



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Blockchain-Technologie und - Sicherheit

- Vorlesung Cyber-Sicherheit -

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 und -Sicherheit

→ Inhalt

- **Ziele und Ergebnisse der Vorlesung**
- **Übersicht**
- **Anwendungssicherheit**
- **Blockchain Beispielanwendungen**
- **Zusammenfassung**

- **Ziele und Ergebnisse der Vorlesung**
- Übersicht
- Anwendungssicherheit
- Blockchain Beispielanwendungen
- Zusammenfassung

Ziele und Ergebnisse der Vorlesung

→ Blockchain-Technologie und -Sicherheit

- Gutes Verständnis für die **Sicherheitseigenschaften** der Blockchain-Technologie.
- Erlangen der Kenntnisse über die zentrale **Datenstruktur**, die **Konsensfindung** in der Blockchain und mögliche **Angriffsszenarien**.
- Gewinnen von praktischen Erfahrungen durch Betrachtung von konkreten **Beispielanwendungen**.

Blockchain-Technologie und -Sicherheit

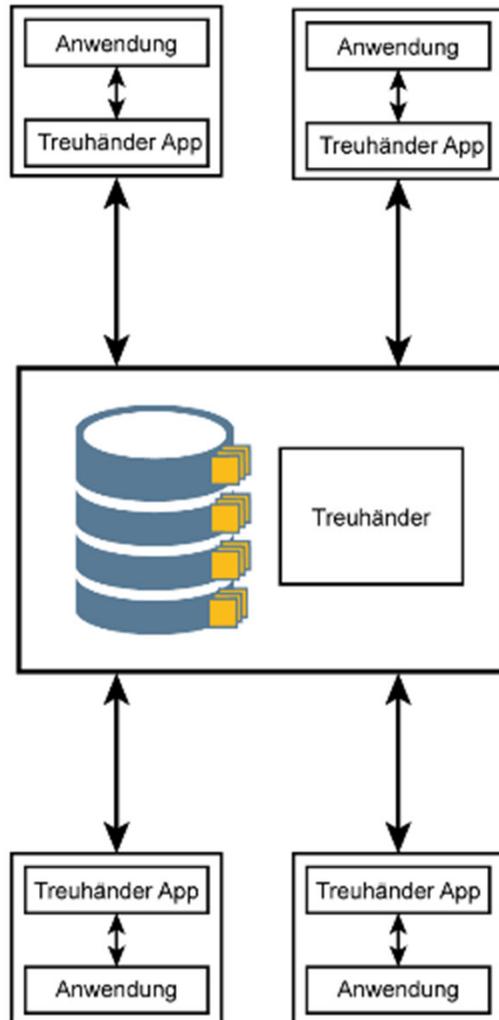
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- **Übersicht**
- Anwendungssicherheit
- Blockchain Beispielanwendungen
- Zusammenfassung

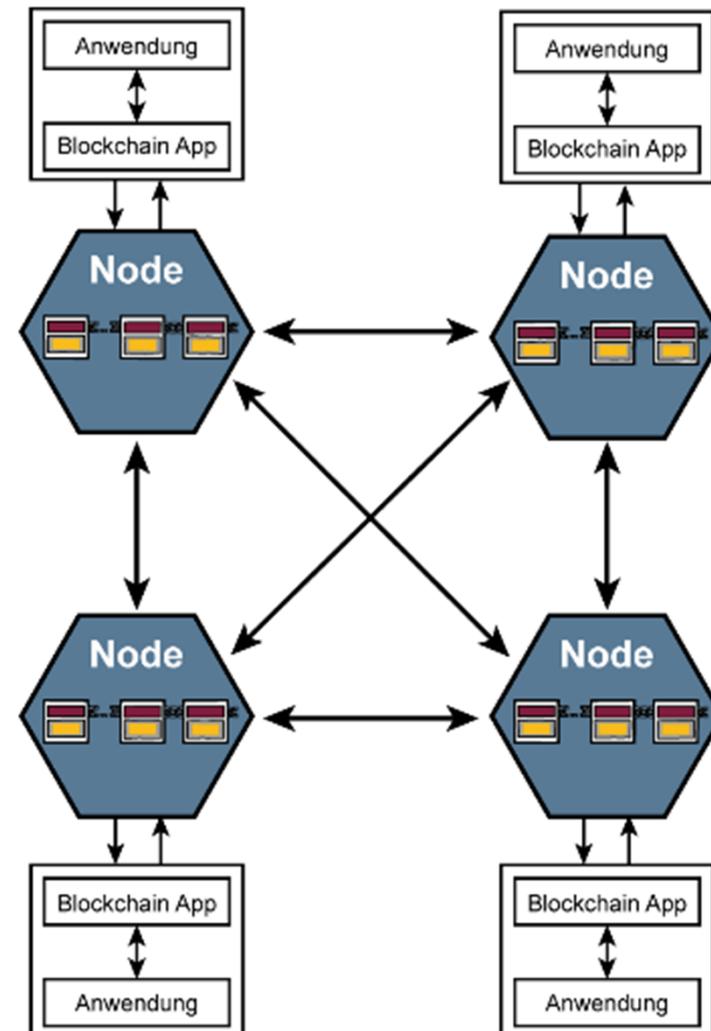
BlockChain-Technologie

→ auf den Punkt gebracht

Transaktionsspeicher



Zentrale Architektur



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-Technologie

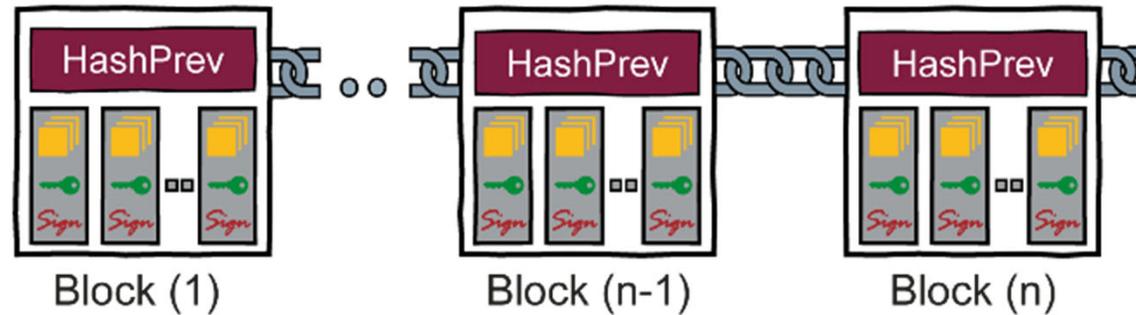
→ Das „Internet der Werte“

- **BlockChain -Technologie**
 - Lassen sich **Eigentumsverhältnisse** (digital Assets)
 - **direkter** und **effizienter** als bislang **sichern** und **regeln**,
 - da eine **lückenlose** und **unveränderliche Datenaufzeichnung** hierfür die Grundlage schafft.
 - Alle **Beglaubigungsprozesse** werden *schneller*, sicherer und *billiger*.

BlockChain → „Internet der Werte“

BlockChain-Technology

→ Sicherheitseigenschaften



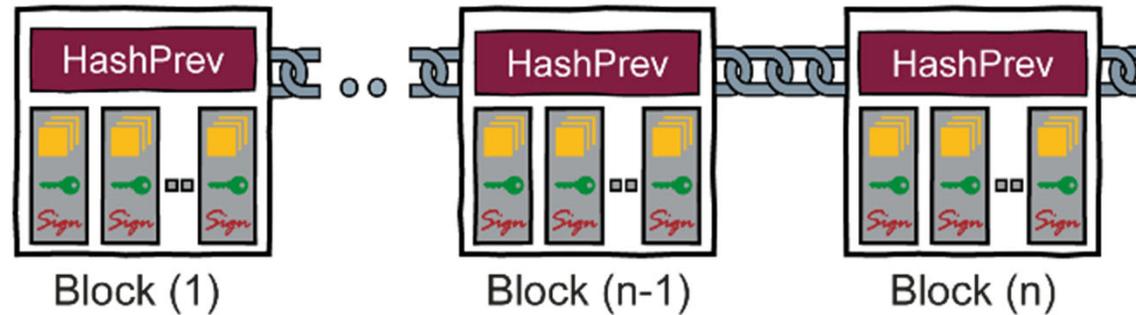
BlockChain

- ist eine **fälschungssichere**, *kryptographische Verfahren (Hashfunktionen / Public-Key-Verfahren)*
- **verteilte, redundante** Datenstruktur *Vielzahl von Teilnehmern gespeichert (jede Note hat die Blockchain gespeichert)*
- in der Transaktionen **in der Zeitfolge protokolliert** *Art der Verkettung (HashPrev)*
- **nachvollziehbar, unveränderlich** und *jeder kann Kryptographie überprüfen (Hashwert, Signatur)*
- **ohne zentrale Instanz** abgebildet sind. *geeignete Konsensfindungsverfahren (Proof of Work, Proof of Stake)*

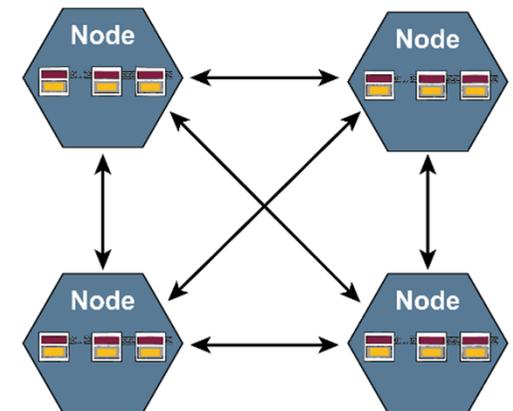
(*Sicherheitseigenschaften einer BlockChain*)

BlockChain-Technology

→ Datenstruktur einer BlockChain



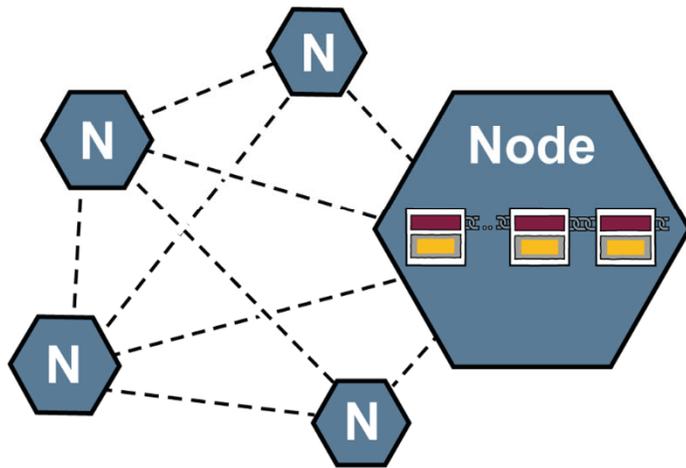
- Die **Daten** sind Transaktionsdaten mit Geldeinheiten, Zertifikaten, Produktionsdaten, Sensordaten, Source Code, ... digitale Werte
- Transaktionen mit **Daten** werden vom Teilnehmer erstellt und **signiert** (Wallet/Schlüssel). Passende **Public Key** in der Transaktion. Verteilung
- **Block** beinhaltet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



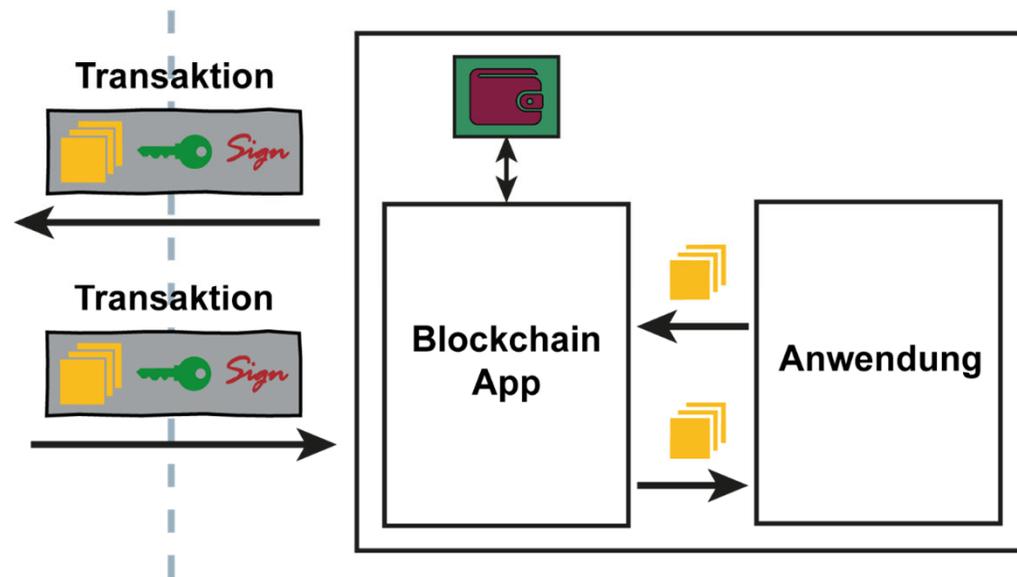
BlockChain-Technologie

→ Infrastruktur und Anwendung

BlockChain-Infrastruktur



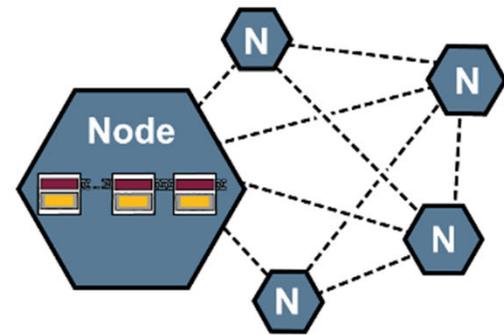
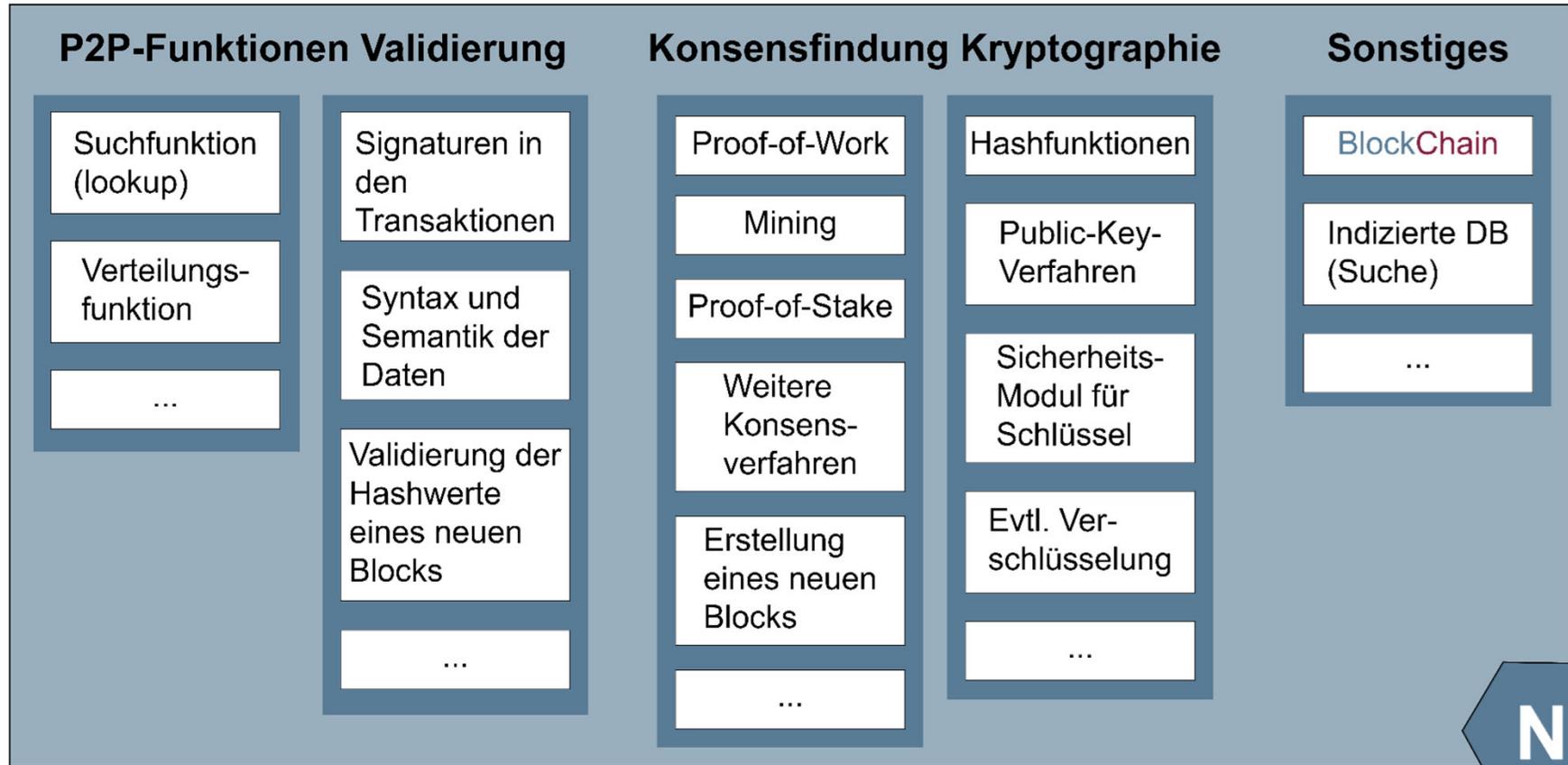
BlockChain-Anwendungen



- 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

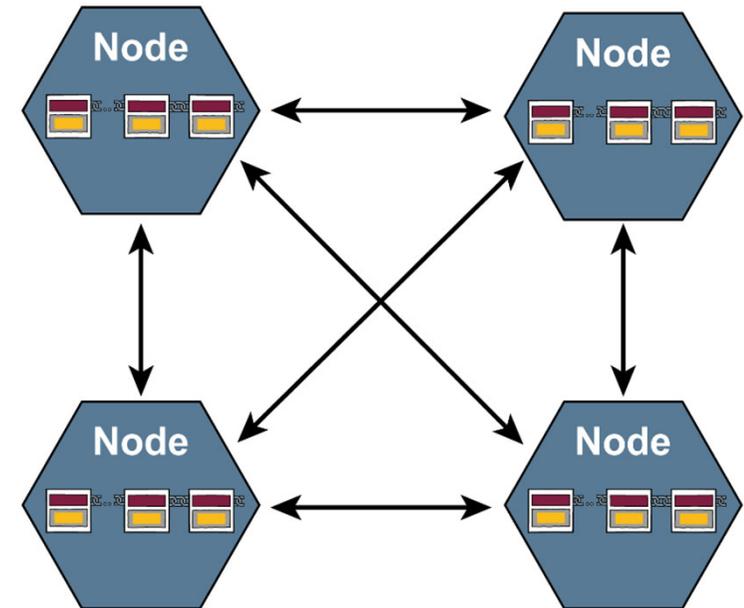


BlockChain-Infrastruktur

→ Eigenschaften: verteilt und redundant

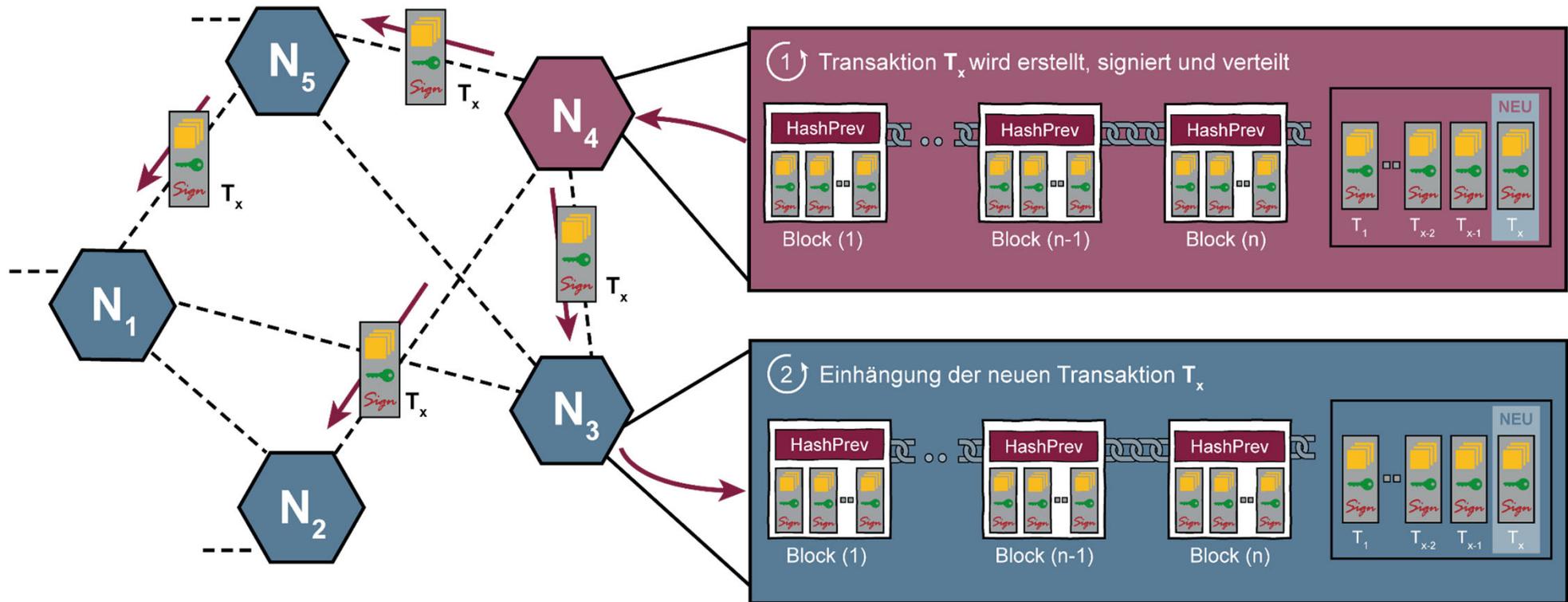
Robustes Peer-to-Peer-Netzwerk

- **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

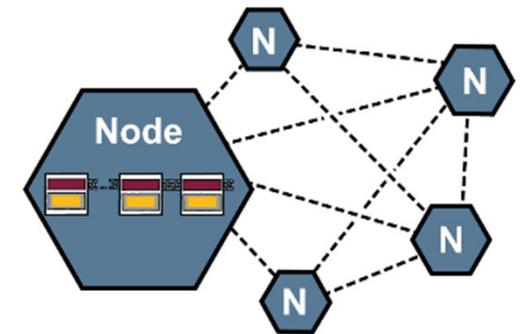
→ Versendung von Transaktionen



BlockChain-Infrastruktur

→ **Eigenschaften: fälschungssicher/unveränderlich**

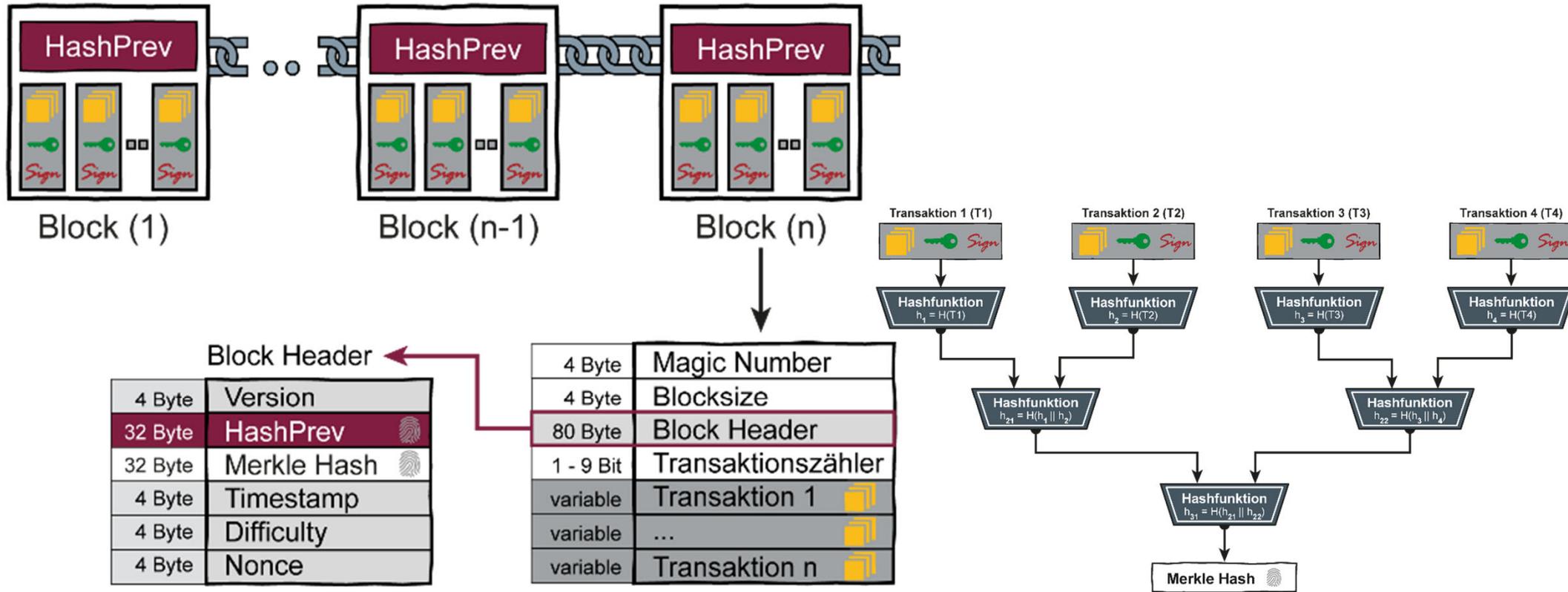
- **Kryptographie-Agilität**
- **Stand der Technik** (Technische Richtlinie: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“)
 - **Public-Key-Verfahren** (Signierung / Verifizierung von Transaktionen)
→ (RSA - 3.000 bit)
 - **Hashfunktionen** (Adresserzeugung, HashPrev, Merkle Hash)
→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

Cleverer Nutzung von Hashfunktionen



$$\text{HashPrev}_n = H(\text{Block-Header}_{n-1})$$

Daten in der BlockChain können nicht gelöscht werden!

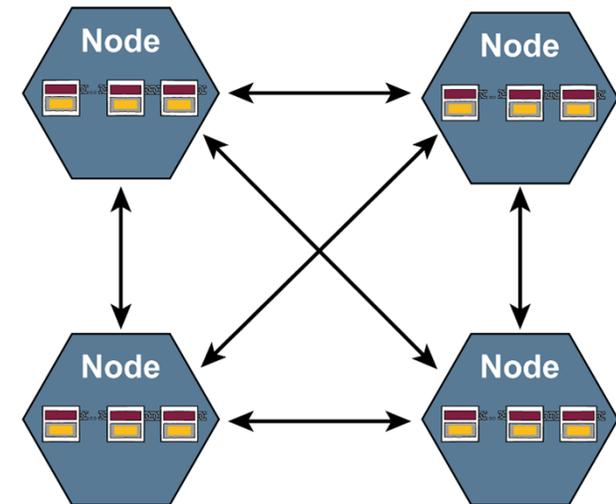
BlockChain-Infrastruktur

→ Eigenschaft: ohne zentrale Instanz (1)

- 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)



BlockChain-Infrastruktur

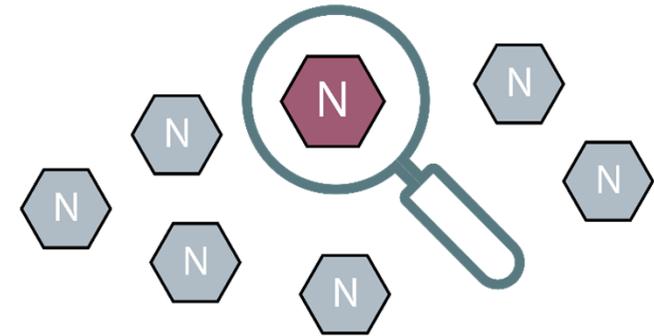
→ Eigenschaft: ohne zentrale Instanz (2)

- **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

→ Konsensfindungsverfahren

- Das Konsensfindungsverfahren hat die Aufgabe, eine **Node auszuwählen**, die einen Block in die **BlockChain** hinzufügen soll.
- Es gibt unterschiedliche Methoden
 - **Proof of Work (PoW)** → „Miner“
 - Aktuelle gebräuchlichste Methode, z.B. bei Bitcoin
 - Lösung eines mathematischen Problems → alle gleichberechtigt (siehe nächste Folie)
 - **Proof of Stake (PoS)**
 - Es werden Nodes gewählt, die nachweislich ein großes Interesse an einer stabilen und sicheren **BlockChain** (sehr viele **Transaktionen**, sehr viele Coins, ...)
 - **Alternativen**
 - „Byzantinische Fault Tolerance“-Verfahren
 - ...



Mining (Proof of Work)

→ Gewinnen der Challenge

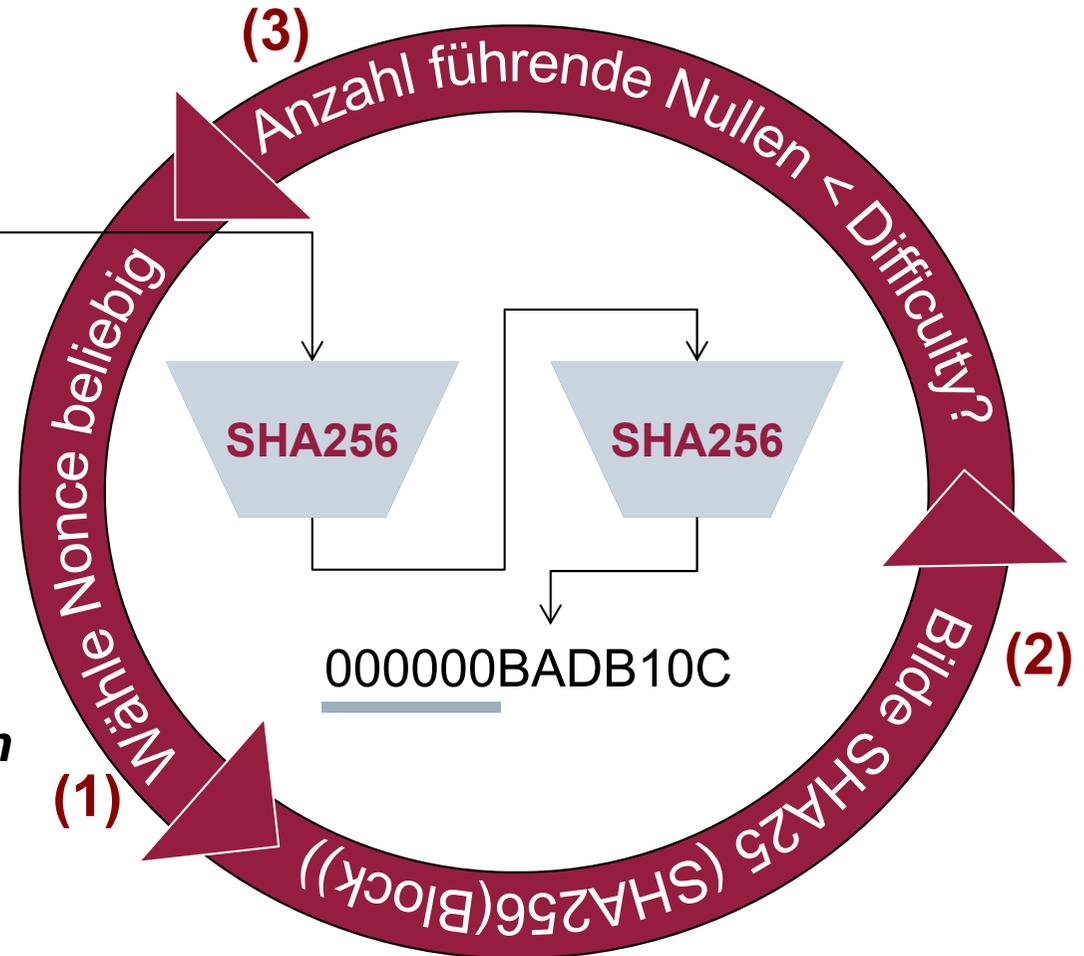
Mining dient als „Proof-of-Work“ und ist bei „Bitcoin“ die einzige Möglichkeit, Bitcoin zu erzeugen.

Block Header

4 Byte	Version
32 Byte	HashPrev
32 Byte	Merkle Root Hash
4 Byte	Timestamp
4 Byte	Difficulty
4 Byte	Nonce

Challenge

Ist die **Anzahl der führenden Nullen** größer oder gleich der **Difficulty**, gilt der Block als geschürft und wird im P2P-Netzwerk verteilt.



Der Miner, der die Challenge als erstes löst, darf den neuen Block mit den neuen **Transaktionen** abschließen und zu der **BlockChain** hinzufügen.

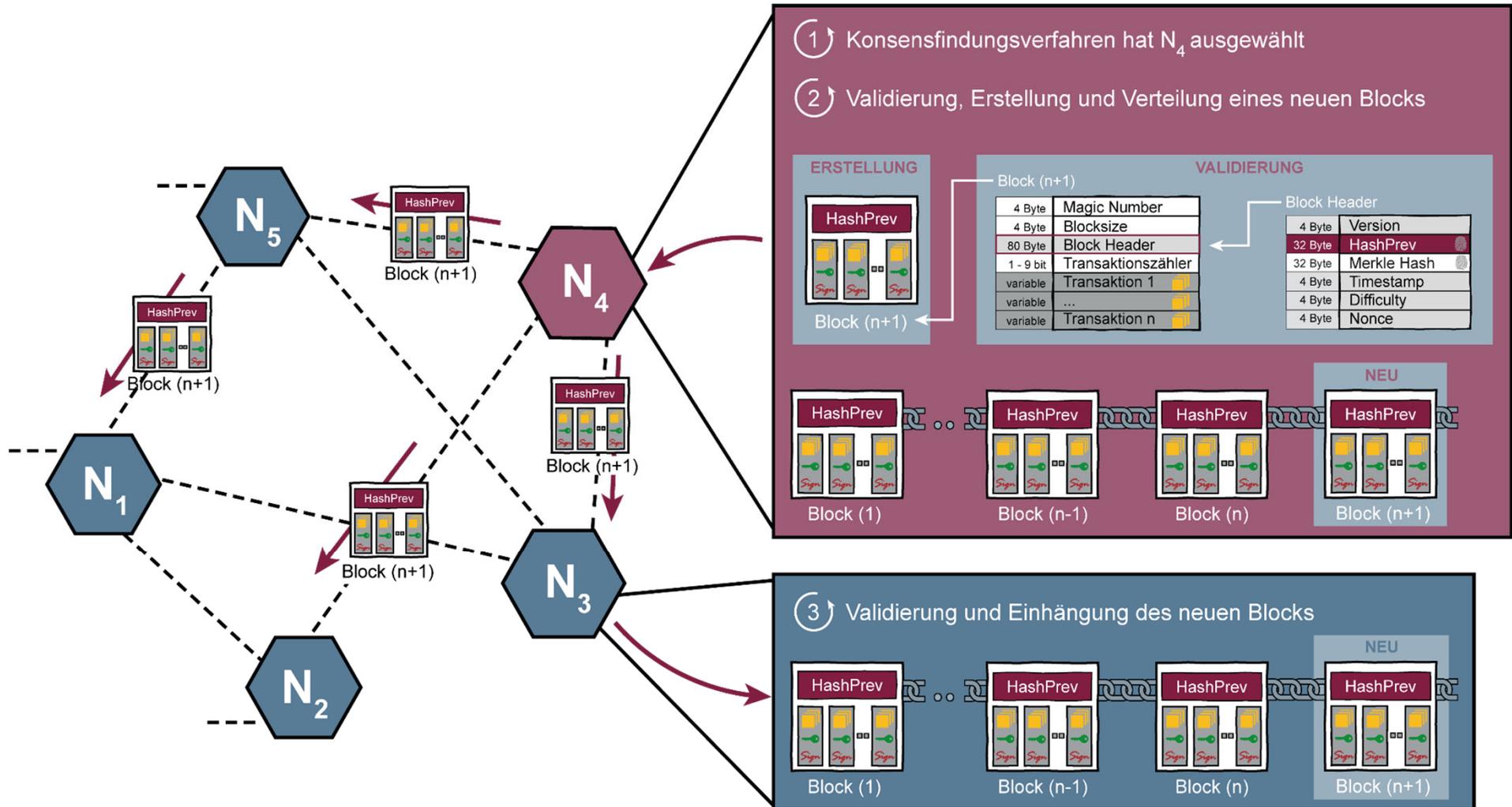
BlockChain-Infrastruktur

→ Bewertung „Mining“

- **Die Challenge kostet sehr viel Energie:**
 - 2,8 Mio. US-Dollar pro Tag (Stromkosten)
 - 1,3 Giga-Watt
 - das sind ca. 10 US-Dollar pro **Transaktion**
- Solange eine **Node nicht die Mehrheit an Miner-Kapazitäten besitzt** (mehr als 51%), ist das Mining-Prinzip robust und nicht zu kompromittieren.
- **Der Zeitauswand der Validierung ist sehr hoch.**
- Der Schwierigkeitsgrad des Minings wird immer so angepasst, dass die Rechenkapazität des gesamten Netzwerkes gerade so groß ist, dass rein statistisch **alle zehn Minuten** ein Miner **eine Lösung** findet.

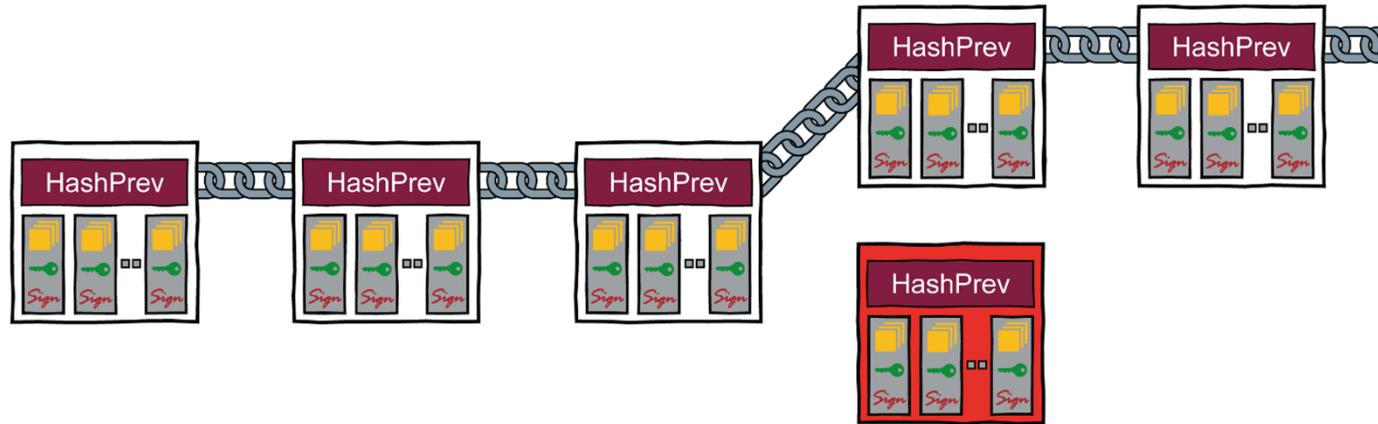
BlockChain-Infrastruktur

→ Validierung von neuen Blöcken

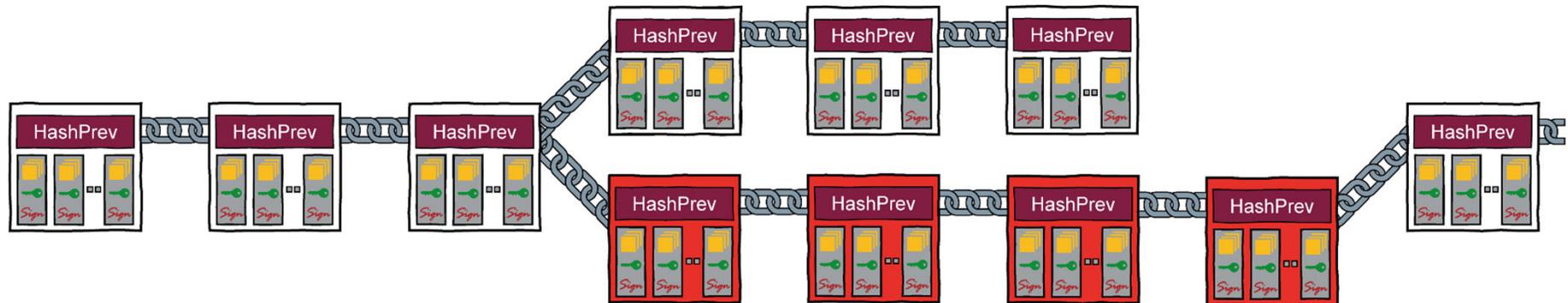


BlockChain-Infrastruktur

→ Angriff auf die Konsensfindung



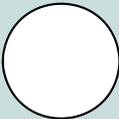
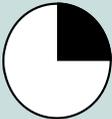
Double Spending



Erfolgreiche Double Spending Attacke

BlockChain-Infrastruktur

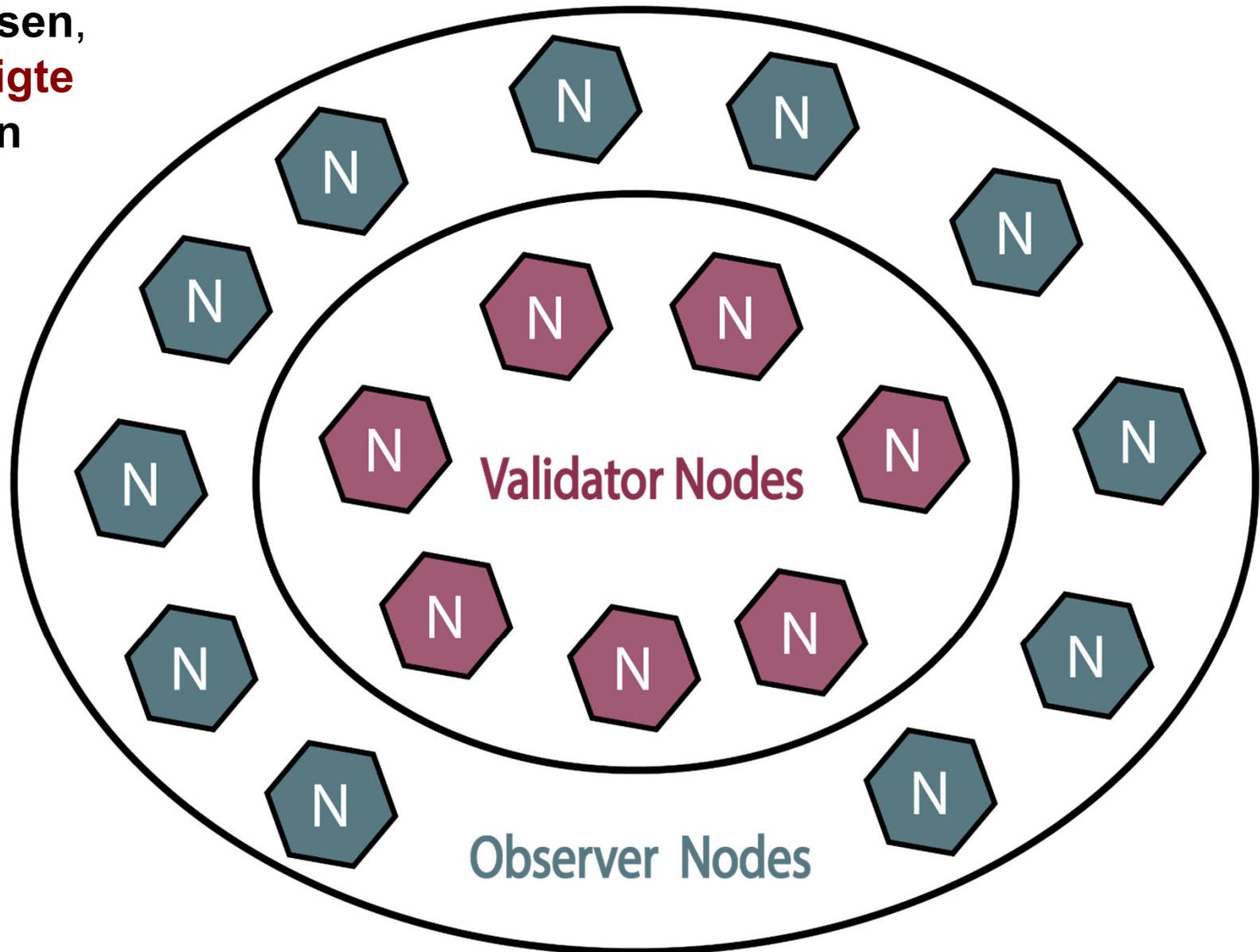
→ Berechtigungsarchitektur

		Validierung	
		Permissionless	Permissioned
Zugriff	Public	<p>„Jeder darf lesen und validieren“</p> 	<p>„Jeder darf lesen, nur Berechtigte validieren“</p> 
	Private	<p>„Nur Berechtigte dürfen lesen und jeder darf validieren“</p> 	<p>„Nur Berechtigte dürfen lesen und validieren“</p> 

BlockChain

→ Moderne Umsetzungsarchitektur

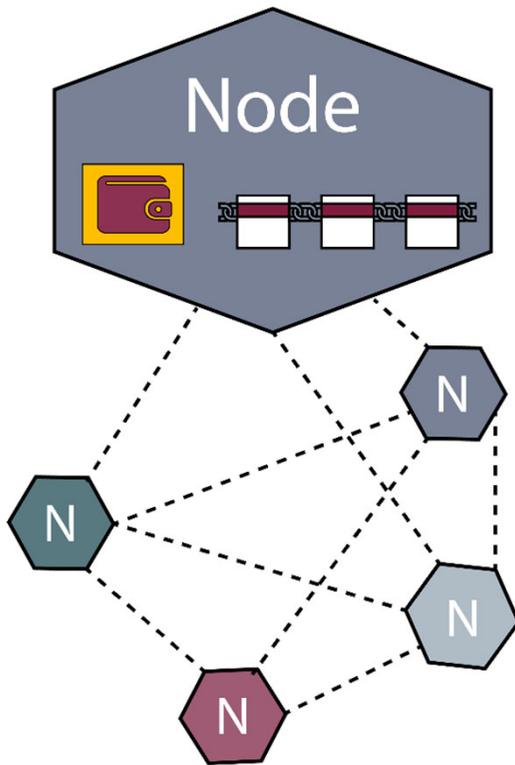
Jeder darf lesen,
nur **Berechtigte**
validieren



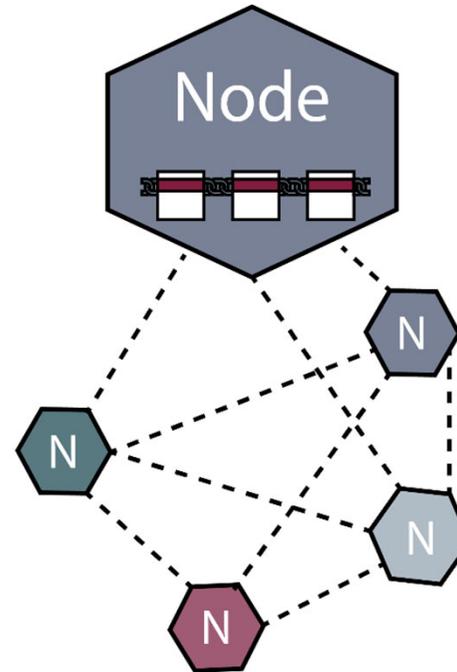
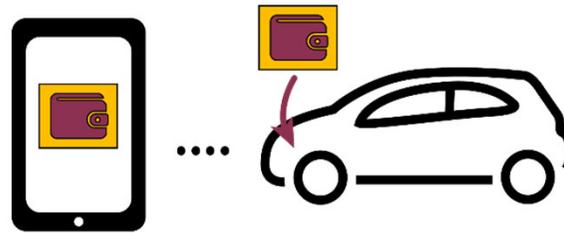
BlockChain

→ Verschiedene Arten von Nodes/Wallets

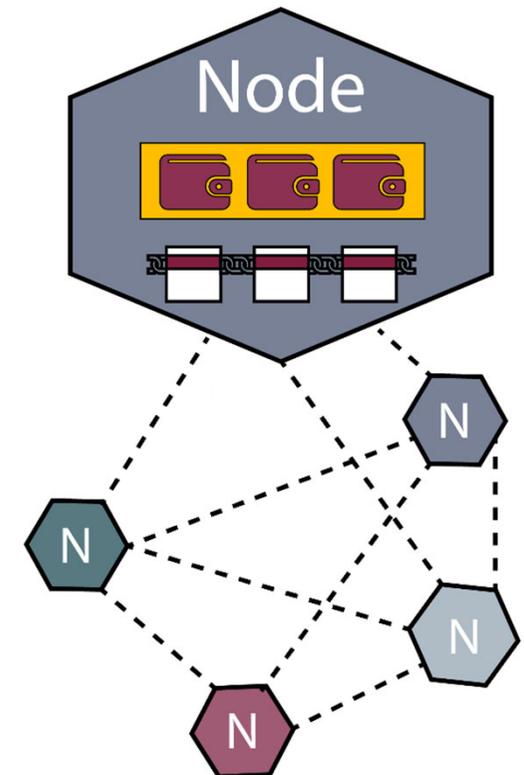
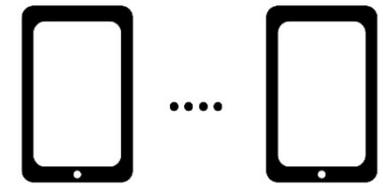
Full Node



Light Node



Service Node



Blockchain-Technologie und -Sicherheit

→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Übersicht
- **Anwendungssicherheit**
- Blockchain Beispielanwendungen
- Zusammenfassung

BlockChain-Anwendungssicherheit

→ Übersicht Anwendung

■ Blockchain-App

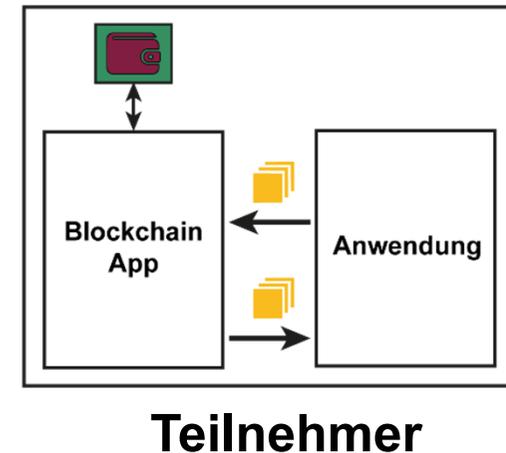
- Daten von der Anwendung werden in Transaktionen vom BlockChain-Teilnehmer (Wallet-Besitzer) signiert und in der BlockChain verstetigt
- Transaktionen werden verifiziert und die Daten von der Anwendung „verarbeitet“

■ Wallet

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

■ Anwendung

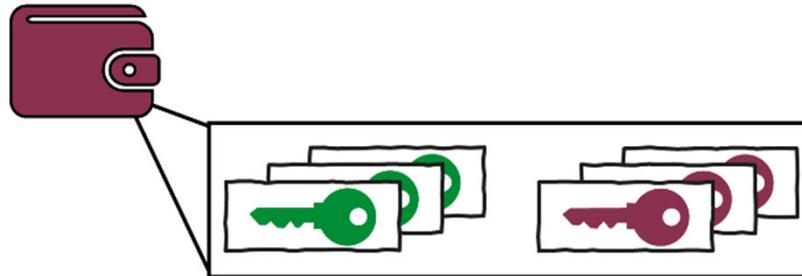
- Die eigentliche Anwendung nutzt die BlockChain-Technologie



BlockChain-Anwendungssicherheit

→ Sicherheit der Schlüssel

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



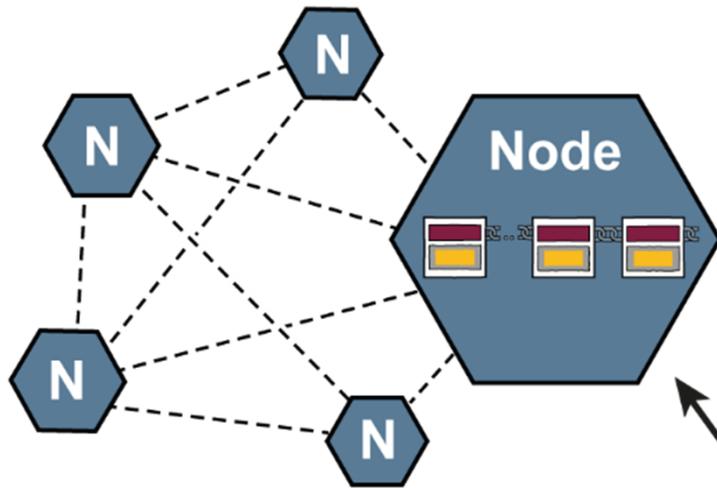
- **Gefahren** bei nicht ausreichendem Schutz des **geheimen Schlüssels**
 - Das **private IT-System / IoT-Gerät** wird **gehackt** (Malware)
 - Die **Website** der Online Wallet (Service Node) wird **gehackt**
 - Ein nicht ausreichend gesichertes **Smartphone** wird **gestohlen** (Light N.)
 - Der **geheimen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



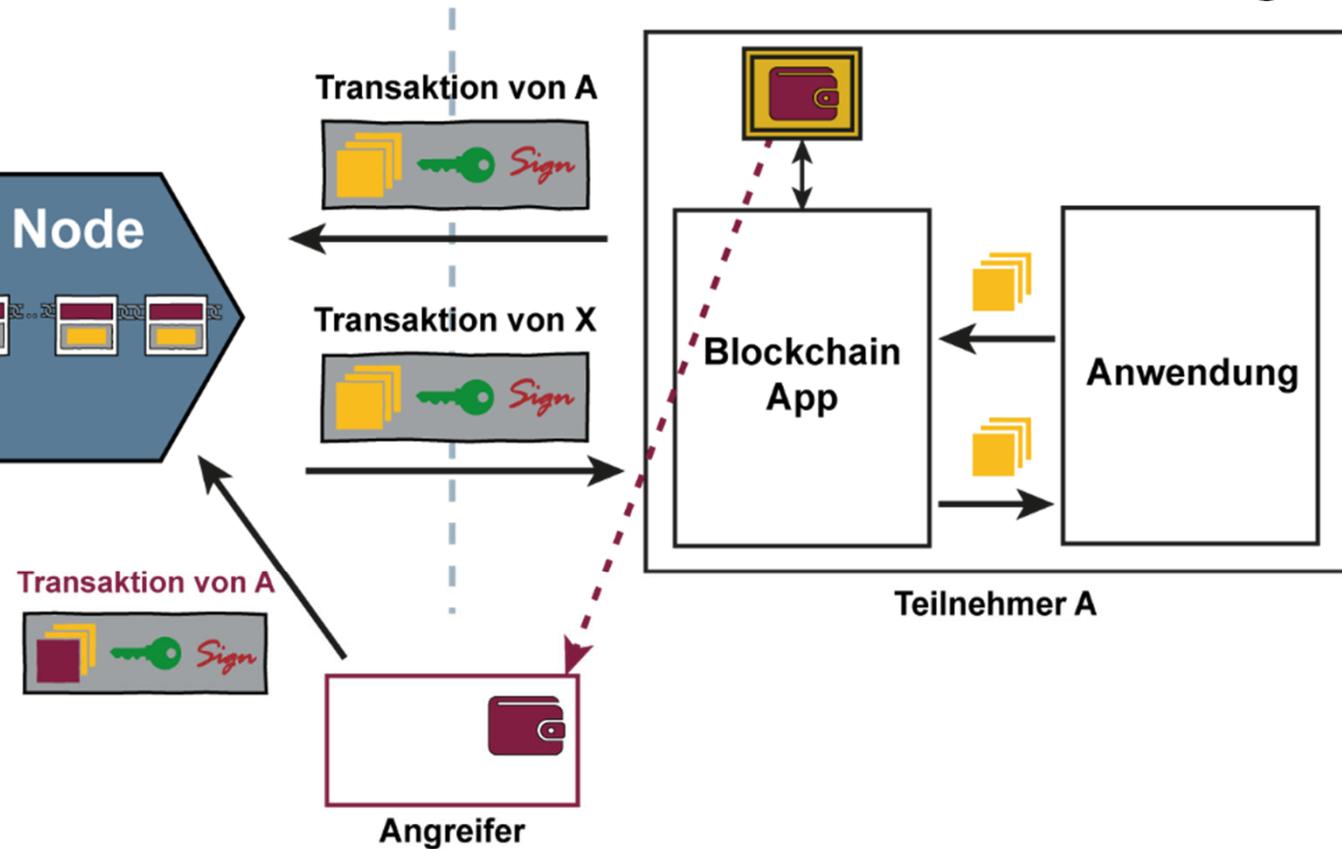
BlockChain-Anwendungssicherheit

→ Manipulationen der Transaktionen

BlockChain-Infrastruktur



BlockChain-Anwendungen

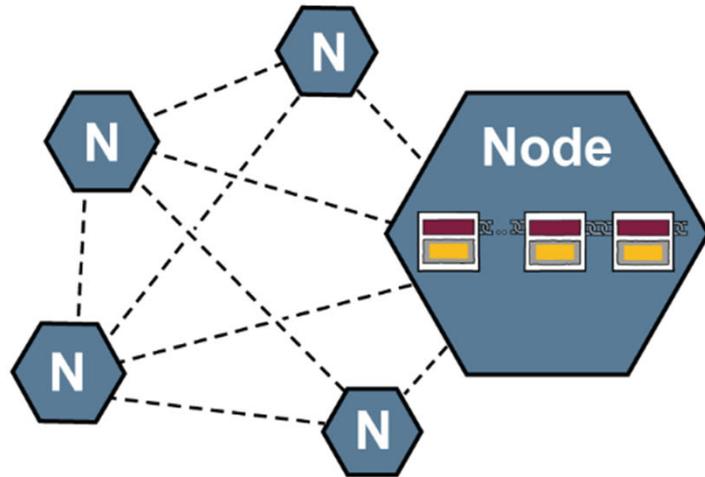


- Der Angreifer „**besitzt**“ die **Wallet/Schlüssel** oder kann sie „**unberechtigt nutzen**“
 - Damit kann er valide Transaktionen für den entsprechenden Teilnehmer A erstellen und die **BlockChain-Anwendung** manipulieren

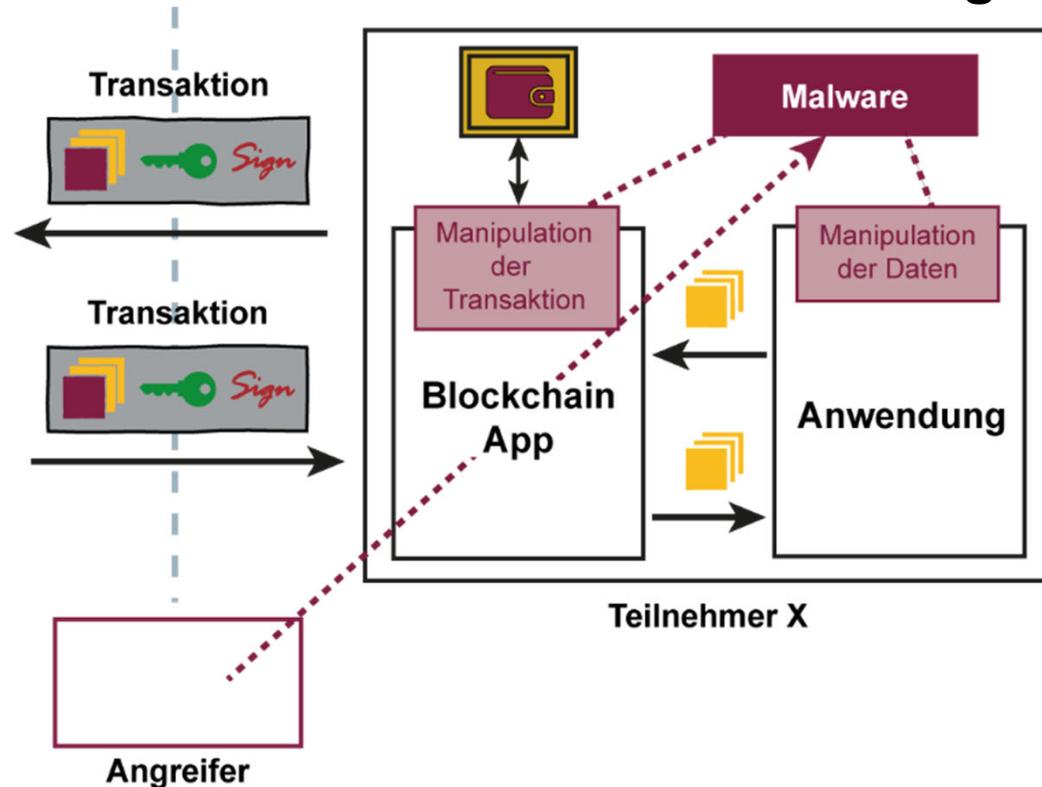
BlockChain-Anwendungssicherheit

→ Manipulationen der Daten

BlockChain-Infrastruktur



BlockChain-Anwendungen



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

BlockChain-Anwendungssicherheit

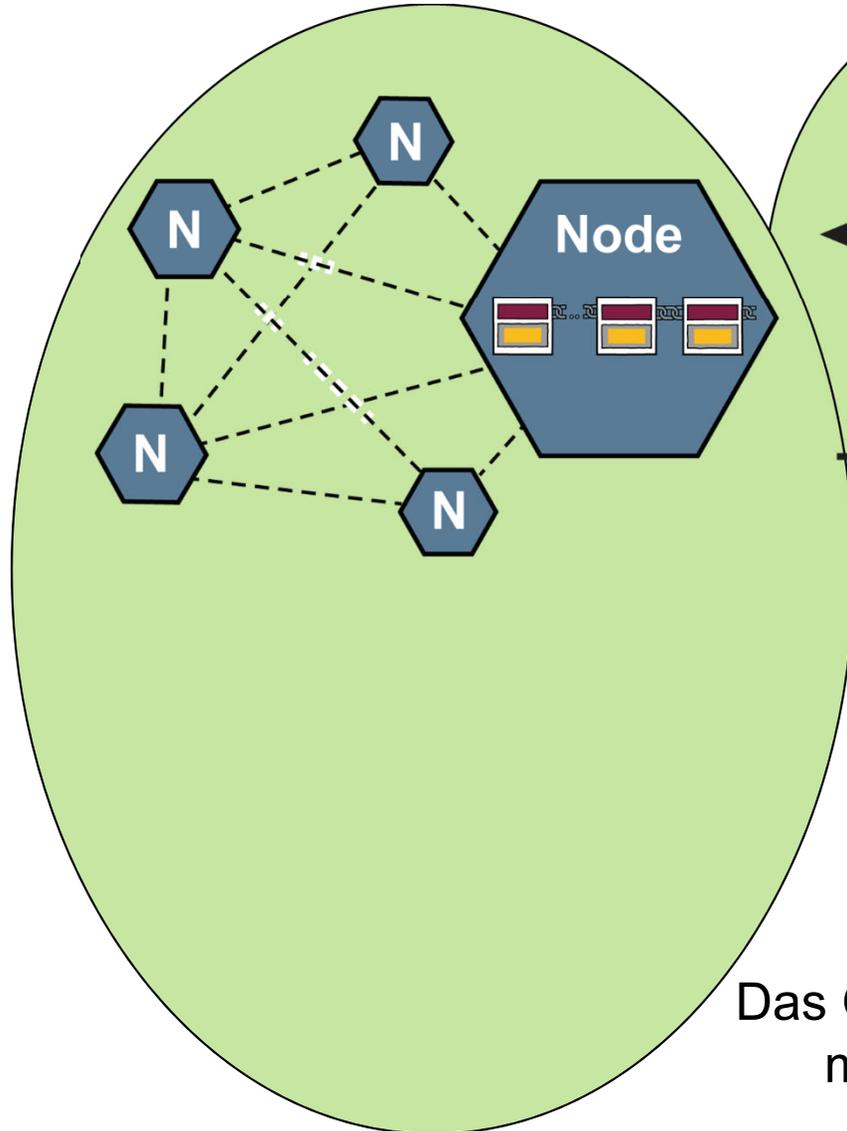
→ Vertrauenswürdig Laufzeitumgebung

- 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
 - ...

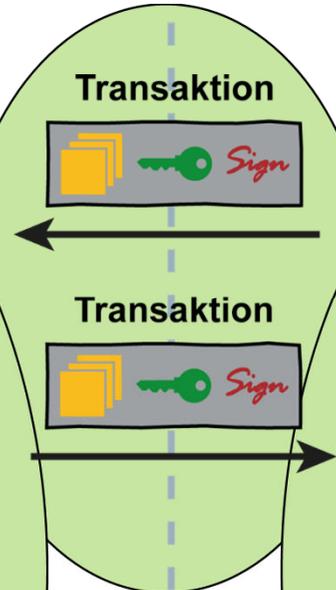
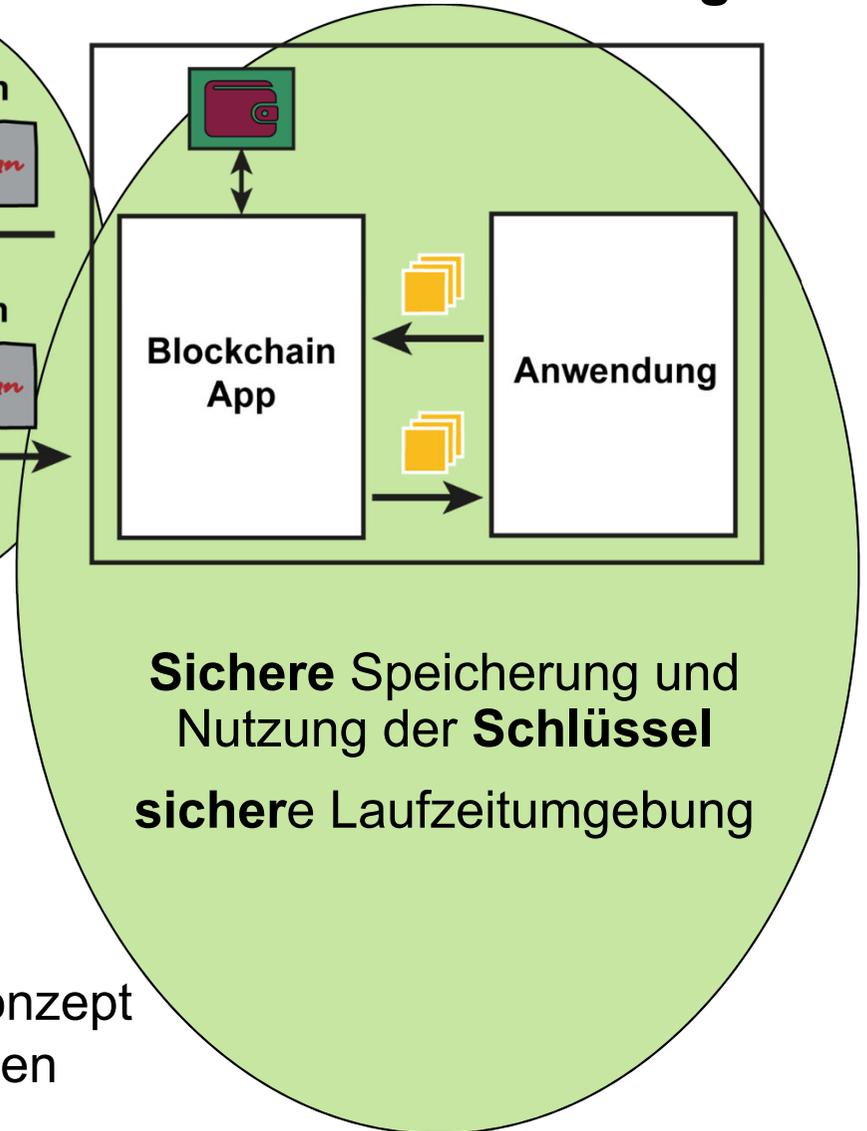
BlockChain-Technologie

→ Trusted BlockChain Interfaces

BlockChain-Infrastruktur



BlockChain-Anwendungen



Das Gesamtkonzept muss passen

Trusted BlockChain Interfaces

Blockchain-Technologie und -Sicherheit

→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Übersicht
- Anwendungssicherheit
- **Blockchain Beispielanwendungen**
- Zusammenfassung

BlockChain Anwendungen

→ Krypto-Währung: Bitcoin

■ Idee:

- Bitcoin ist eine **Internetwährung**, die verteilt, dezentral und unabhängig von einer Zentralbank ein **globales Zahlungsnetzwerk** zur Verfügung stellt.



■ Verfahren:

- Die Funktionsweise des **Bitcoin-Systems** stellt sicher, dass es in ein paar Jahrzehnten maximal 21.000.000 Bitcoins weltweit geben wird.
→ Die Node, die beim Mining gewonnen hat, bekommt 12,5 Bitcoins als Belohnung – Stand 2018 (*ca. 80.000 Euro, alle 10 Min.*)
- Jede Person hat eine **Wallet** und der **Public-Key** entspricht der **Kontonummer**. Mit dem Private-Key werden **Transaktionen** signiert, um **Guthaben** auf diesem Bitcoin-Konto an eine andere Adresse zu überweisen (*public permissionless Blockchain*).

■ Herausforderungen:

- Gesetzliche Grundlage, schwankender Kurs (Zahlungssystem), globale Souveränität, ...



(Ein Bitcoin = 6.375 €, 17,01 Mio. Bitcoins, 108 Mrd. € Kapitalisierung – 26.05.18)

BlockChain Anwendungen

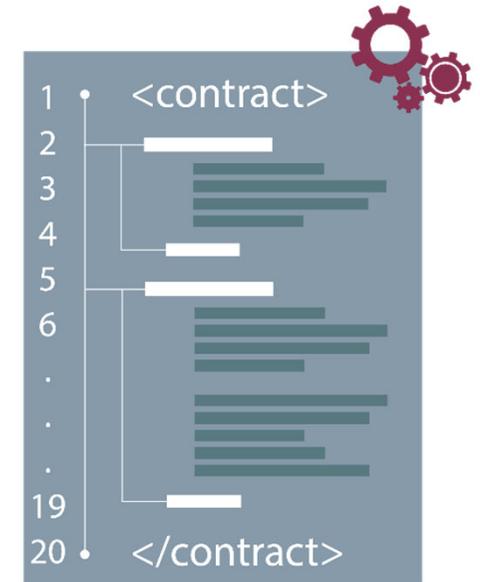
→ Smart Contracts

■ Idee:

- Automatische Umsetzung von Verträgen.

■ Verfahren:

- Programmierbare Verträge werden durch einen **Quelltext** (ausführbarer Programmcode) definiert und bei zuvor festgelegten Bedingungen automatisch auf **BlockChain** ausgeführt.
- Smart Contracts stellen eine Kontroll- oder Geschäftsregel innerhalb eines technischen Protokolls dar.



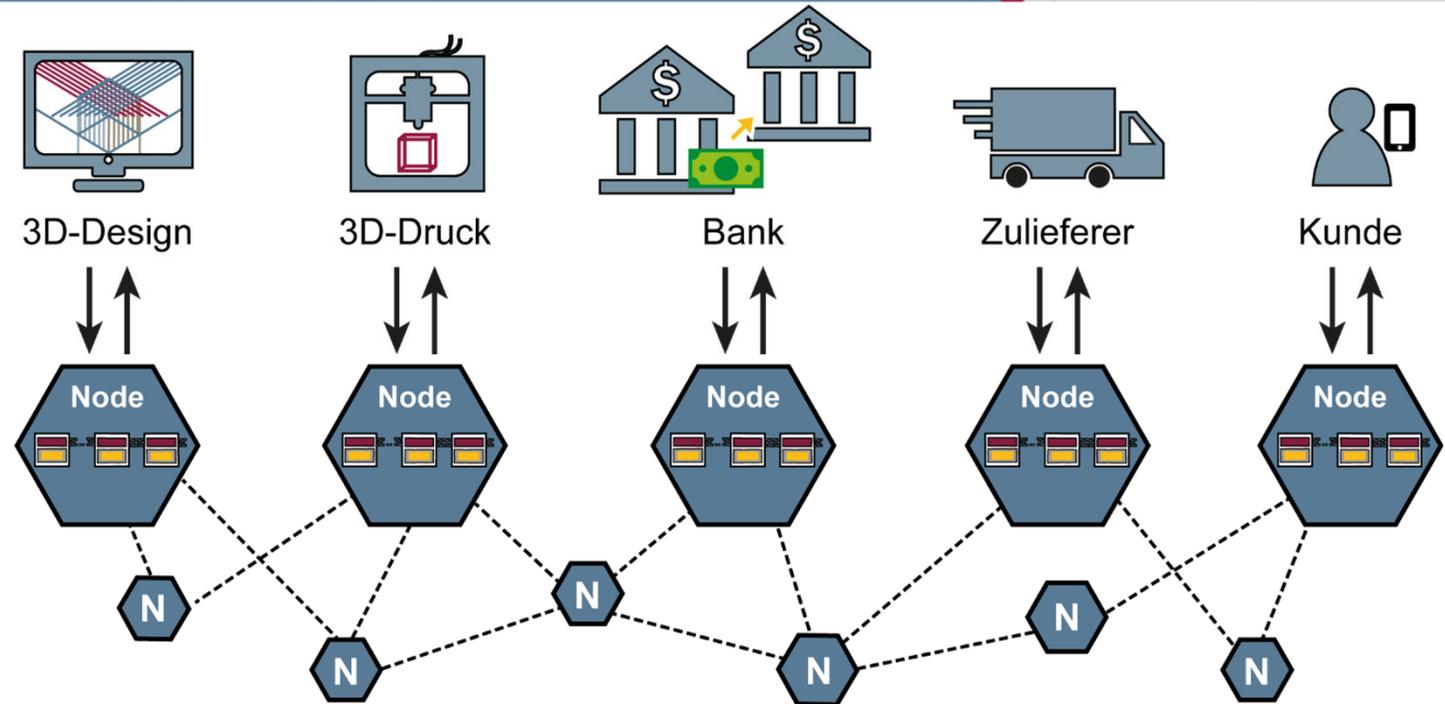
Beispiel:

- Ein geleastes Auto startet nur, wenn die Leasingrate eingegangen ist.
- Eine entsprechende Anfrage des Autos an die **BlockChain** würde genügen.

BlockChain Anwendung

→ Auto. Produktions-, Bezahl- u. Lieferkette

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

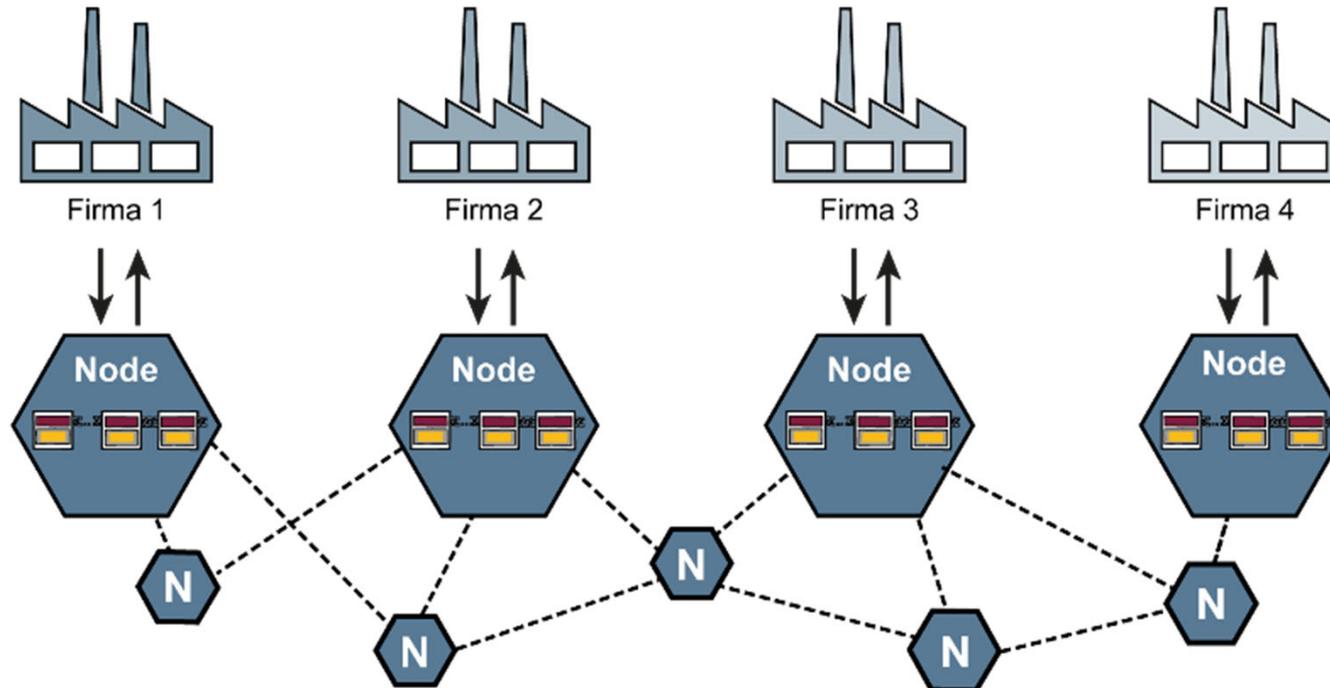


Automatischer Ablauf

- **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 Anwendung

→ Lieferkette, Austausch, ...



Automatisierte und vertrauenswürdige Zusammenarbeit

- Bestellungen für Produktion und Wartung
- Sensordaten für viele Anwendungen
- Automatisierte und vertrauenswürdige Zusammenarbeit mehrere Maschinen
- ...

BlockChain Anwendungen

→ Manipulationssicherheit von Tachometern

■ Idee:

- Das Manipulieren von Tachometern bei Autos erkennen und Schaden daraus verhindern.



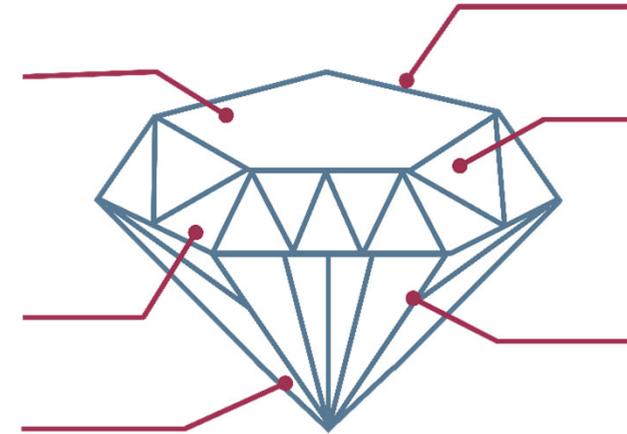
■ Verfahren:

- Wird ein Auto gestartet, wird eine **Transaktion** vom Auto (mit Kennzeichen – **Motornummer**, ...) mit dem **Kilometerstand** an die „**BlockChain**“ gesendet und dort unveränderlich in der richtigen Zeitfolge protokolliert.
- **So kann über die Zeit die Transaktion auf Plausibilität überprüft werden.**
- Eine Manipulation, z.B. durch das Rücksetzen des Kilometerstands wird dadurch erkennbar und verhindert einen Schaden für den Käufer.

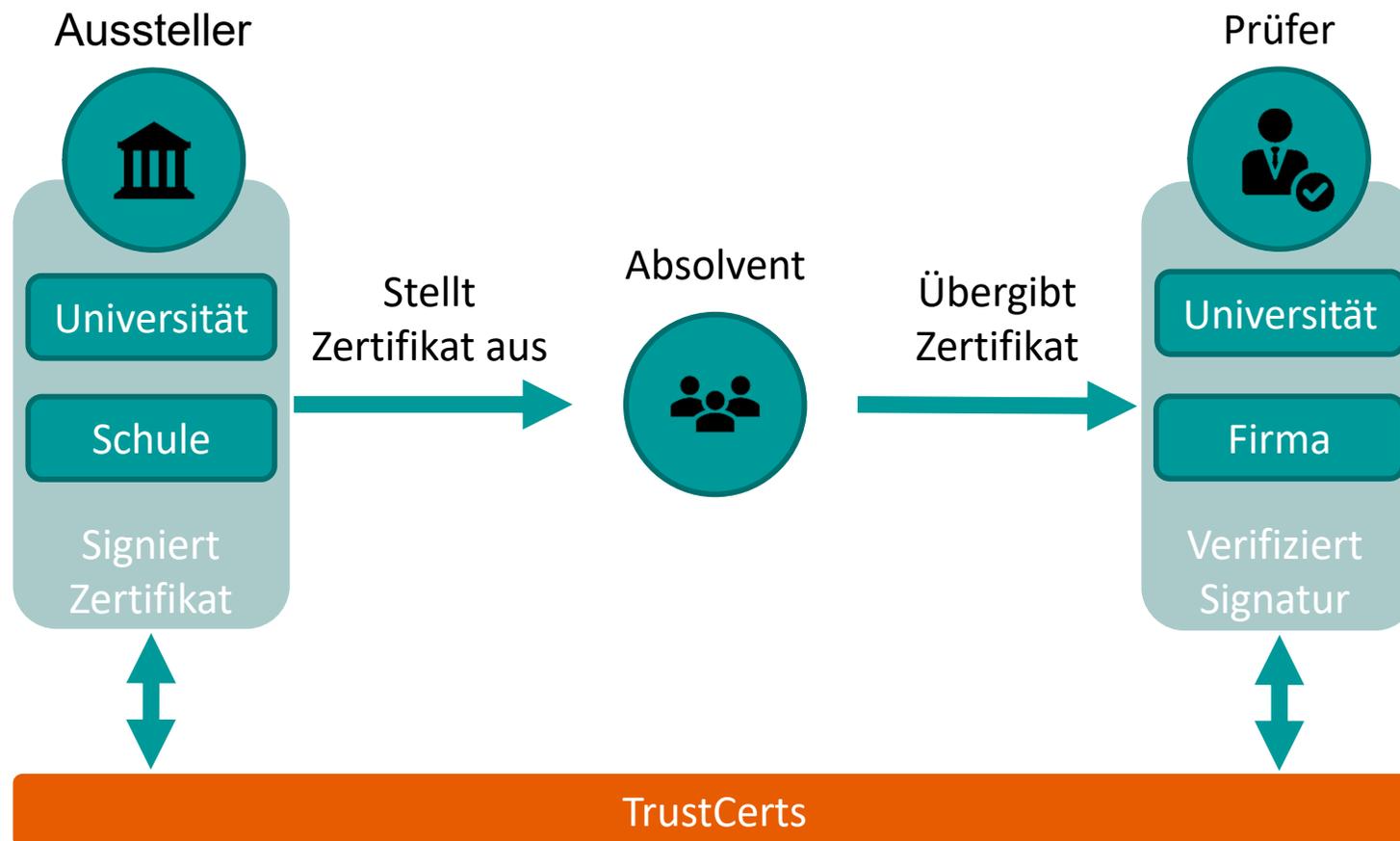
BlockChain Anwendungen

→ Diamantenhandel

- **Idee:**
 - Fälschungen von Diamanten aufdecken
 - Betrüger von Diamanten entlarven
- **Alle Diamanten werden „zertifiziert“** (beglaubigt).
 - Was für eine Qualität des Diamanten vorliegt.
 - **Mehr als 40 Merkmale** zeichnen einen Diamanten aus.
 - **+ Informationen über dem Besitzer**
- **Ablauf und Zahlen**
 - Wird ein Diamant von Person A an Person B verkauft, wird an die **BlockChain** einfach ein neuer Block gehängt mit den Informationen von Diamant X, nur dass als Besitzer Person B eingetragen ist.
 - **Ca. 800.000 Diamanten** wurden bereits eingetragen.



Vertrauensdienste → TrustCerts



Blockchain-Technologie und -Sicherheit

→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Übersicht
- Anwendungssicherheit
- Blockchain Beispielanwendungen
- **Zusammenfassung**

Blockchain-Technologie und -Sicherheit

→ Zusammenfassung (1/2)

- **BlockChain-Anwendungen (Chancen)**
 - Die IT-Marktführer aus den USA bieten eher zentrale Dienste an
 - Für DE und EU mit sehr vielen KMUs eine **ideale Technologie** für eine **vertrauenswürdige verteilte Zusammenarbeit**.
 - **Vertrauensdienste** spielen eine immer **wichtigere Rolle** in der Zukunft!
 - Die **BlockChain-Technologie** schafft eine **Basis** für eine **verteilte** und **vertrauenswürdige Zusammenarbeit** und stellt damit ein **hohes Potential** für neue Geschäftsmodelle und Ökosysteme dar.

Blockchain-Technologie und -Sicherheit

→ Zusammenfassung (2/2)

- Herausforderungen (Risiken)
 - 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.



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Blockchain-Technologie und - Sicherheit

- Vorlesung Cyber-Sicherheit -

Prof. Dr. (TU NN)

Norbert Pohlmann

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

if(is)
internet-sicherheit.

Wir empfehlen

- **Kostenlose App securityNews**



securityNews



- **7. Sinn im Internet (Cyberschutzraum)**

<https://www.youtube.com/cyberschutzraum>



- **Master Internet-Sicherheit**

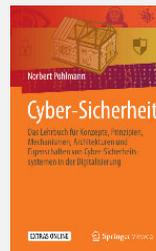
<https://it-sicherheit.de/master-studieren/>



- **Cyber-Sicherheit**

Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2019

- <https://norbert-pohlmann.com/cyber-sicherheit/>



Quellen Bildmaterial

Eingebettete Piktogramme:

- Institut für Internet-Sicherheit – if(is)

Besuchen und abonnieren Sie uns :-)

WWW

<https://www.internet-sicherheit.de>

Facebook

<https://www.facebook.com/Internet.Sicherheit.ifis>

Twitter

[https://twitter.com/ ifis](https://twitter.com/ifis)

YouTube

<https://www.youtube.com/user/InternetSicherheitDE/>

Prof. Norbert Pohlmann

<https://norbert-pohlmann.com/>

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 / Bücher

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: „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-Vertrauensw%C3%BCrdigkeit-kryptografisch-verkettete-Datenbl%C3%B6cke-Prof.-Norbert-Pohlmann.pdf>

M. Mollik, N. Pohlmann: „Trust as a Service – Vertrauen als Dienstleistung – Validierung digitaler Nachweise mit der Blockchain“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 3/2019

<https://norbert-pohlmann.com/wp-content/uploads/2019/08/399-Trust-as-a-Service-Vertrauen-als-Dienstleistung-Validierung-digitaler-Nachweise-mit-der-Blockchain-Prof.-Norbert-Pohlmann.pdf>

N. Pohlmann: "Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, ISBN 978-3-658-25397-4; 594 Seiten, Springer-Vieweg Verlag, Wiesbaden 2019

<https://norbert-pohlmann.com/cyber-sicherheit/>