

**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

BlockChain-Technologie

→ Sicherheit und Anwendungen

Prof. Dr. (TU NN)

Norbert Pohlmann

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

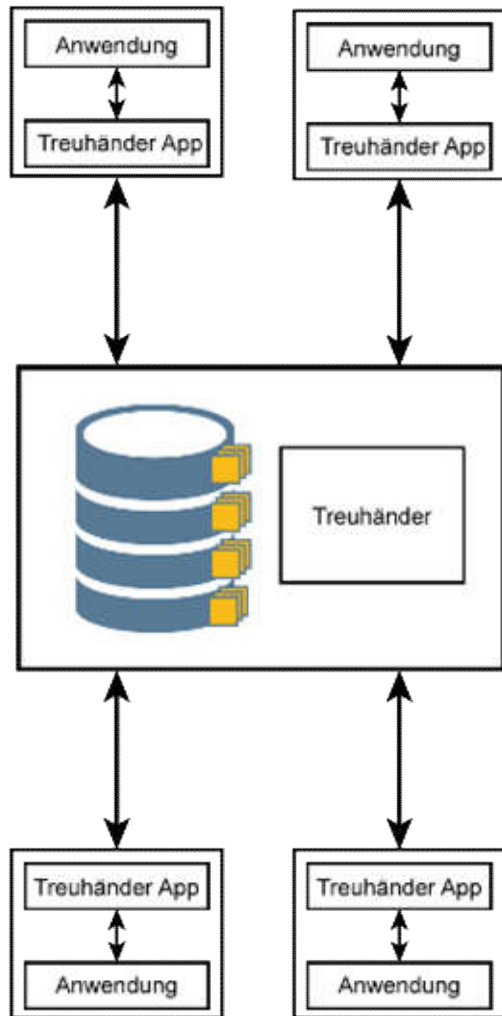
if(is)
internet-sicherheit.

- **Übersicht**
(Sichtweisen, Sicherheitseigenschaften, ...)
- **Anwendungssicherheit**
(Schlüsselspeicherung, Manipulation, ...)
- **Blockchain Beispielanwendungen**
(Bitcoin, Smart Contracts, automatisierte Zusammenarbeit, ...)
- **Zusammenfassung**
(Chancen und Risiken)

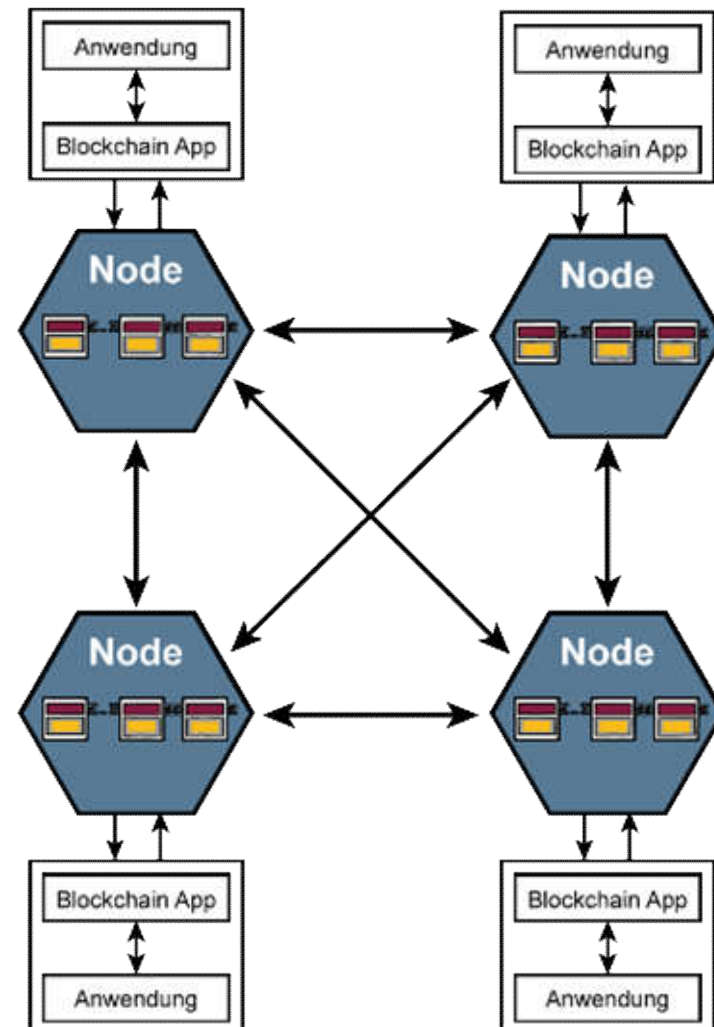
- **Übersicht**
(Sichtweisen, Sicherheitseigenschaften, ...)
- **Anwendungssicherheit**
(Schlüsselspeicherung, Manipulation, ...)
- **Blockchain Beispielanwendungen**
(Bitcoin, Smart Contracts, automatisierte Zusammenarbeit, ...)
- **Zusammenfassung**
(Chancen und Risiken)

BlockChain-Technologie → auf den Punkt gebracht

Transaktionsspeicher



Zentrale Architektur



Dezentrale Architektur

BlockChain-Technologie

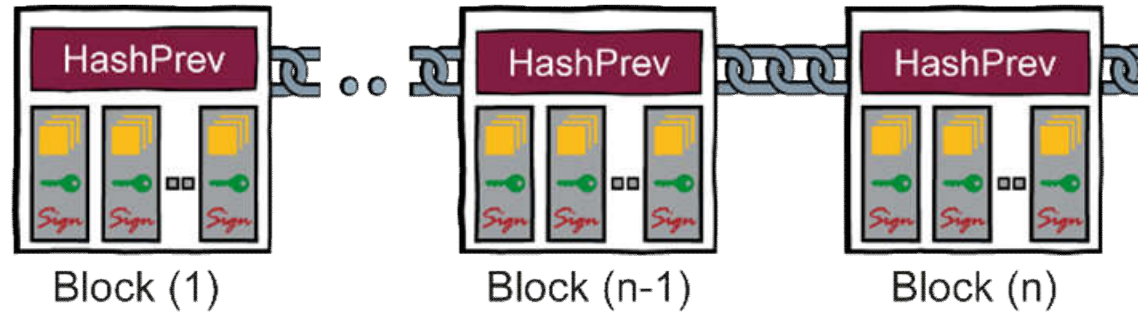
→ Das „Internet der Werte“

- **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



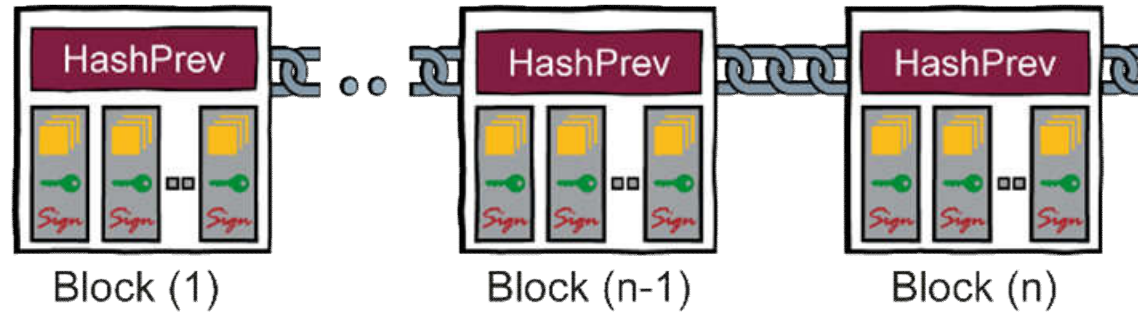
BlockChain

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

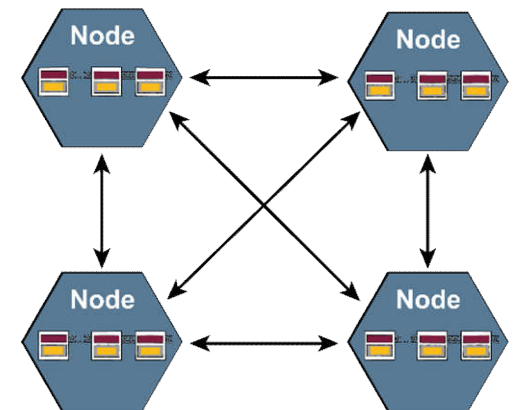
(Sicherheitseigenschaften einer **BlockChain**)

BlockChain-Technology

→ Datenstruktur einer BlockChain



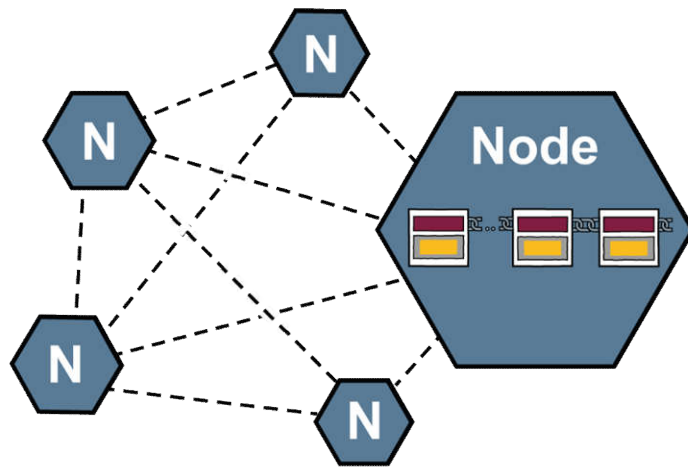
- Die **Daten** sind Transaktionsdaten mit Geldeinheiten, Zertifikaten, Produktionsdaten, Sensordaten, Source Code, ... digitale Werte
- Transaktionen mit **Daten** werden vom Teilnehmer erstellt und **signiert** (Wallet/Schlüssel). Passende **Public Key** in der Transaktion. Verteilung
- **Block** beinhaltet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



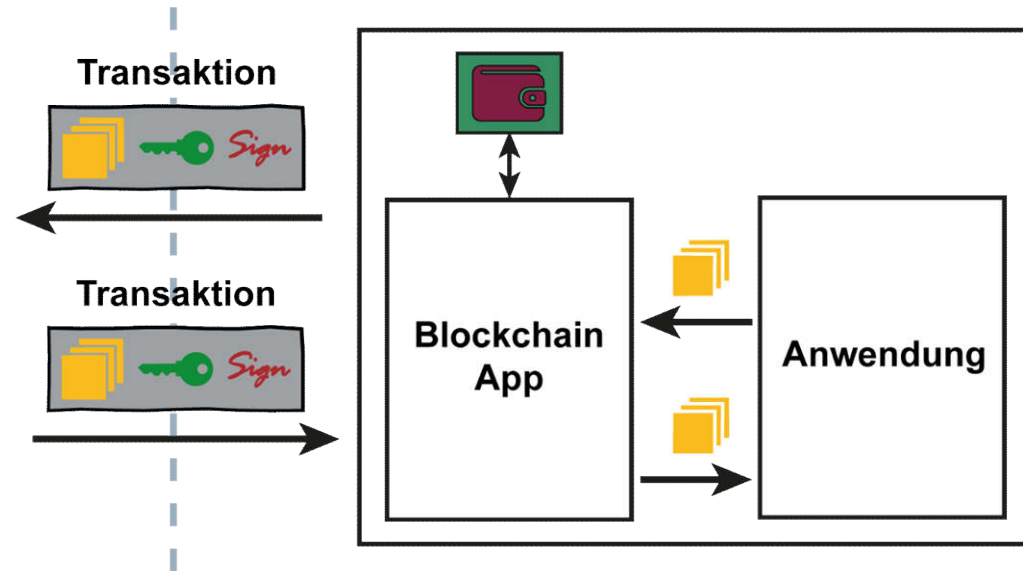
BlockChain-Technologie

→ Infrastruktur und Anwendung

BlockChain-Infrastruktur



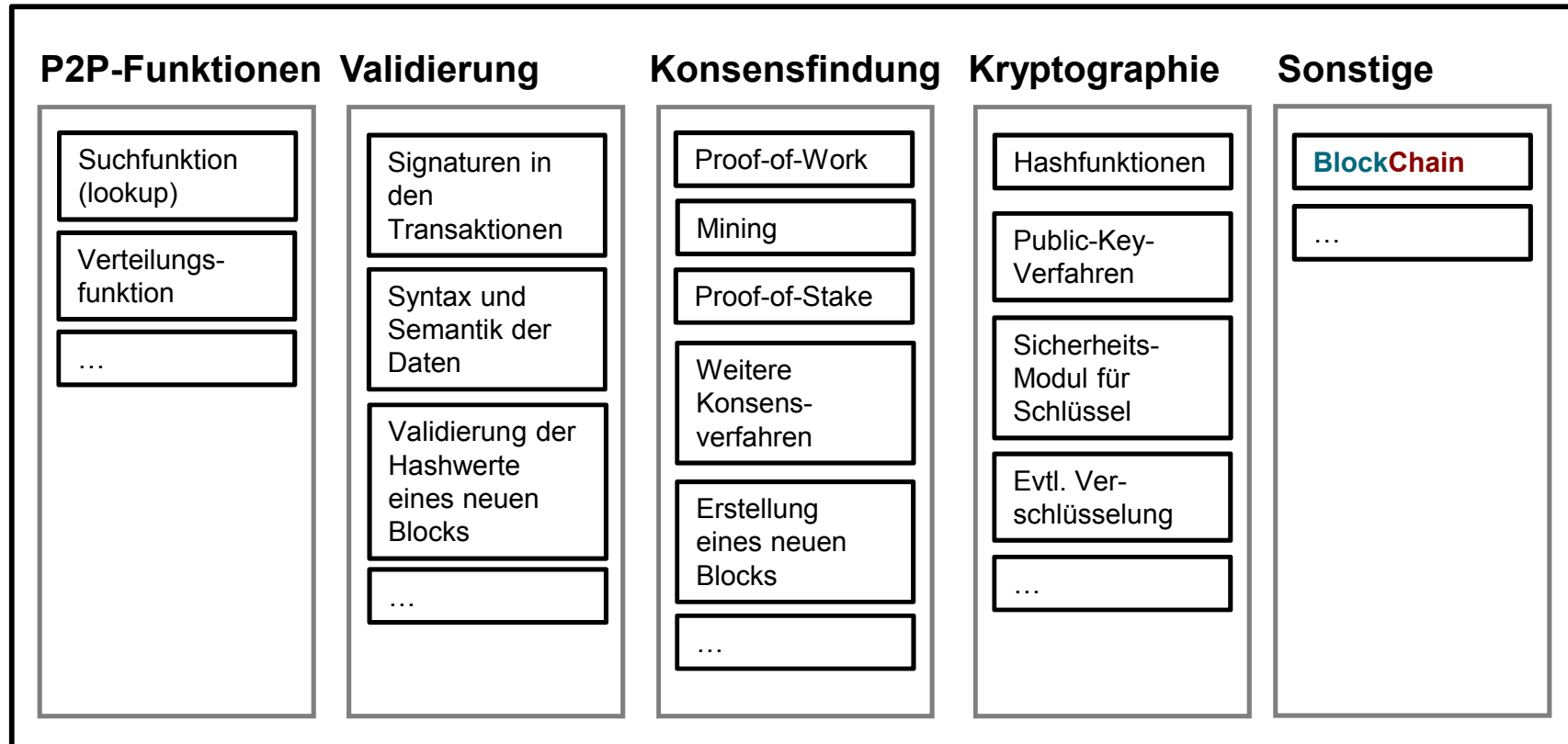
BlockChain-Anwendungen



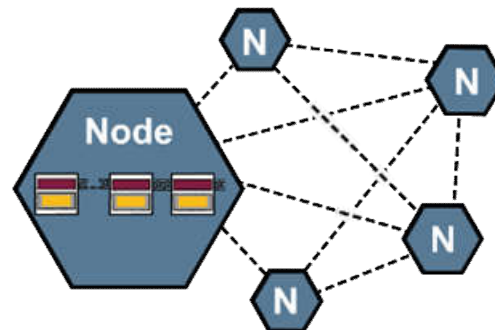
- Die **BlockChain-Infrastruktur**
(Peer-to-Peer-Netzwerk, Nodes mit allen Kommunikations-, Sicherheits- und Vertrauensfunktionen, die **BlockChain** als Datenstruktur, ...)
- Die **BlockChain-Anwendungen**
(Blockchain-App, Wallet/Schlüssel, eigentliche Anwendung, ...)
- Die **Transaktionen** als Schnittstelle dazwischen

BlockChain-Infrastruktur

→ Funktionen in einer Node



Node



BlockChain-Infrastruktur

→ Eigenschaften: **verteilt** und **redundant**

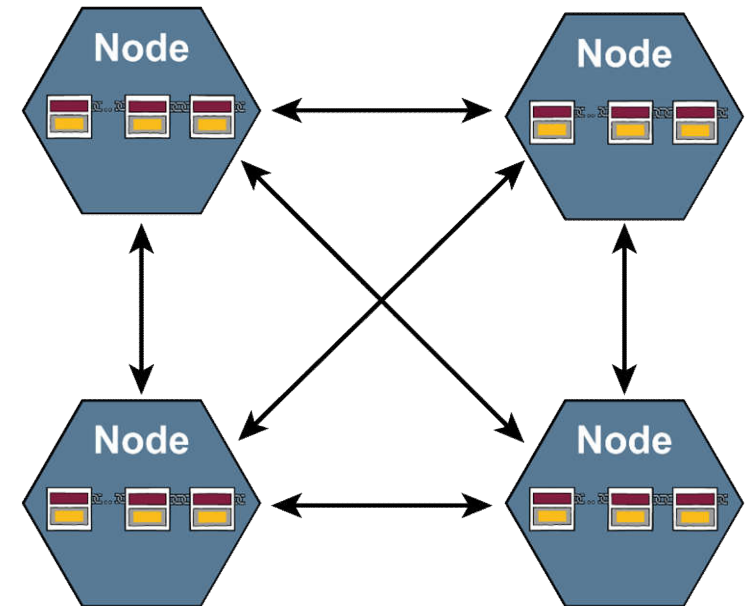
Robustes Peer-to-Peer-Netzwerk

■ Skalierbarkeit / Ressourcenbedarf

- Bandbreite zwischen den Nodes
- Speicherplatzkapazität auf der Node (Bitcoin **BlockChain** hat eine Größe von 160 G Byte)
- Rechnerkapazität (CPU, RAM, ...)
- einer Node
- ...

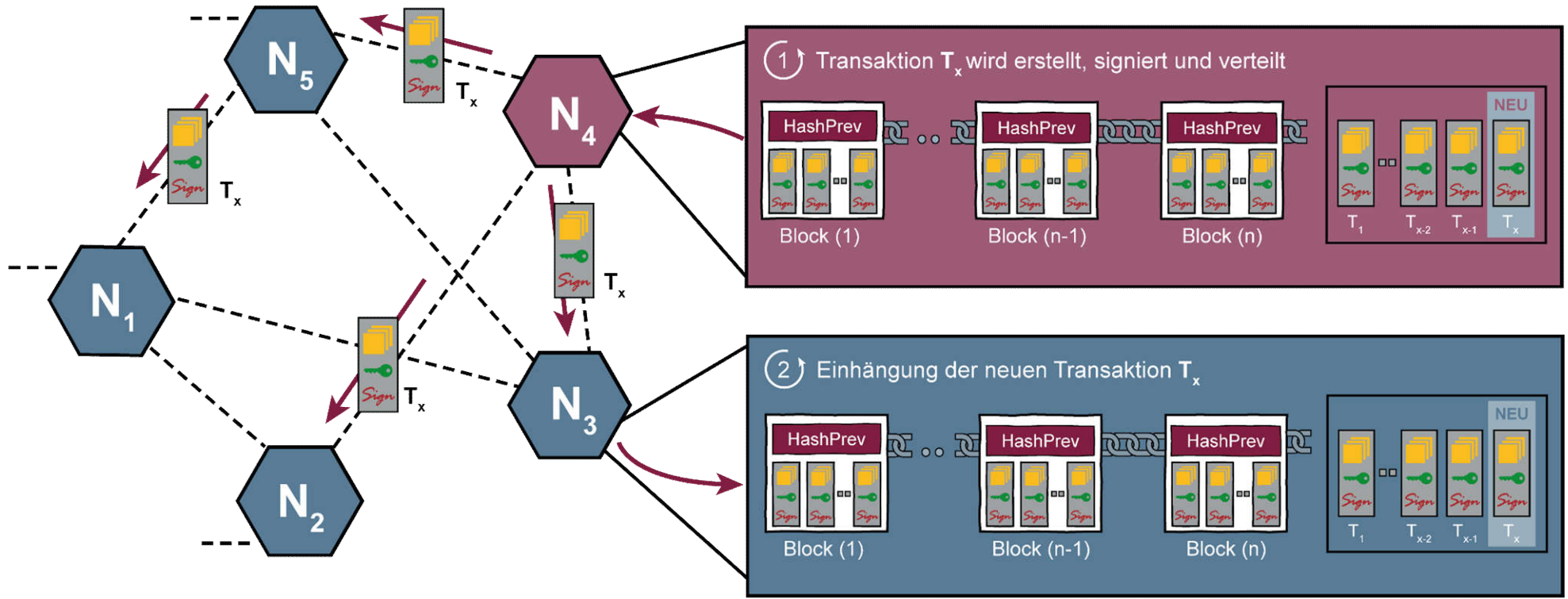
■ Zuverlässigkeit / Verfügbarkeit

- Anzahl der Nodes
- Robust für die Verteilung von Transaktionen und neue Blöcke
- Robust gegen DDoS-Angriffe
- ...



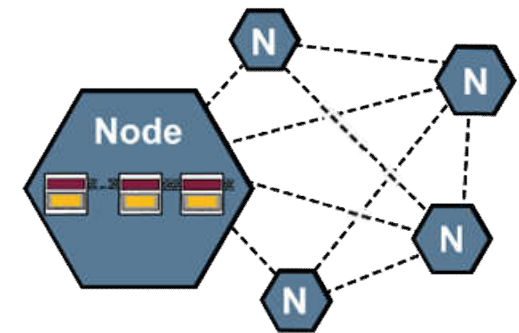
BlockChain-Infrastruktur

→ Versendung von Transaktionen



Kryptographie-Agilität

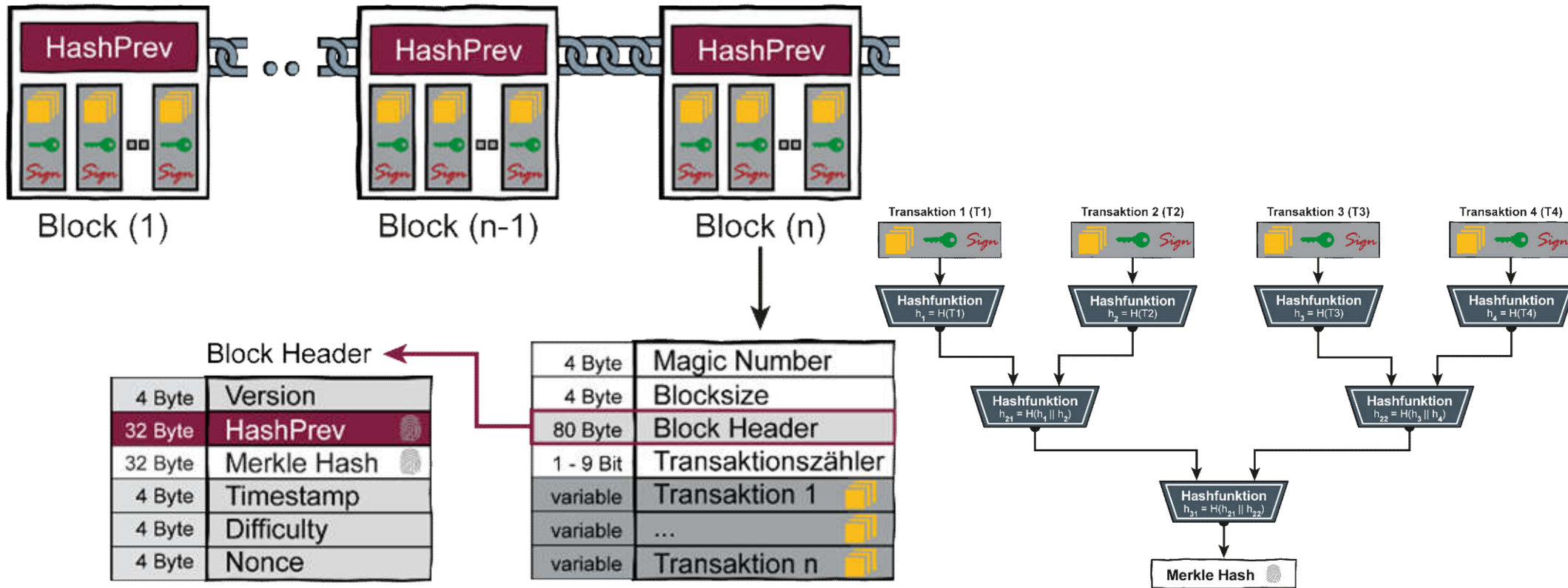
- **Stand der Technik** (Technische Richtlinie: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“)
 - **Public-Key-Verfahren** (*Signierung / Verifizierung* von Transaktionen)
→ (*RSA - 3.000 bit*)
 - **Hashfunktionen** (*Adresserzeugung, HashPrev, Merkle Hash*)
→ (*SHA-3 - 256 bit*)
- **Risiko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



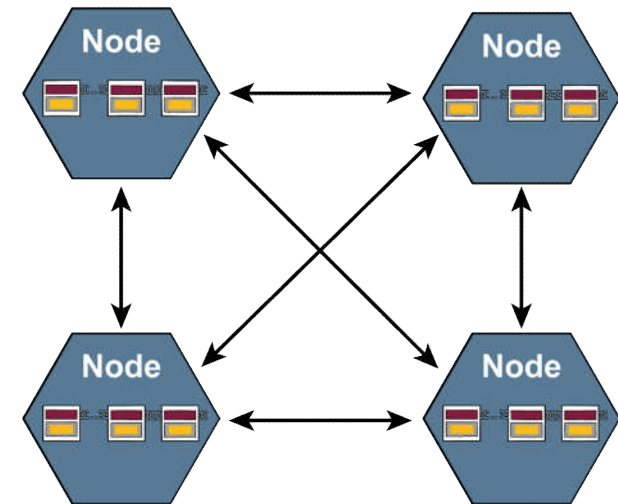
$$\text{HashPrev}_n = H(\text{Block-Header}_{n-1})$$

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

- 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.



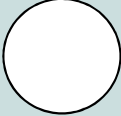

Vertrauenswürdigkeitsmechanismen

- **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, ...



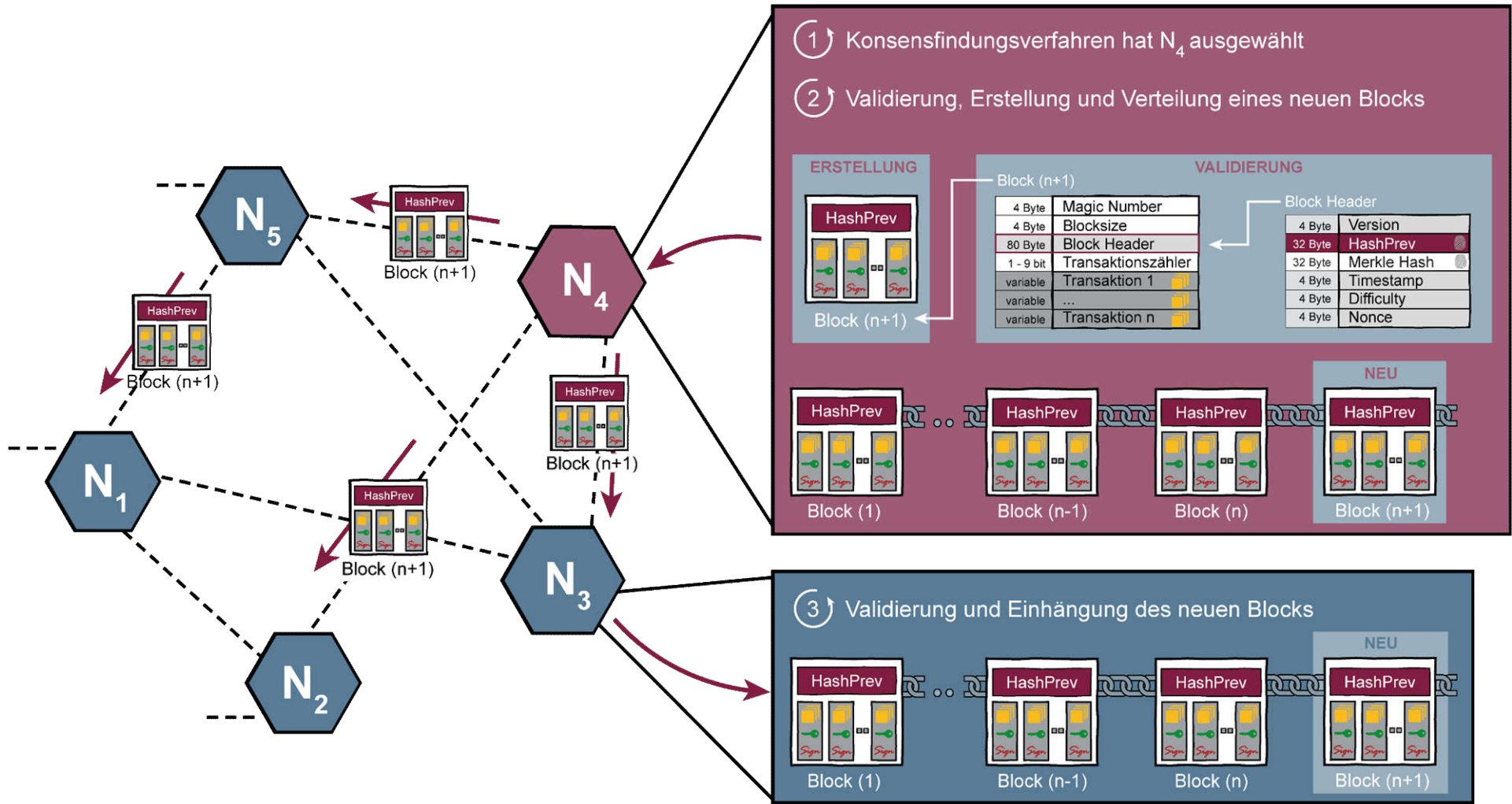
BlockChain-Infrastruktur

→ 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-Infrastruktur

→ Validierung von neuen Blöcken



- **Übersicht**
(Sichtweisen, Sicherheitseigenschaften, ...)
- **Anwendungssicherheit**
(Schlüsselspeicherung, Manipulation, ...)
- **Blockchain Beispielanwendungen**
(Bitcoin, Smart Contracts, automatisierte Zusammenarbeit, ...)
- **Zusammenfassung**
(Chancen und Risiken)

BlockChain-Anwendungssicherheit

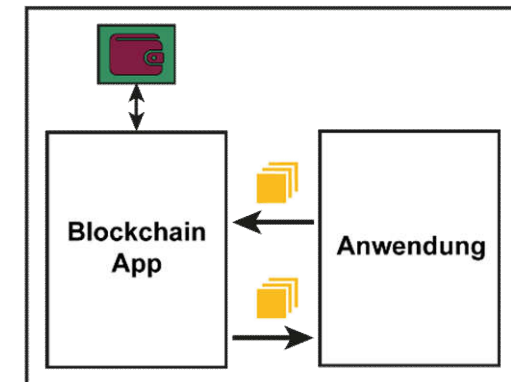
→ Übersicht Anwendung

■ 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



Teilnehmer

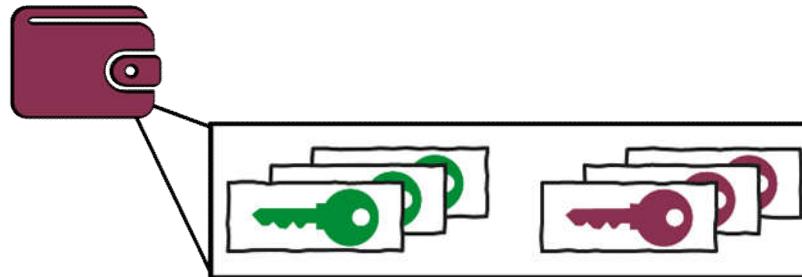
■ Anwendung

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

Blockchain-Anwendungssicherheit

→ Sicherheit der Schlüssel

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

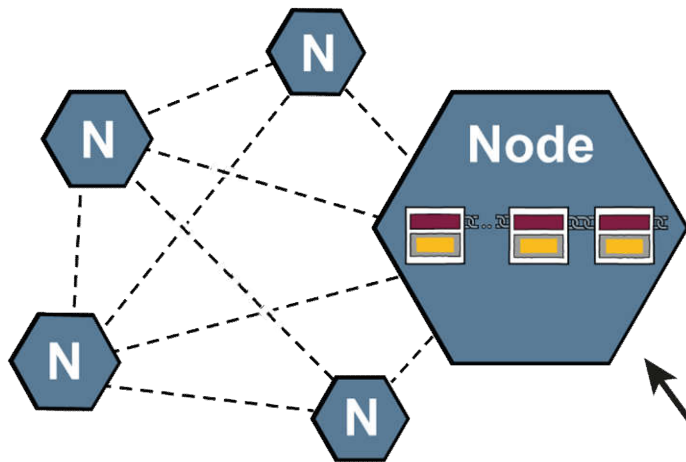


- Gefahren** bei nicht ausreichendem Schutz des **privaten Schlüssels**
 - Der **private Rechner / IoT-Gerät** wird **gehackt** (Malware)
 - Die **Website** der Online Wallet (Service Node) wird **gehackt**
 - Ein nicht ausreichend gesichertes **Smartphone** wird **gestohlen** (Light N.)
 - Der **private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

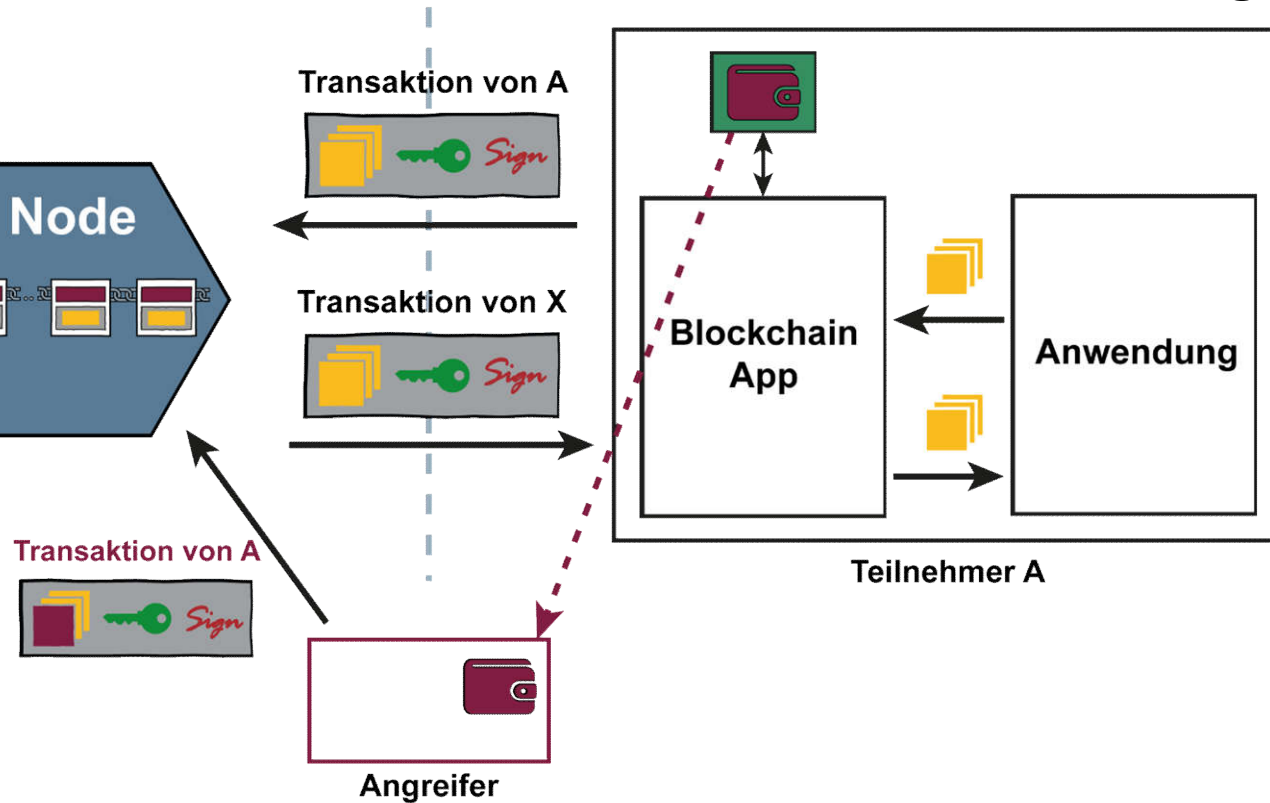
BlockChain-Anwendungssicherheit

→ Manipulationen der Transaktionen

BlockChain-Infrastruktur



BlockChain-Anwendungen

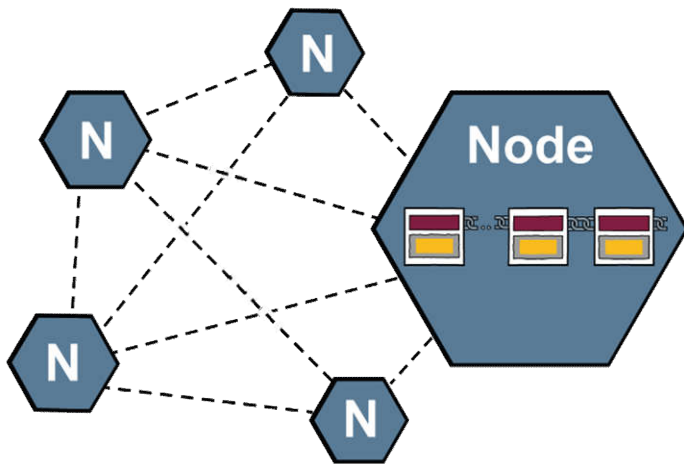


- Der Angreifer „*besitzt*“ die **Wallet/Schlüssel** oder kann sie „*unberechtigt nutzen*“
 - Damit kann er valide Transaktionen für den entsprechenden Teilnehmer A erstellen und die **BlockChain**-Anwendung manipulieren

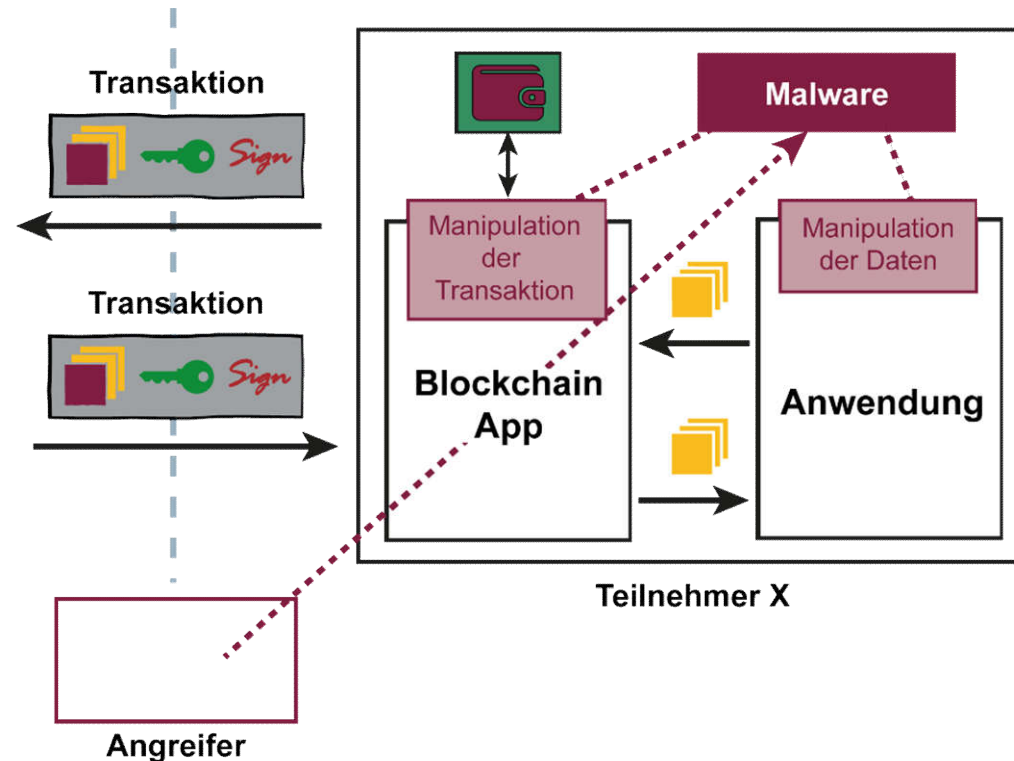
BlockChain-Anwendungssicherheit

→ 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 und eingehende Transaktionen
 - Die Transaktionen sind im **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
 - ...

- **Übersicht**
(Sichtweisen, Sicherheitseigenschaften, ...)
- **Anwendungssicherheit**
(Schlüsselspeicherung, Manipulation, ...)
- **Blockchain Beispielanwendungen**
(Bitcoin, Smart Contracts, automatisierte Zusammenarbeit, ...)
- **Zusammenfassung**
(Chancen und Risiken)

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

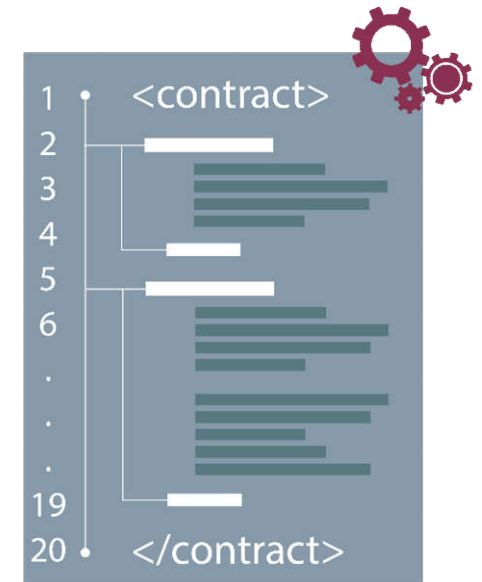
→ Smart Contracts

■ 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.



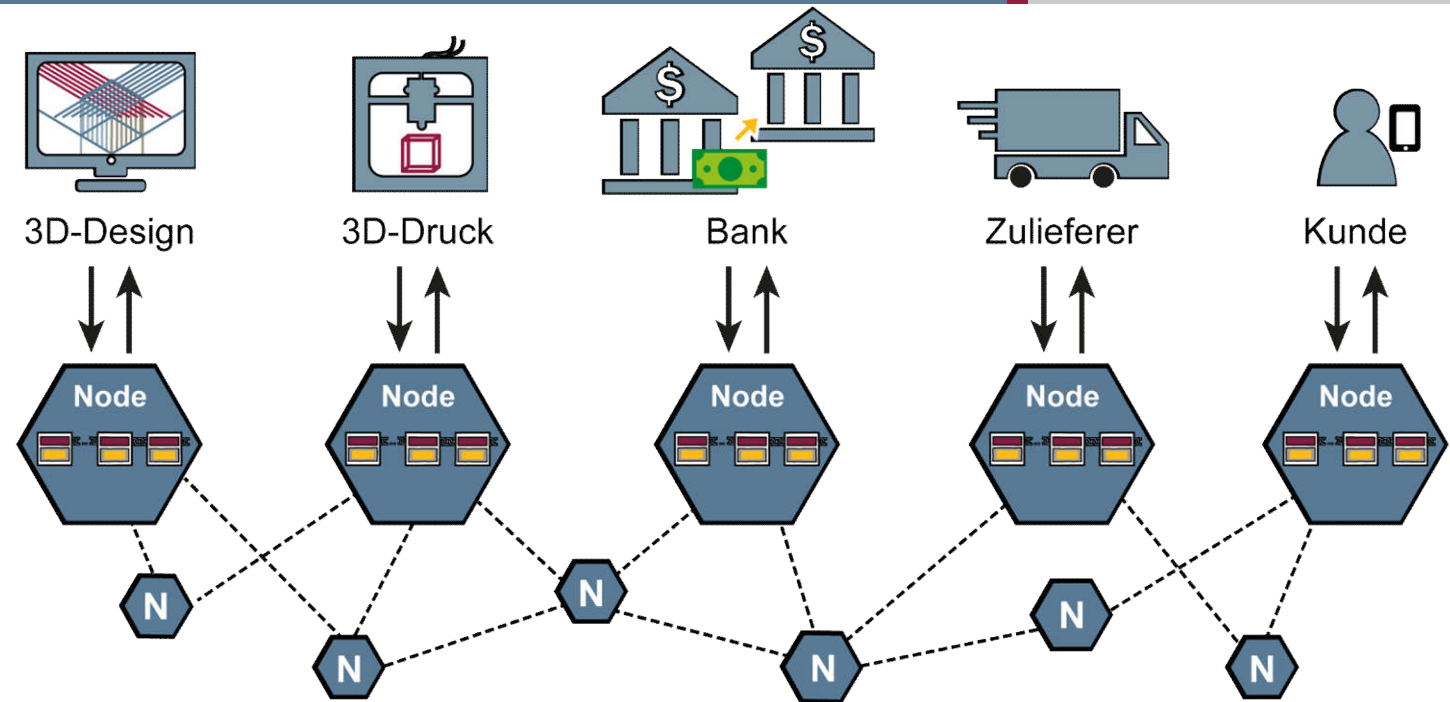
Beispiel:

- 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.

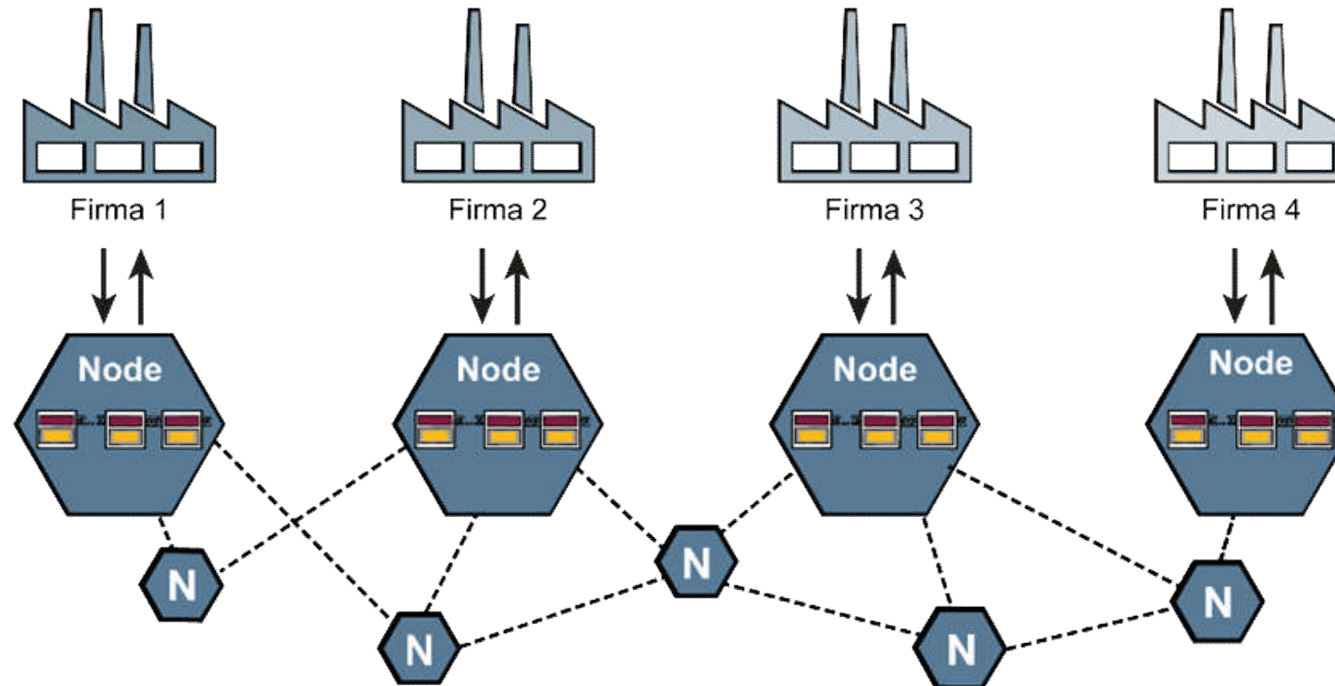


Automatischer Ablauf

- **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, ...

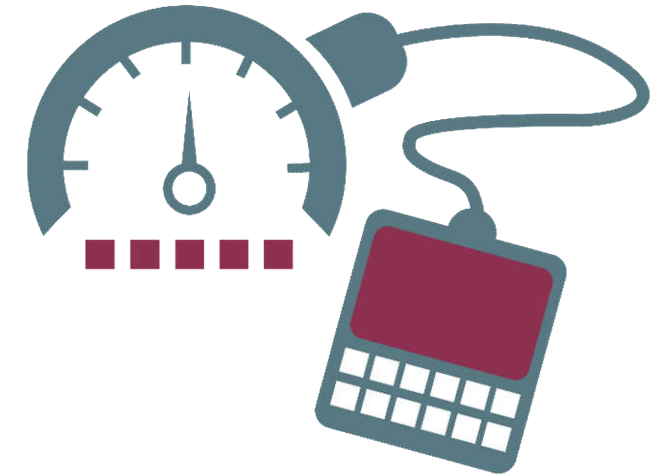


Automatisierte und vertrauenswürdige Zusammenarbeit

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

- **Idee:**

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



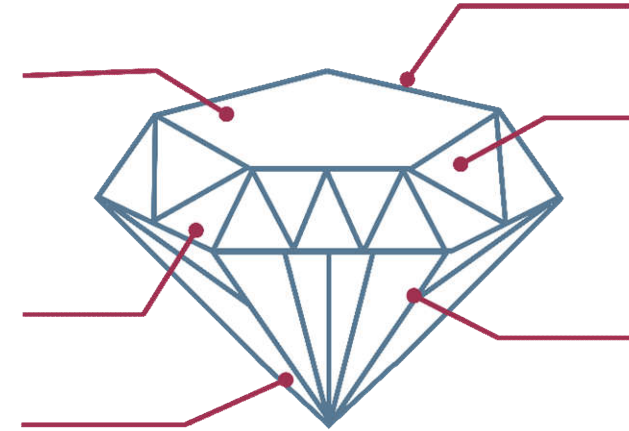
- **Verfahren:**

- 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.

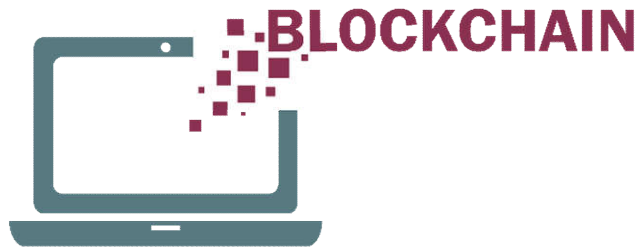


- **Übersicht**
(Sichtweisen, Sicherheitseigenschaften, ...)
- **Anwendungssicherheit**
(Schlüsselspeicherung, Manipulation, ...)
- **Blockchain Beispielanwendungen**
(Bitcoin, Smart Contracts, automatisierte Zusammenarbeit, ...)
- **Zusammenfassung**
(Chancen und Risiken)

BlockChain

→ Zusammenfassung

- **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.
- **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

→ Sicherheit und 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.

Wir empfehlen

- **Kostenlose App securityNews**



securityNews



- **7. Sinn im Internet (Cyberschutzraum)**
https://www.youtube.com/channel/UCEMkJW9dHcWfek_En3xhjg

- **Cybärcast – Der IT-Sicherheit Podcast**
<https://podcast.internet-sicherheit.de/>



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



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>

Google+

<https://plus.google.com/107690471983651262369/posts>

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/>

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>