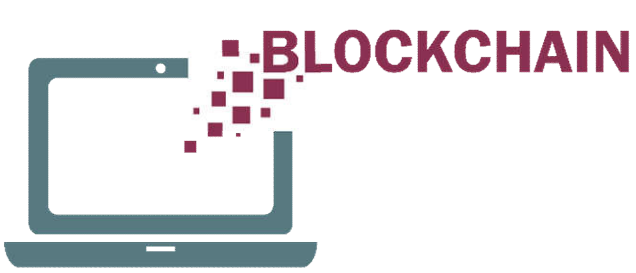


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

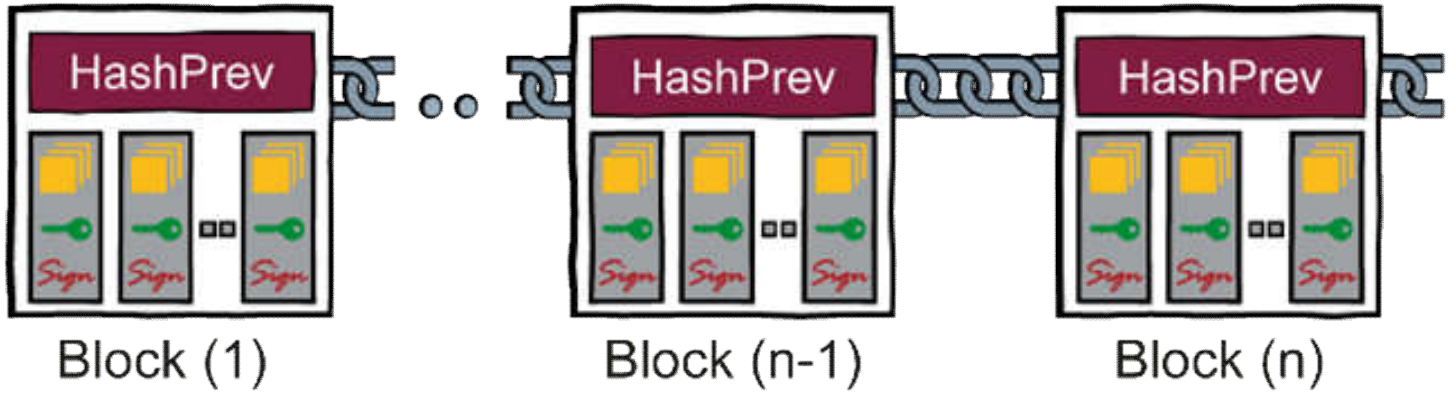
Wie sicher ist eigentlich die BlockChain?

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet-sicherheit.

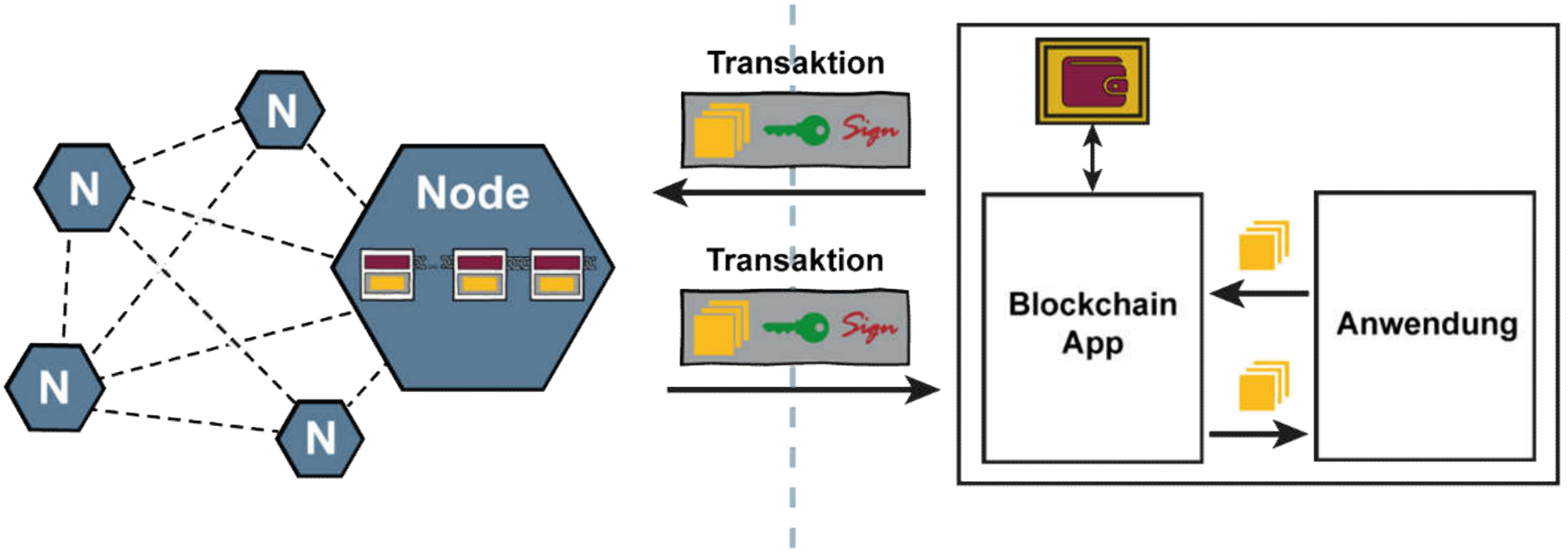
BlockChain-Technology
→ Sicherheitsattribute



BlockChain

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

BlockChain-Technologie
→ Sicherheit und Vertrauenswürdigkeit



- **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, …)

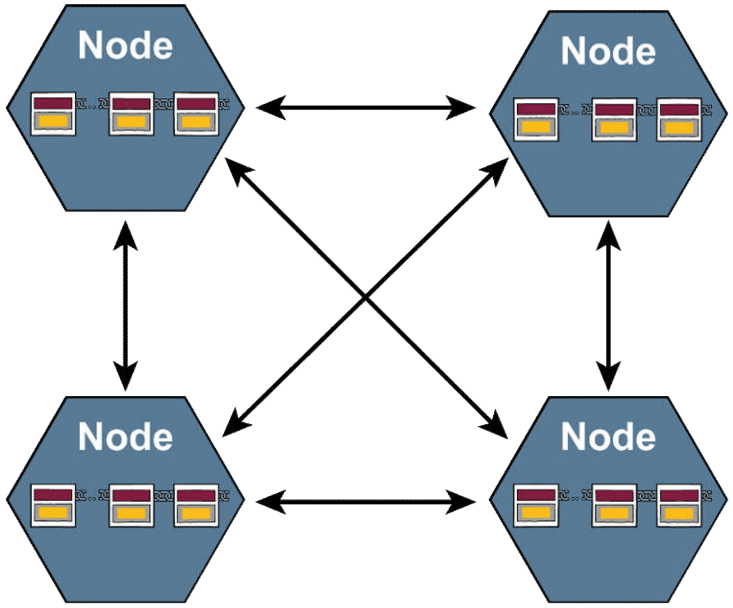
- Die **Transaktionen** als Schnittstelle dazwischen

BlockChain-Infrastruktur
→ Sec-Attribute: verteilt und redundant

if(is) internet-sicherheit.

Sicherheitseigenschaft: Verfügbarkeit der Daten

Robustes Peer-to-Peer-Netzwerk



- **Skalierbarkeit / Ressourcenbedarf**
  - ***Bandbreite*** zwischen den Nodes
  - ***Speicherplatzkapazität*** auf der Node (Bitcoin **BlockChain** hat eine Größe von 193 G Byte)
  - ***Rechnerkapazität*** (CPU, RAM, …) einer Node
  - …
- **Zuverlässigkeit der Nodes / Verfügbarkeit der Daten**
  - Anzahl der Nodes
  - Robust für die Verteilung von Transaktionen und neue Blöcke
  - Robust gegen DDoS-Angriffe
  - …

BlockChain-Infrastruktur

→ Sec-Attribute: fälschungssicher/unveränderlich

if(is) internet-sicherheit.

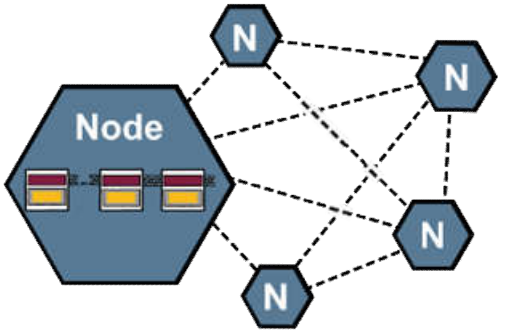
Sicherheitseigenschaft: Integrität und Authentizität der Daten

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)

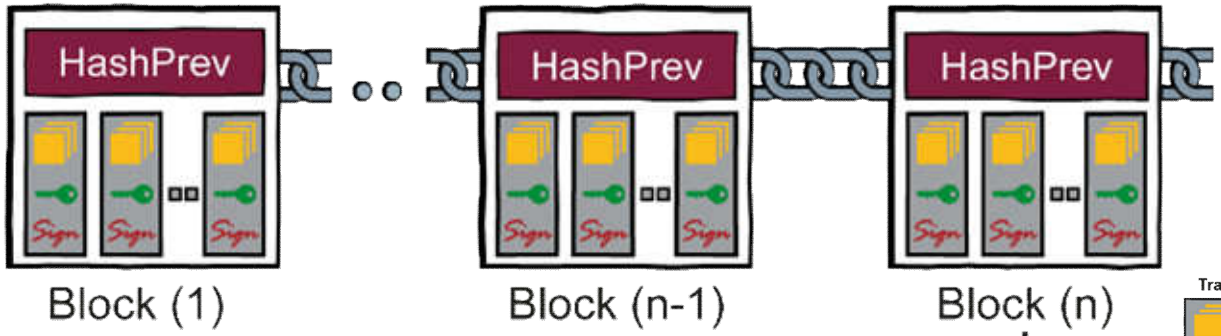


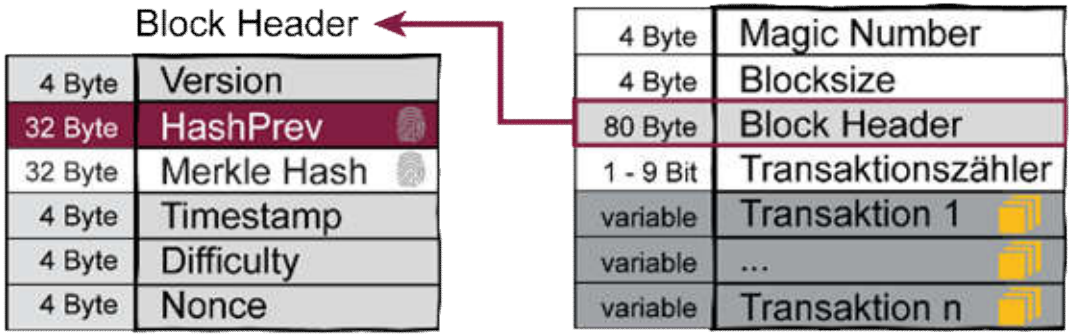
BlockChain-Infrastruktur

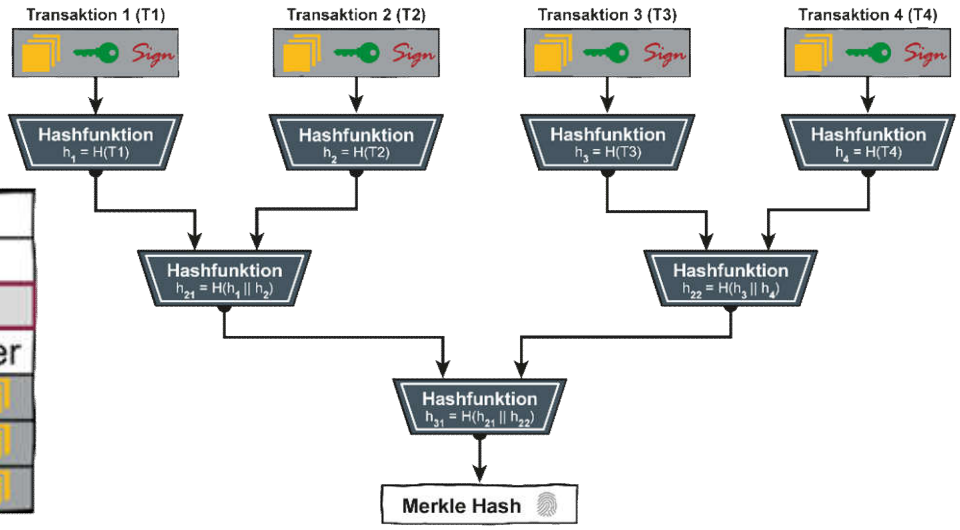
→ Sec-Attribute: Zeitfolge protok./nachvollziehbar

Sicherheitseigenschaft: Integrität der BlockChain

Clevere Nutzung von Hashfunktionen







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

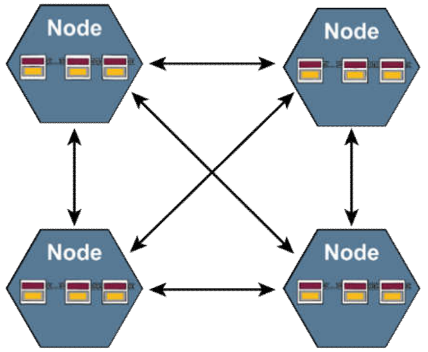
BlockChain-Infrastruktur
→ Sec-Attribute: ohne zentrale Instanz

if(is) internet-sicherheit.

Sicherheitseigenschaft: Vertrauen durch "Security-by-Design"

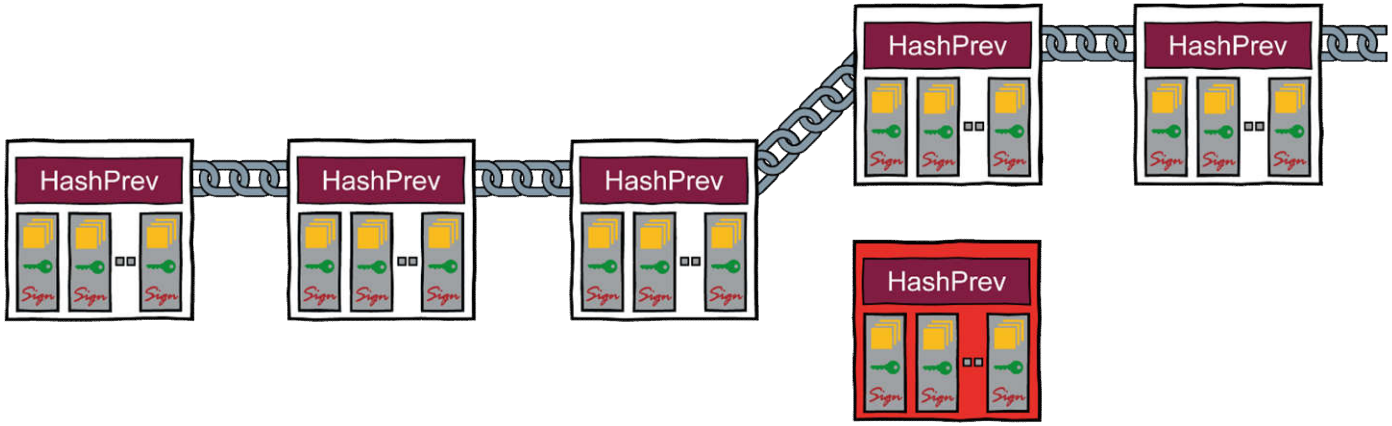
- Die **BlockChain**-Technologie bietet **"programmiertes Vertrauen"** mit Hilfe verschiedener IT-Sicherheits- und Vertrauensmechanismen.
- Alle IT-Sicherheits- und Vertrauensfunktionen sind inhärent als **"Security-by-Design"** in die **BlockChain**-Technologie integriert.

Vertrauenswürdigkeitsmechanismen

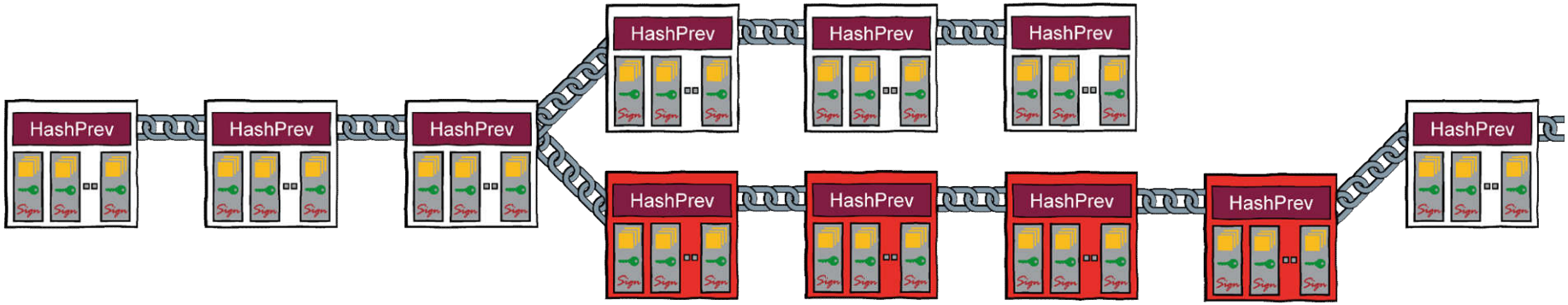


- **Verteilte Konsensfindungsverfahren**
  - Gewinnen einer Krypto-Aufgabe (Proof-of-Work)
  - Wichtig für die **BlockChain** (Proof-of-Stake), …
- **Verteilte Validierung**
  - Echtheit der Transaktionen (Überprüfung der Hashwerte/Signatur)
  - Korrektheit der Blöcke (Überprüfung der Hashwerte/Konsens),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

BlockChain-Infrastruktur
→ Angriff auf die Konsensfindung



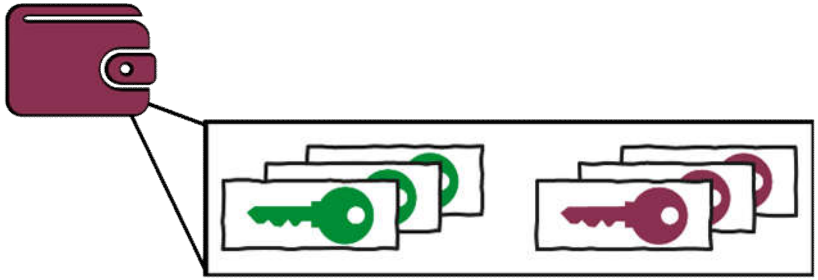
Double Spending



Erfolgreiche Double Spending Attacke

BlockChain-Anwendungssicherheit
→ Sicherheit der Schlüssel

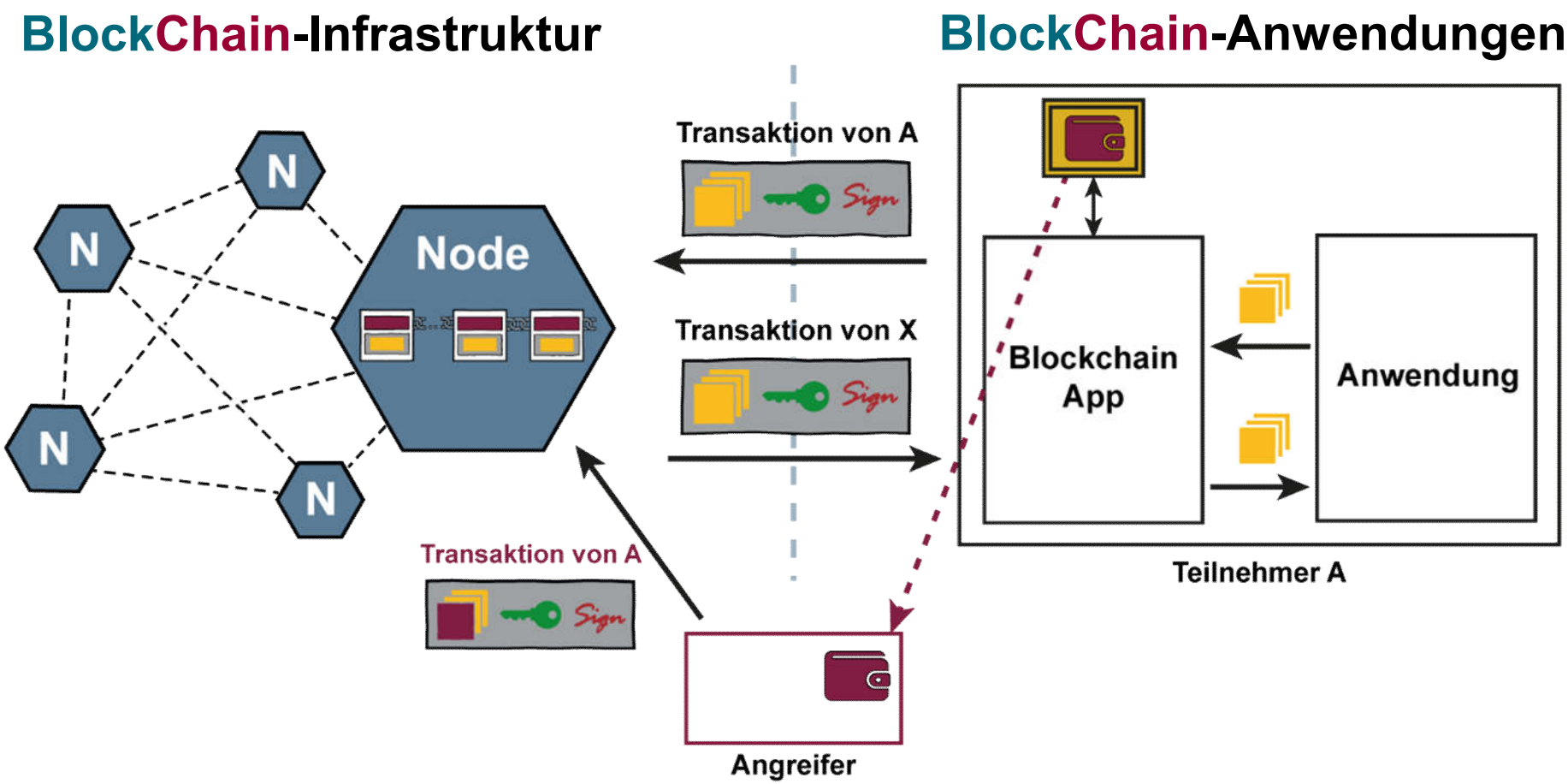
- Die Sicherheit der **BlockChain**-Technologie hängt auch von der **Geheimhaltung der geheimen Schlüssel** des Public-Key-Verfahrens ab (Wallet).



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

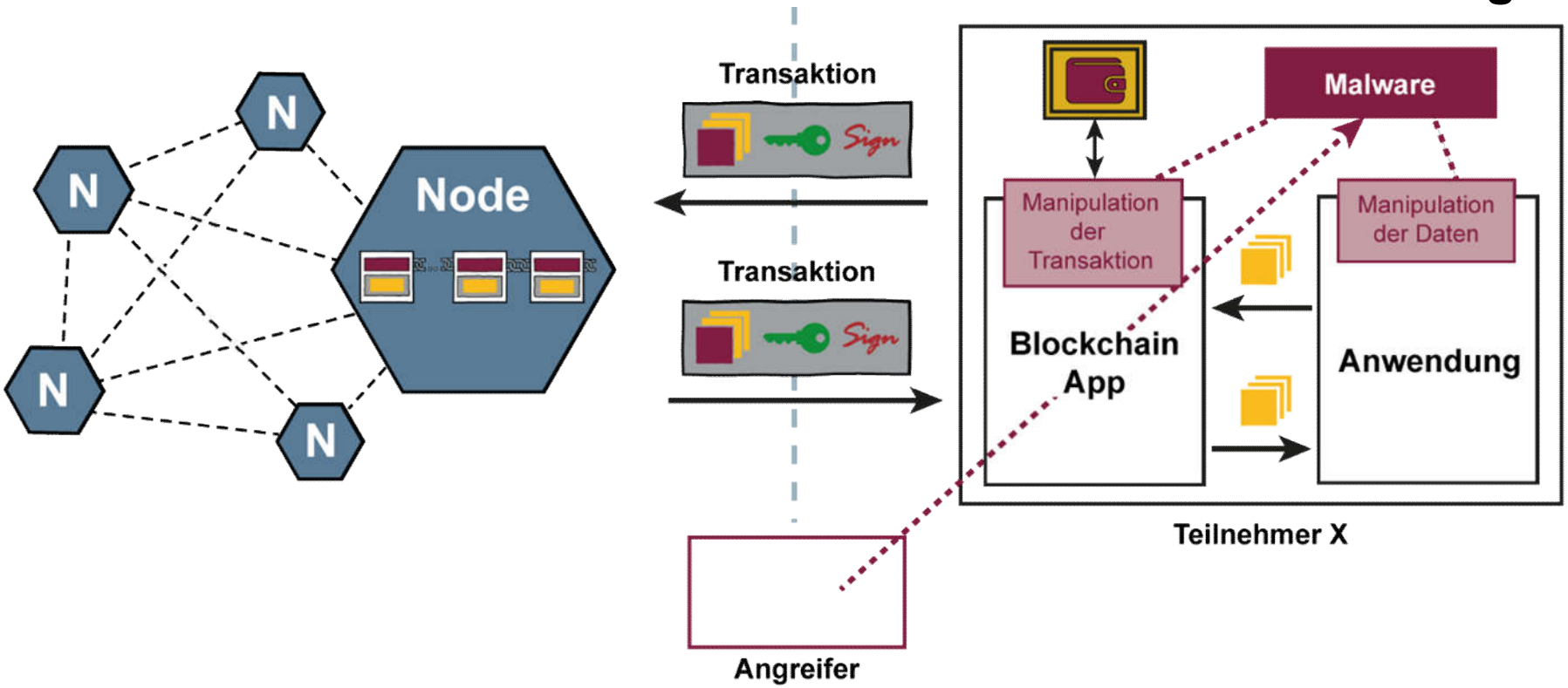
- Der Schutz des **geheimen Schlüssels** sollte mit Hilfe von **Hardware-Security-Module** realisiert werden (Smartcards, Sec-Token, High-Level-Sicherheitsmodule) und **unberechtigte Nutzung muss aktiv verhindert werden**!

BlockChain-Anwendungssicherheit
→ 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-Anwendungssicherheit
→ Manipulationen der Daten



Der **Angreifer „betreibt“** auf dem IT-System des Teilnehmers X eine **Malware**

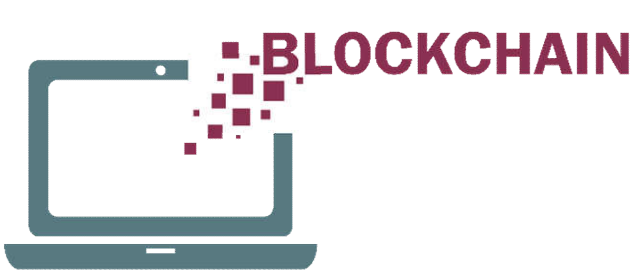
- Damit kann der Angreifer die Daten der **BlockChain**-Anwendung manipulieren
- Sowohl ausgehende als auch eingehende Transaktionen
- Die Transaktionen sind in der **BlockChain** sicher gespeichert

Wie sicher ist BlockChain?
→ Zusammenfassung

- Die **BlockChain**-Infrastruktur hat **komplexe Kommunikations-**, **Sicherheits-** und **Vertrauenswürdigkeitsfunktionen**, die im Einklang zueinander die notwendigen Sicherheits- und Vertrauenseigenschaften erbringen müssen.

- 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 **BlockChain** ist nicht per se sicher, kann aber sicher und vertrauenswürdig umgesetzt werden, wenn **alle Aspekte berücksichtigt werden**.



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Wie sicher ist eigentlich die BlockChain?

So sicher wie die Umsetzung der
BlockChain-*Infrastruktur und* ***BlockChain-****Anwendung!*

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

N. Pohlmann: „Eine vertrauenswürdige Zusammenarbeit mit Hilfe der Blockchain-Technologie“, Buch: „Cybersecurity Best Practices - Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden“, Herausgeber: M. Bartsch, S. Frey; Springer Vieweg Verlag, Wiesbaden 2018

N. Pohlmann: „Blockchain-Technologie unter der Lupe – Sicherheit und Vertrauenswürdigkeit kryptografisch verkettete Datenblöcke“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 5/2018
https://norbert-pohlmann.com/app/uploads/2018/10/388-Blockchain-Technologie-unter-der-Lupe-–-Sicherheit-und-Vertrauenswürdigkeit-kryptografisch-verkettete-Datenblöcke-Prof.-Norbert-Pohlmann.pdf