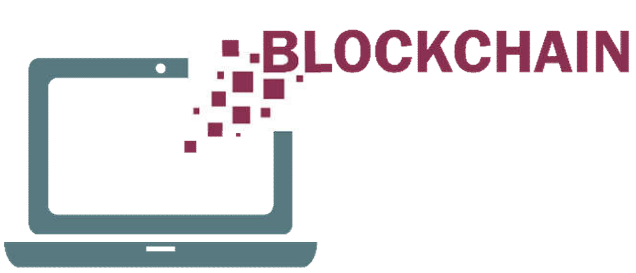
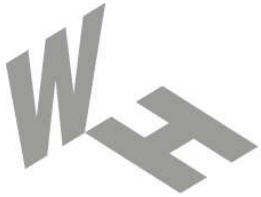




Westfälische Hochschule

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

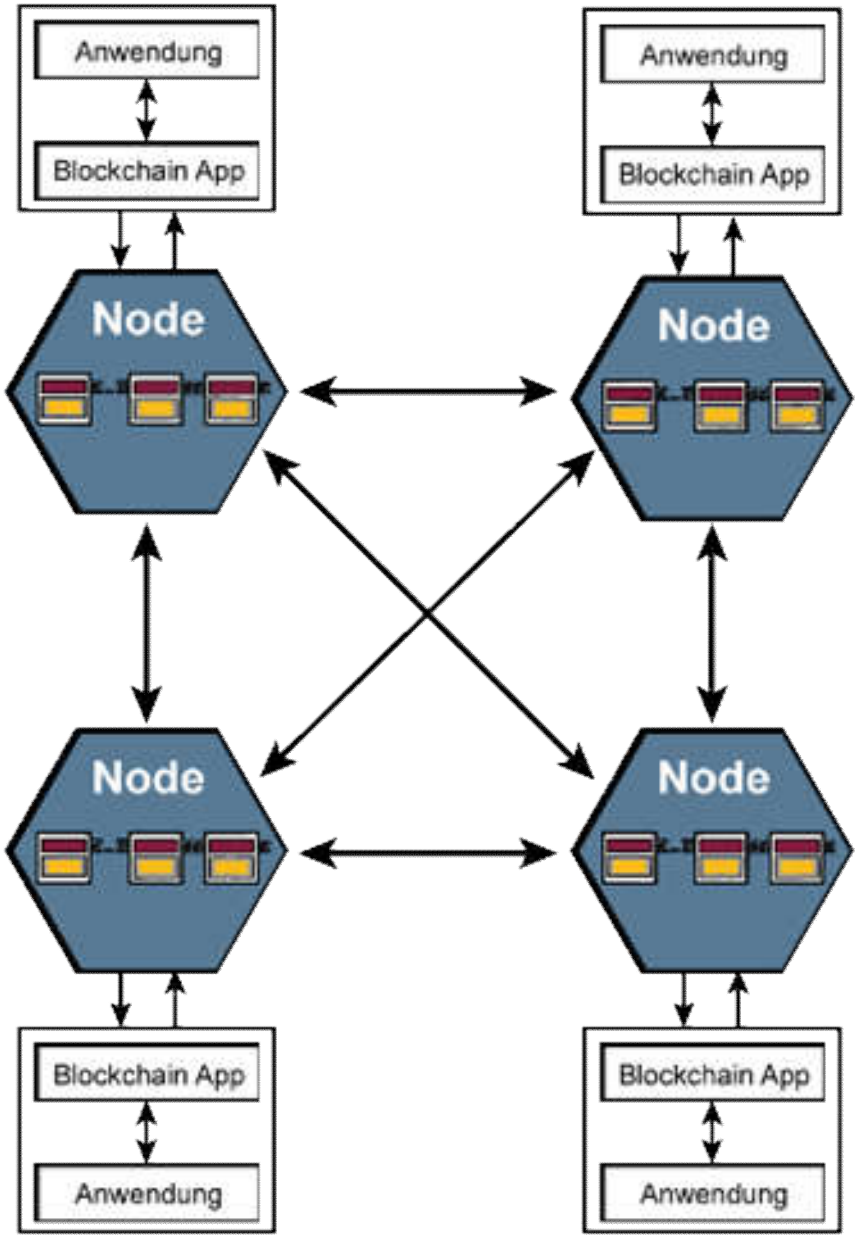
Sicherheit von Blockchain-Anwendungen

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
→ Gewünschte Eigenschaften



- Blockchain ist eine einfache **Datenstruktur**
- Blockchain **redundant** im Netz verteilt
- Daten **manipulationssicher** gespeichert
- **Überprüfbarkeit**:
  - Echtheit
  - Ursprung
  - Unversehrtheit

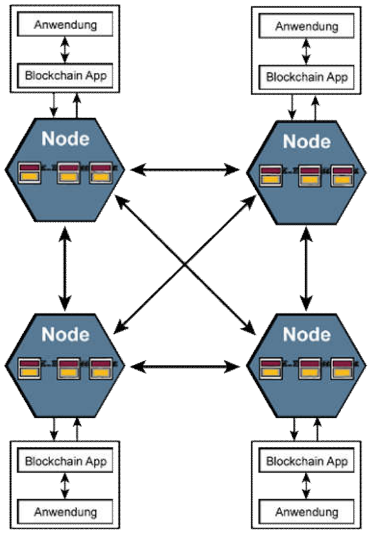
  der gespeichert Daten
- Alle IT-Sicherheitseigenschaften als **Security-by-Design** inhärent in der Blockchain-Technologie eingebunden
- **Automatisierte** vertrauenswürdige **Zusammenarbeit** zwischen verschiedenen Organisationen
- **Eigentumsverhältnisse** (digital Assets) vertrauenswürdig verwalten und übertragen

BlockChain-Technologie
→ Weitere Eigenschaften

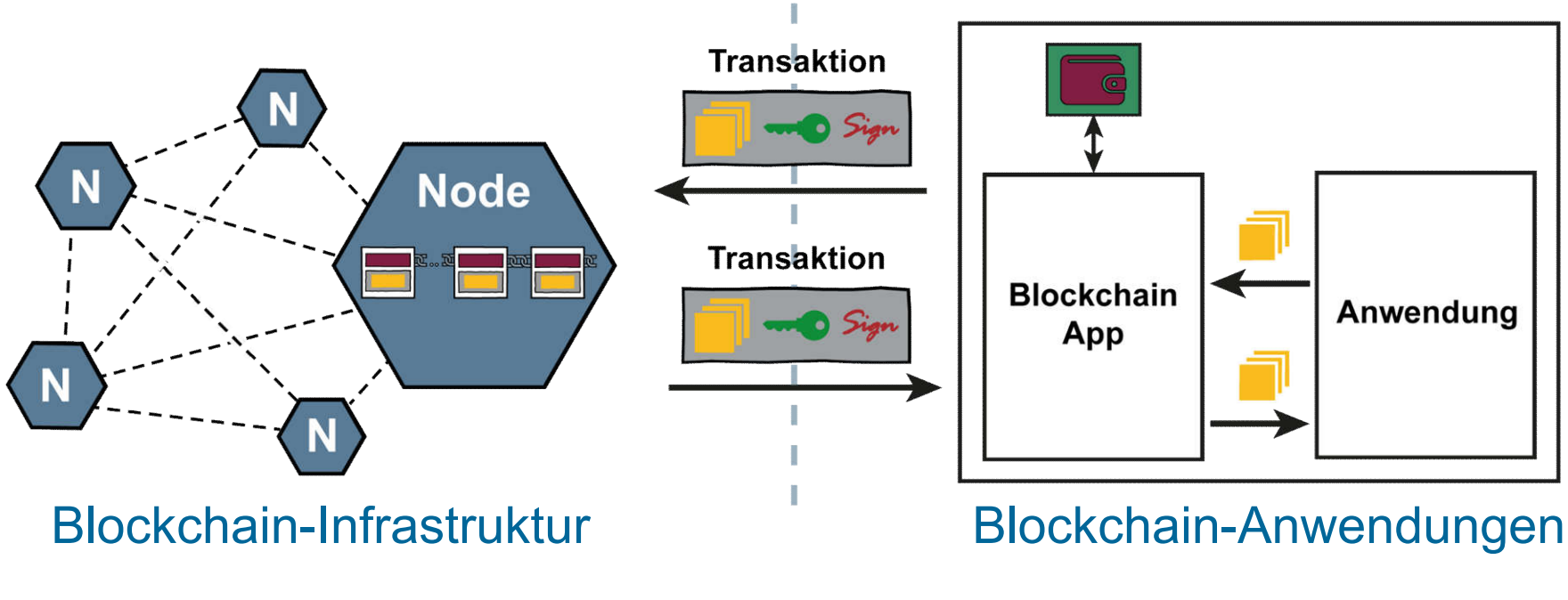
- **Prinzipielle Pseudonymität**
  (Blockchain-Adressen … *Übergänge, Darstellung, Inhalte,* …)

- **Besitz der Wallet**
  (wer die Wallet besitzt kann die Transaktionen für die entsprechenden Blockchain-Adresse erstellen … *Verifizierung der Identität*)

- **Blockverkettung**
  (Keine Löschung von Transaktionen/Daten, … *ungewünschte Inhalte / Datenschutzanforderungen*)



BlockChain-Technologie
→ Infrastruktur und Anwendung

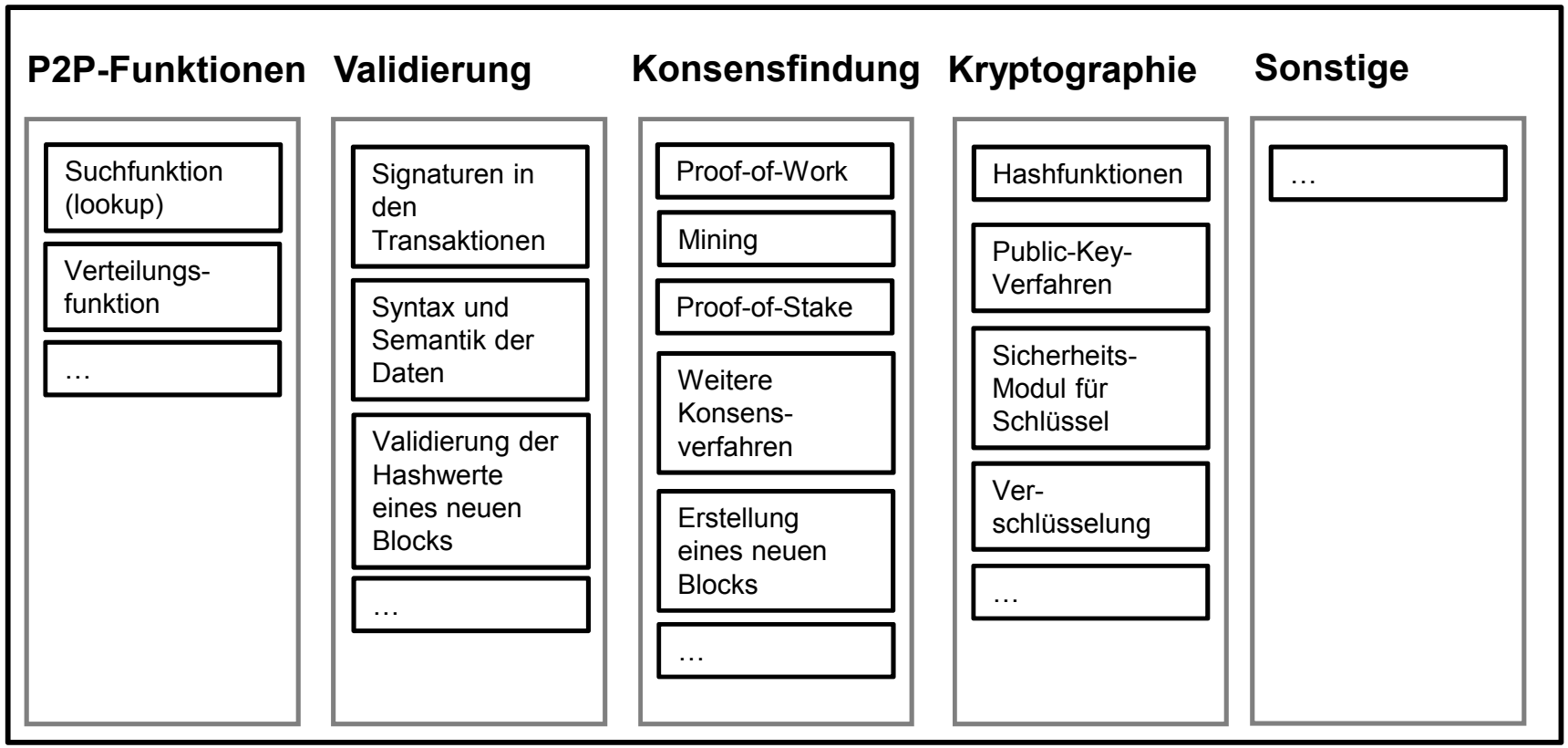


Blockchain-Infrastruktur

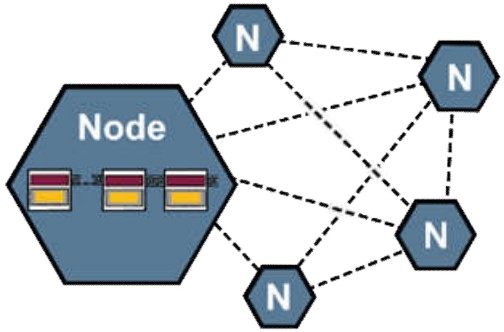
Blockchain-Anwendungen

- **Die Blockchain-Infrastruktur**
  (Peer-to-Peer-Netzwerk, Nodes mit allen Kommunikations- und Sicherheitsfunktionen, die Blockchain als Datenstruktur, …)
- **Die Blockchain-Anwendungen**
  (Blockchain-App, Wallet/Sicherheitsmodul, Anwendung, …)
- Die **Transaktionen** als Schnittstelle dazwischen

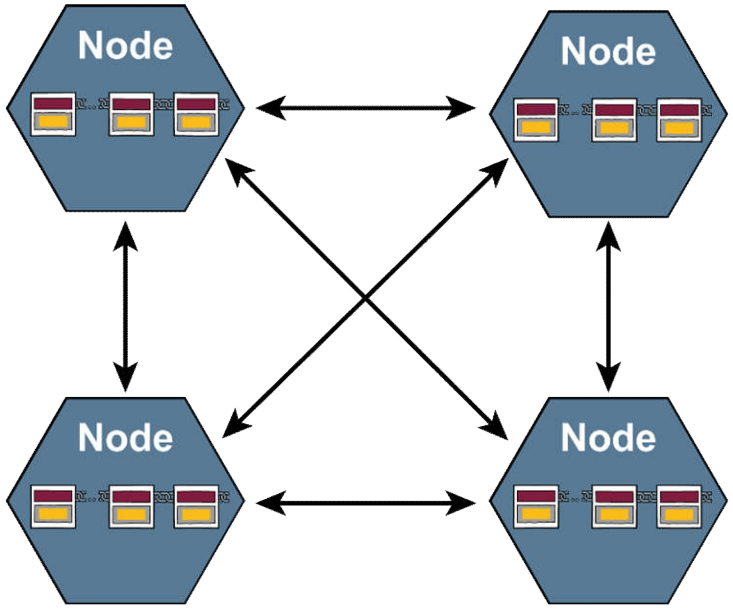
BlockChain-Infrastruktur
→ Funktionen in einer Node



Node



BlockChain-Infrastruktur
→ Eigenschaften: Verteilt und redundant



Robustes Peer-to-Peer-Netzwerk

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

Was sind die richtigen Kriterien, wie können diese überprüft werden?

Statistische Werte: Bitcoin-Blockchain (April 2018)
- ca. 200.000 Transaktionen am Tag
- mehr als 1.000 Nodes
- mehr als 14 Mio. Bitcoin-Konten mit entsprechenden Blockchain-Teilnehmers

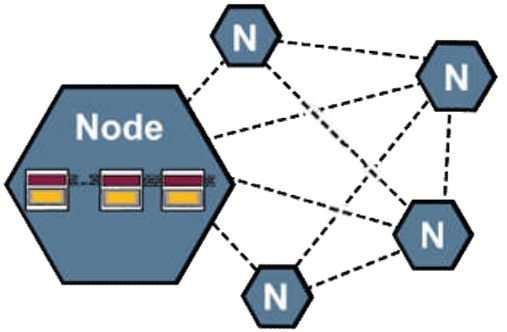
BlockChain-Infrastruktur
→ Kryptographie-Agilität

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

- **Risiko Quantencomputing** (Post-Quantum-Kryptoverfahren)

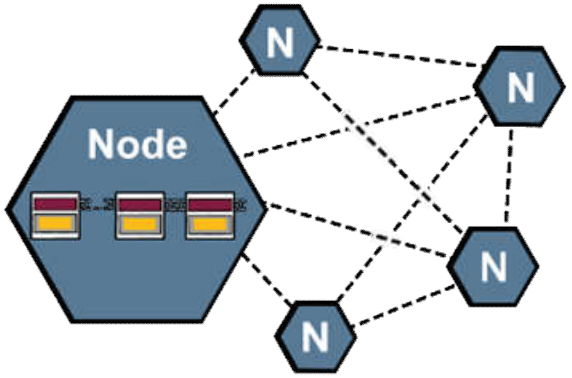
- **Lebensdauer der Blockchain / Kryptographie**
  - Wechseln von kryptographischen Verfahren (z.B. alle 10 Jahre Organisation eines Hard Fork)

Wie kann ein Hard Fork geplant und erfolgreich umgesetzt werden?
- **private, kleine Blockchain**
- **öffentliche, große Blockchain**



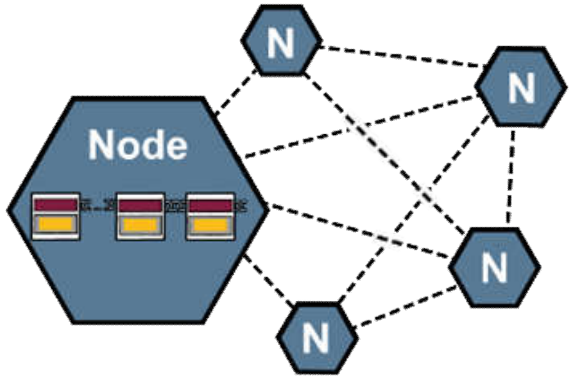
BlockChain-Infrastruktur
→ Vertrauenswürdigkeitsmechanismen

- **Verteilte Konsensfindungsverfahren** (Proof-of-Work, Proof-of-Stake)
  - Double Spending (Proof-of-Work)
  - Vertrauen (Proof-of-Stake)
  - Practical Byzantine Fault Tolerance
  - …
- **Verteilter Validierungsalgorithmus**
  - Echtheit der Transaktionen (Überprüfung der Hashwerte/Signatur)
  - Syntax, Semantik, …
    → Schutz gegen Fremdnutzung … (Kinderpornographie, …)
- **Berechtigungsarchitektur**
  - Zugriff, Validierung, …
  - privat, öffentlich, …
  - **Was ist die beste Berechtigungsarchitektur für welches Problem?**
  - …



BlockChain-Infrastruktur
→ Sicherheit/Zuverlässigkeit: Software

- **Zertifizierung der Software?**
  - Peer-to-Peer-Mechanismen
  - Vertrauenswürdigkeitsmechanismen
  - Kryptographie
  - Smart-Contract-Umsetzung
  - …



- **Entwicklerkonsortien**
  (Auswahl, Mitarbeit, Finanzen, …)

- **Souveränität der Blockchain-Technologie**
  - **Eigene Technologie in DE / der EU?**
  - **Gemeinsame Blockchain?**

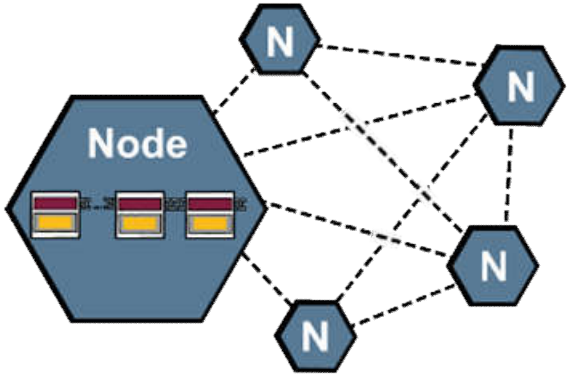
- **Updates**

- …

BlockChain-Infrastruktur
→ Verschlüsselung der Daten

- **Notwendigkeit**
  - EU Datenschutzgrundverordnung
    - Welche Anforderung werden mit Verschlüsselung gelöst?
    - **Löschen des Schlüssel → wie Löschen der Daten?**
    - …
  - Vertraulichkeit von weiteren Inhalten (Patente, Preislisten, …)

- **Konzepte**
  - Transaktionsinhalte
  - Größere Inhalte in einem Verschlüsselungsserver
    - nur zentraler Dienst
    - alle Node
  - Key-Konzept
  - Berechtigungskonzept
  - …

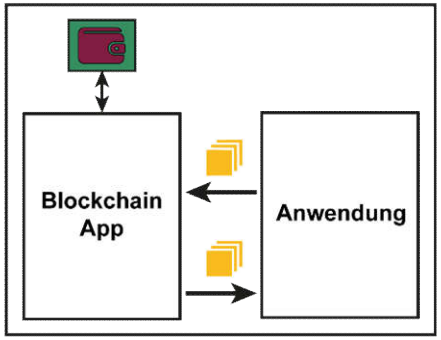


BlockChain-Anwendung
→ Übersicht

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

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

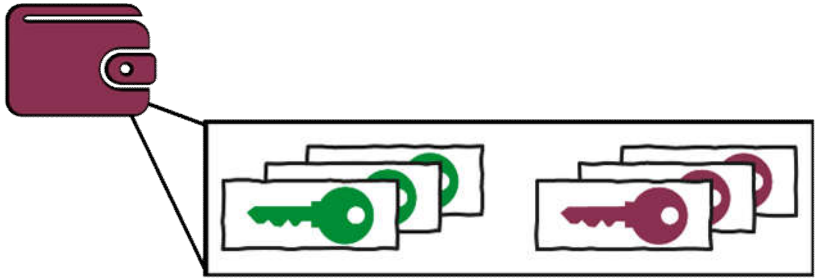
- **Anwendung**
  - Anwendung nutzt die Blockchain-Technologie



Teilnehmer

BlockChain-Anwendung
→ Sicherheit der Schlüssel

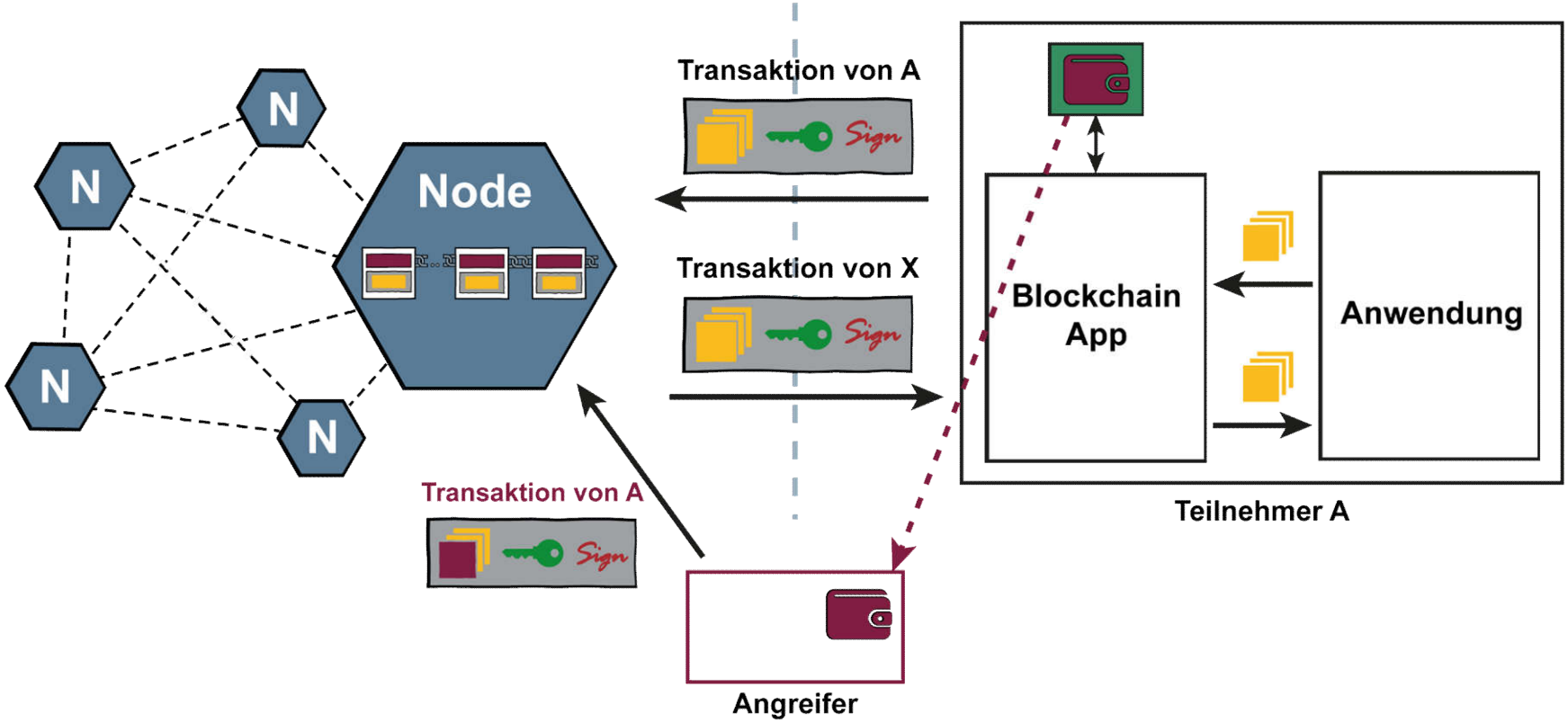
- Die Sicherheit der **BlockChain**-Technologie hängt auch von der **Geheimhaltung der privaten Schlüssel** der Public-Key-Verfahren ab (Wallet).



- **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***

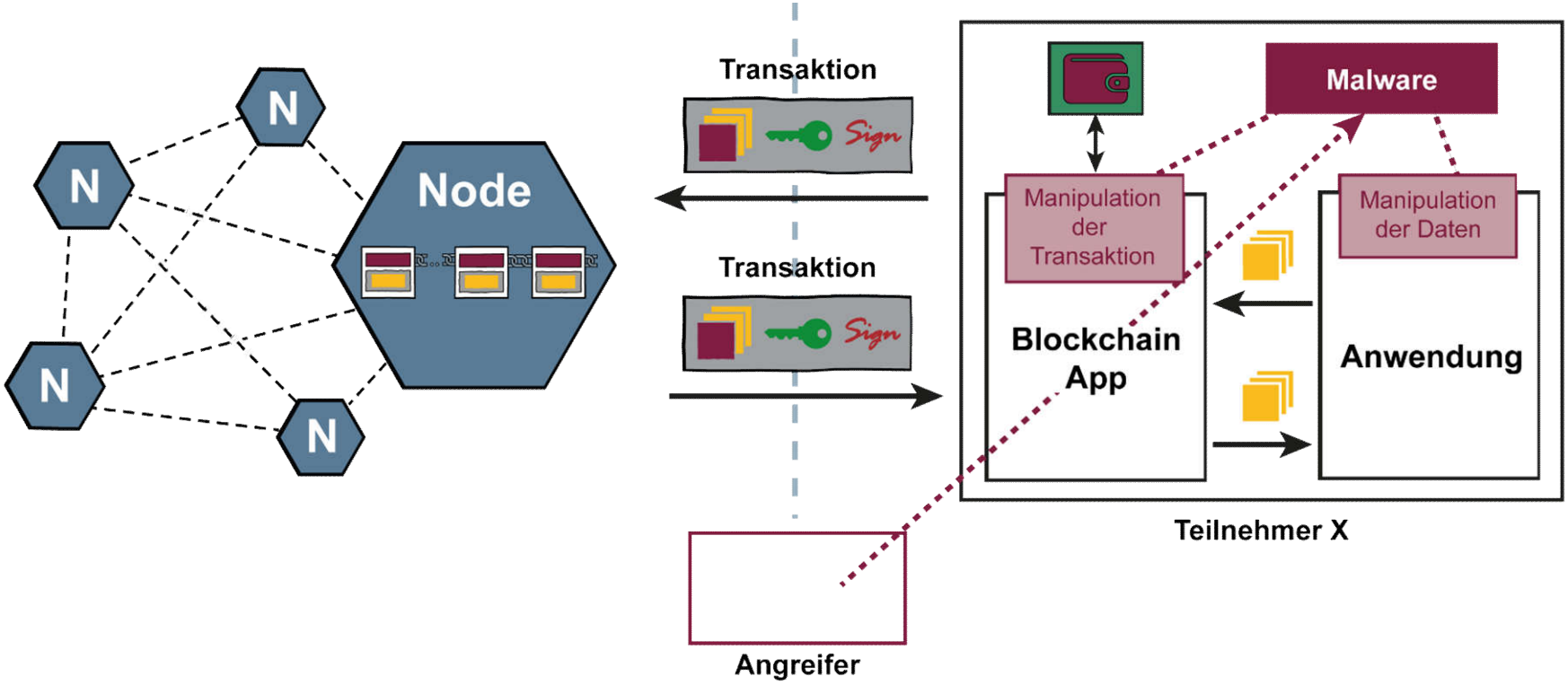
- Der Schutz des **privaten Schlüssels** sollte mit Hilfe von **Hardware-Security-Module** realisiert werden (Smartcards, Sec-Token, High-Level-Sicherheitsmodule) und **unberechtigte Nutzung muss aktiv verhindert werden**!

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

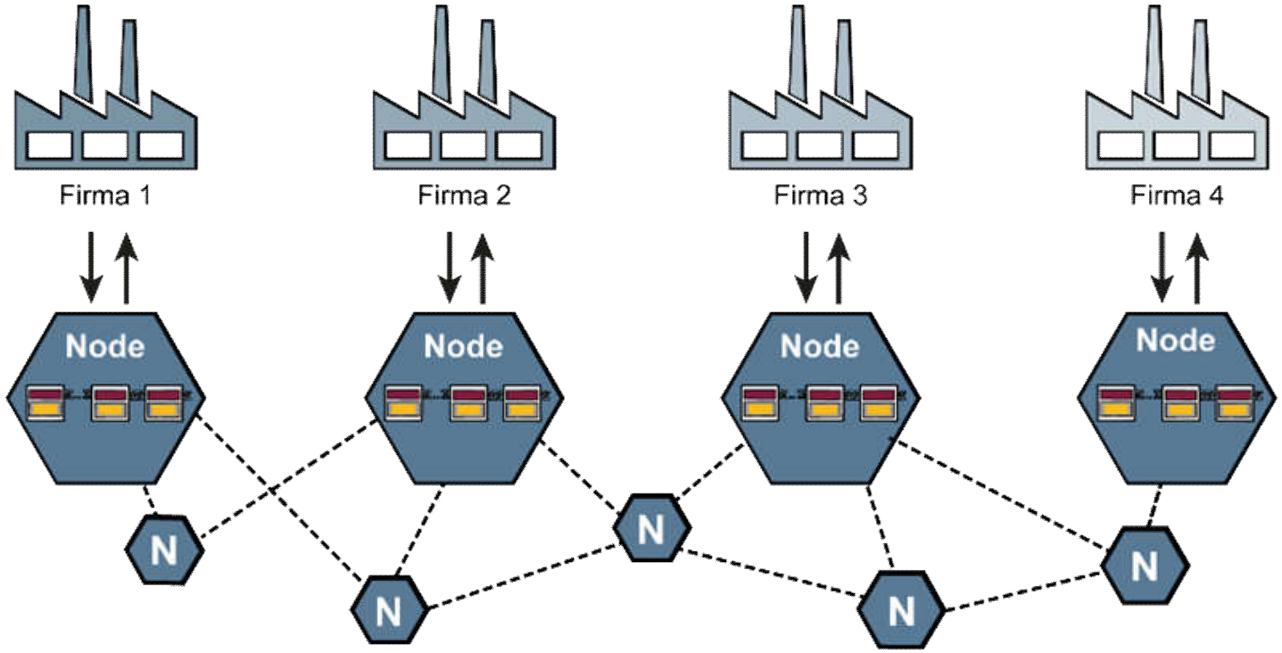


- Der Angreifer „betreibt“ auf dem IT-System des Teilnehmers X eine **Malware**
  - Damit kann der Angreifer die Daten der Blockchain-Anwendung manipulieren
  - Sowohl ausgehende und eingehende Transaktionen
  - Die Transaktionen sind im Blockchain sicher gespeichert

BlockChain-Anwendung
→ Vertrauenswürdig Laufzeitumgebung

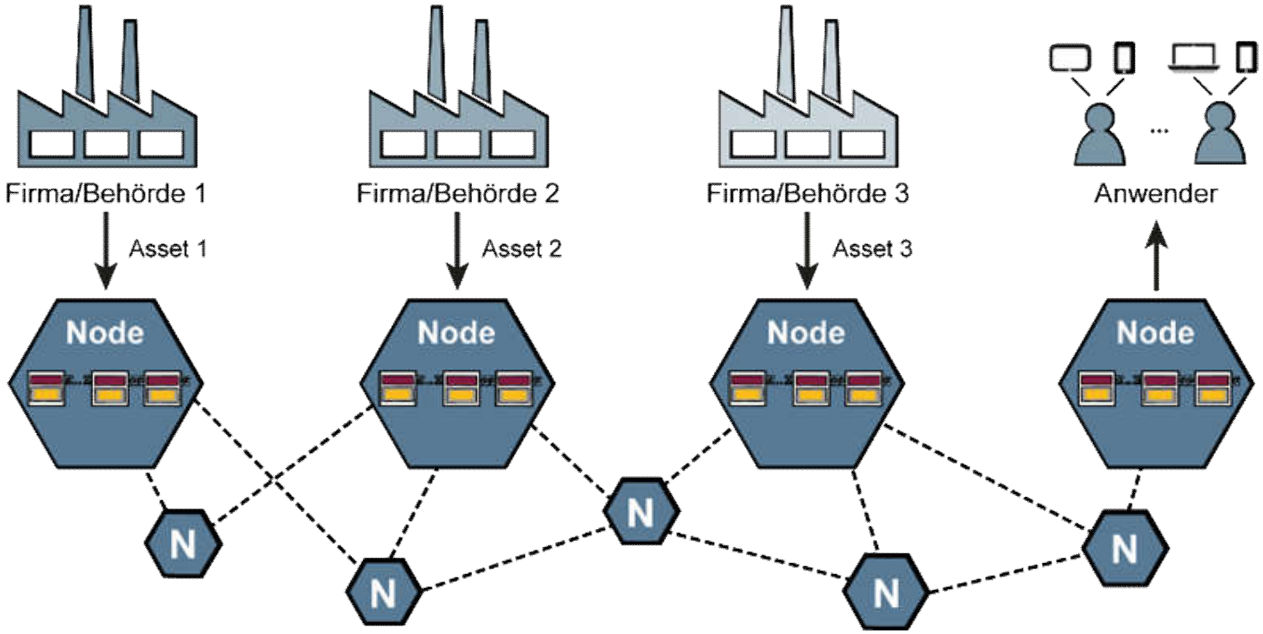
- Wie kann die **Wallet angemessen geschützt** werden?
  - Hardwaresicherheitsmodul
  - Verhinderung der unberechtigten Nutzung
  - …
- Wie kann ein **Malware-Angriff verhindert** werden?
  - Trusted Computing
  - Sandboxing
  - …

BlockChain-Technologie
→ Recht (Sichtweise Informatiker) – 1/2



- **Privatrechtlicher Vertrag**
  - Automatisierte Zusammenarbeit (Smart Contract)
  - Private Blockchain – Permissionless / Permissioned
  - Haftung? – max. Schadensumme von 100.000 Euro
  - Welche Risiken können/müssen vertraglich geregelt werden und welche nicht?
  - …

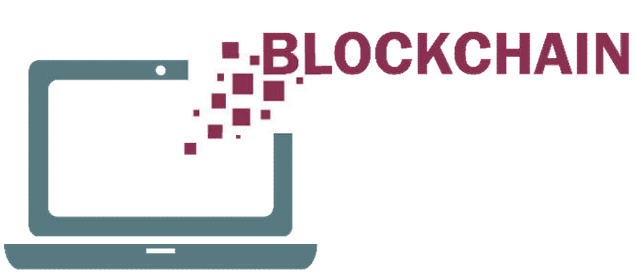
BlockChain-Technologie
→ Recht (Sichtweise Informatiker) – 2/2



- **AGBs**
  - Verwalten und Übertragen von Eigentumsverhältnissen (digital Assets)
  - Öffentliche Blockchain – Permissionless / Permissioned
  - Haftung? Was ist sinnvoll, was nicht?
  - Welche Risiken können/müssen vertraglich geregelt werden und welche nicht?
  - …

BlockChain-Technologie
→ Was können wir gemeinsam tun?

- Welche technischen Konzepte sind sinnvoll?
- Welche Vorgehensweisen sollten Standard werden?
- Welche Sichtweisen helfen, mehr Zuversicht für weitere Anwendungen zu motivieren?
- Für welche Probleme brauchen wir gemeinsame Lösungen?
- Welche Richtlinien helfen, Herausforderungen zu lösen?
- …



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Sicherheit von Blockchain-Anwendungen

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