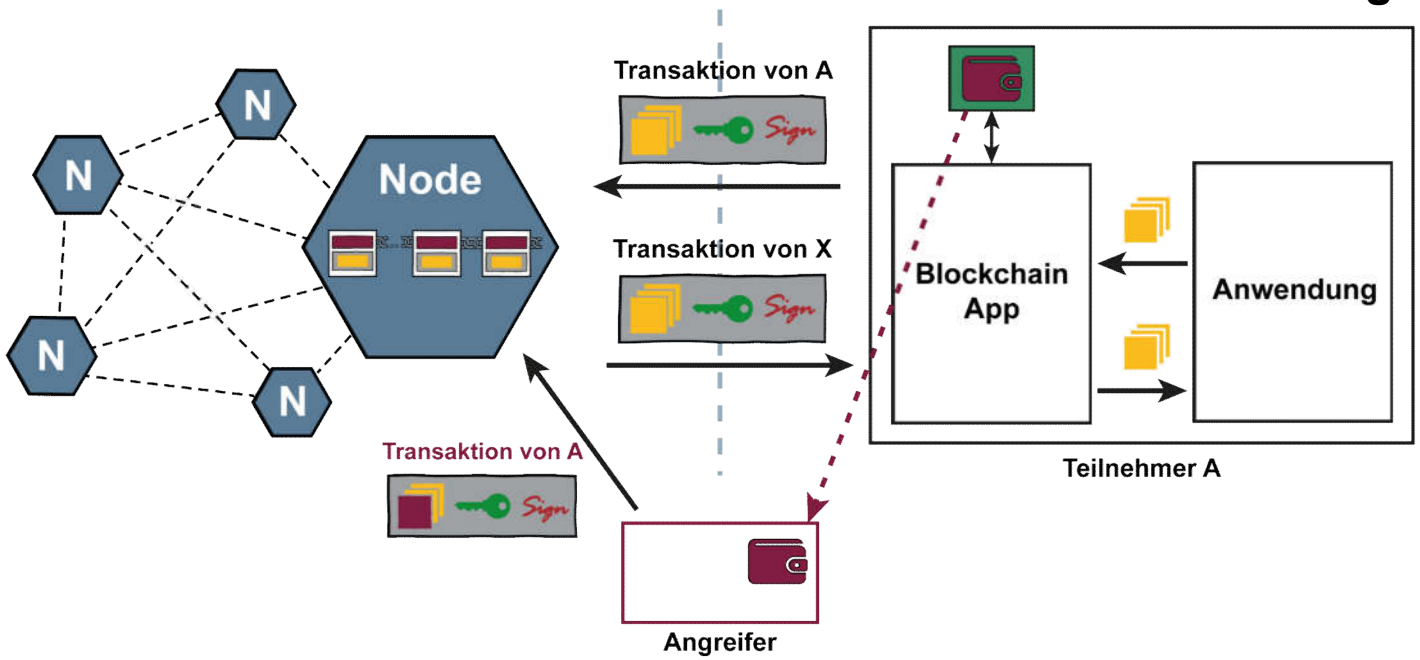
- Die **BlockChain**-Technologie bietet **"programmiertes Vertrauen"** mit Hilfe verschiedener IT-Sicherheits- und Vertrauensmechanismen.
- Alle IT-Sicherheits- und Vertrauensfunktionen sind inhärent als **"Security-by-Design"** in die **BlockChain**-Technologie integriert.



Vertrauenswürdigkeitsmechanismen

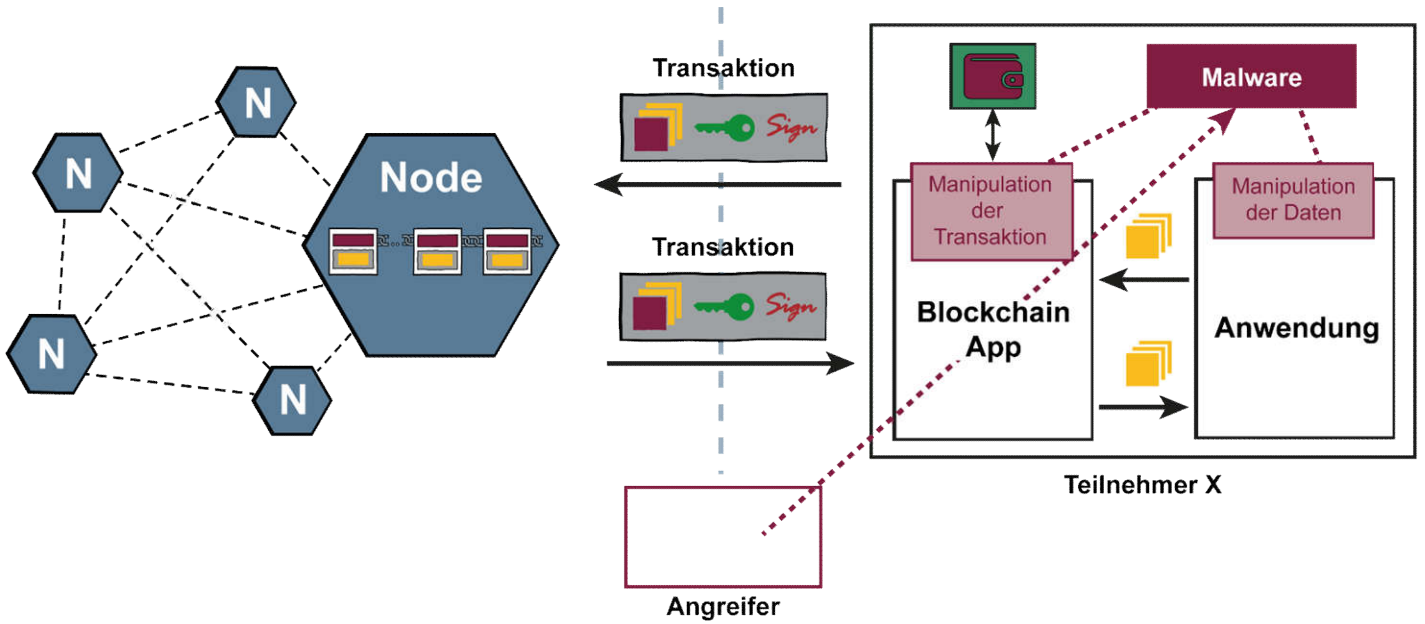
- **Verteilte Konsensfindungsverfahren**
  - Gewinnen einer Krypto-Aufgabe (Proof-of-Work)
  - Wichtig für die **BlockChain** (Proof-of-Stake)
- **Verteilte Validierung**
  - Echtheit der Transaktionen (Überprüfung der Hashwerte/Signatur)
  - Korrektheit der Blöcke (Überprüfung der Hashwerte/Konsens)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

BlockChain-Anwendung
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

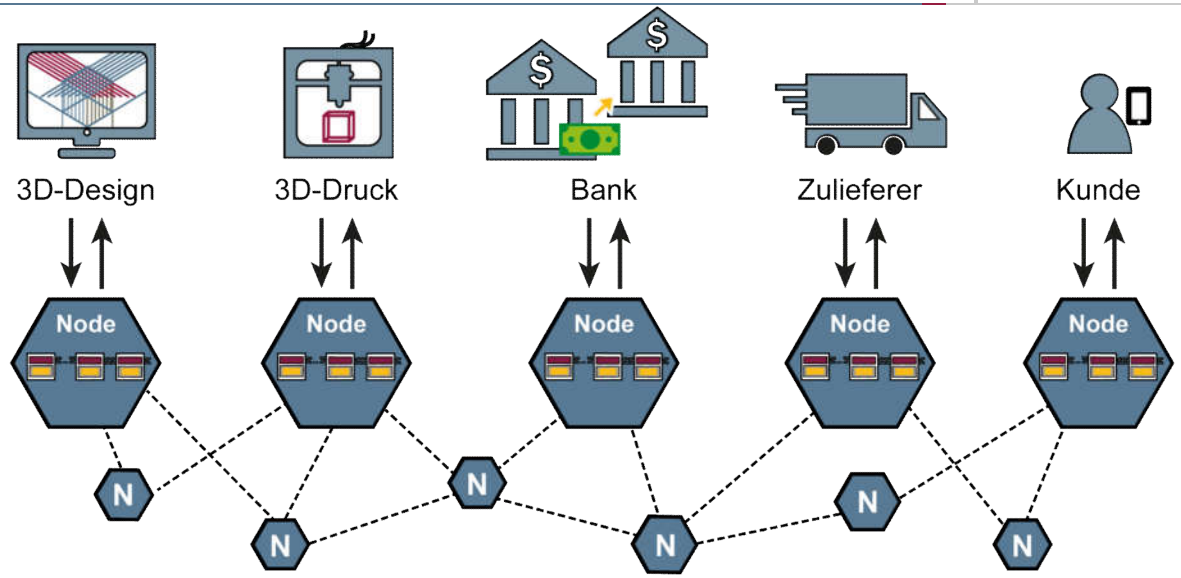
BlockChain-Anwendung
Manipulationen der Daten



- 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-Technologie-Anwendung
Automatische Produktions-, Bezahl- u. Lieferkette

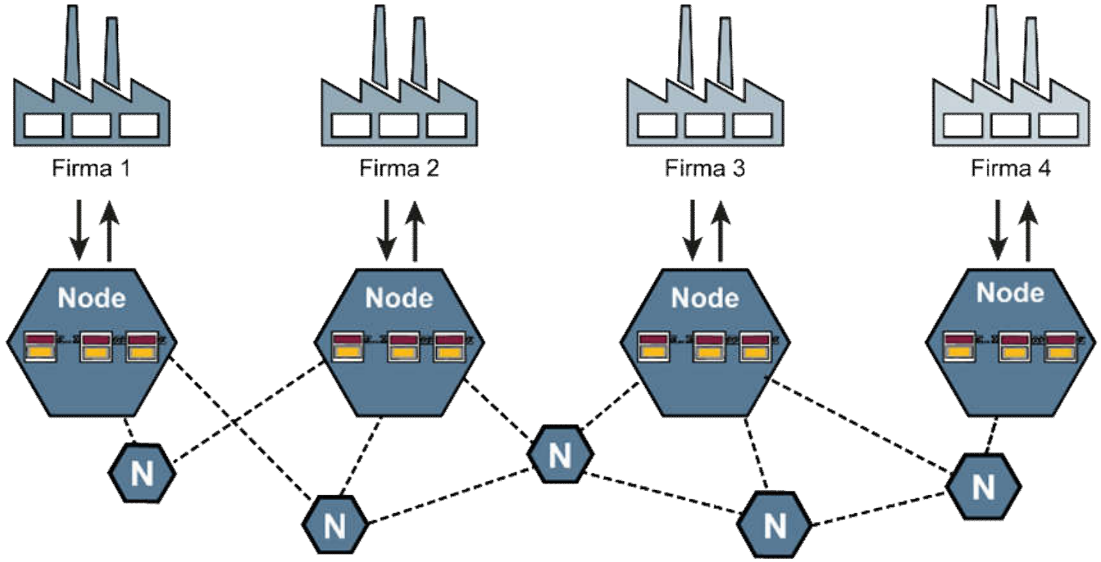
Kunde bestellt
Tasse und Lieferung,
zahlt sofort
mit der Bedingung,
dass innerhalb
von 7 Tagen geliefert wird.



Automatischer Ablauf

- **Kunde:** Bestellung → **BlockChain**
- **Design-Firma:** 3D-Design (one time use only) → **BlockChain**
- **Drucker-Firma:** Tasse wird als 3D-Druck gedruckt … Info → **BlockChain**
- **Versanddienst:** Transportiert Tasse, Bestätigung → **BlockChain**
- **Bank:** Transferiert die Gelder entsprechend … Info → **BlockChain**
- ***automatisch abgelaufen u. in der Blockchain vertrauenswürdig protokolliert***

BlockChain-Technologie-Anwendung
Lieferkette, Austausch, …

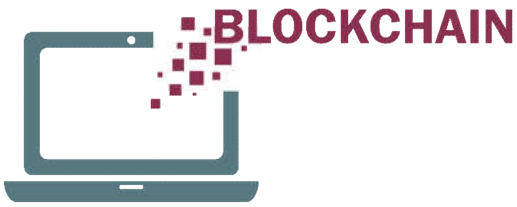


Automatisierte und vertrauenswürdige Zusammenarbeit

- Bestellungen für Produktion und Wartung
- Sensordaten für viele Anwendungen
- Automatisierte und vertrauenswürdige Zusammenarbeit mehrerer Maschinen
- …

BlockChain-Technologie
Zusammenfassung

- Die **BlockChain**-Technologie schafft eine Grundlage für verteilte, automatisierte und **vertrauenswürdige Zusammenarbeit**
- Die **BlockChain**-Technologie hat **"Security-by-Design"**
- Die **BlockChain**-Technologie braucht **keine zentrale Instanz**
- Die **BlockChain**-Technologie hat ein **hohes Potenzial** für neue Geschäftsmodelle und Ökosysteme.
- Die **BlockChain**-Anwendung muss auch **sicher und vertrauenswürdig** sein.
- Die **BlockChain**-Technologie wird ein immer wichtigeres **Tool für Industrial Security**



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Blockchain-Technologie als Tool für Industrial Security

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**

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