

**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Die **BlockChain**

Potenziale, Chancen und Risiken der Querschnittstechnologie

Prof. Dr. (TU NN)

Norbert Pohlmann

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

if(is)
internet-sicherheit.

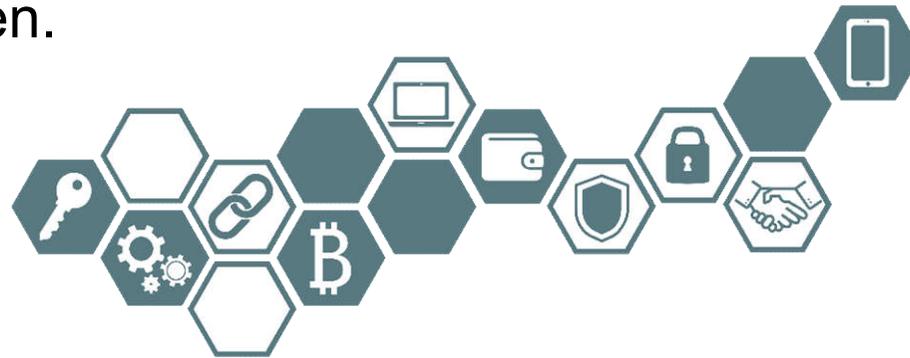
- **Übersicht**
(Chancen, Sichtweiten, Tools)
- **Elemente, Prinzipien, Architekturen, ...**
(Daten, Transaktionen, Block, ..., verteilt, Konsens, ...)
- **Anwendungen**
(Bitcoin, Smart Contracts, Diamantenhandel, ...)
- **Sicherheitsherausforderungen**
(Kryptosystem, Schlüsselspeicherung, Anzeige, ...)
- **Zusammenfassung**
(Chancen und Risiken)

- **Übersicht**
(Chancen, Sichtweiten, Tools)
- **Elemente, Prinzipien, Architekturen, ...**
(Daten, Transaktionen, Block, ..., verteilt, Konsens, ...)
- **Anwendungen**
(Bitcoin, Smart Contracts, Diamantenhandel, ...)
- **Sicherheitsherausforderungen**
(Kryptosystem, Schlüsselspeicherung, Anzeige, ...)
- **Zusammenfassung**
(Chancen und Risiken)

BlockChain → Distributed Ledger

→ Übersicht

- Die „**BlockChain**“ ist eine **spannende und faszinierende IT-Technologie**, die das Potential hat, Politik, Verwaltung und Wirtschaftszweige gewaltig auf den Kopf zu stellen.



- Die **BlockChain**-Technologie ist eine **Querschnittstechnologie** mit hohem **disruptiven Potenzial** für viele Wirtschaftsbereiche.
- Die **BlockChain**-basierten Systeme könnten in vielen Bereichen **zentrale Instanzen ablösen**, wie Banken, Notare oder Treuhänder.
- Das ist möglich, weil die **Validierungsalgorithmen** der **BlockChain**-Technologie, ganz ohne solche Intermediäre, die **Vertrauenswürdigkeit der aufgezeichneten Transaktionsdaten garantieren**.
- Die **BlockChain**-Technologie macht IT-Systeme **effektiver und sicherer in bestimmten Bereichen und Situationen**.

BlockChain Konzept

→ Unterschiedliche Sichtweisen

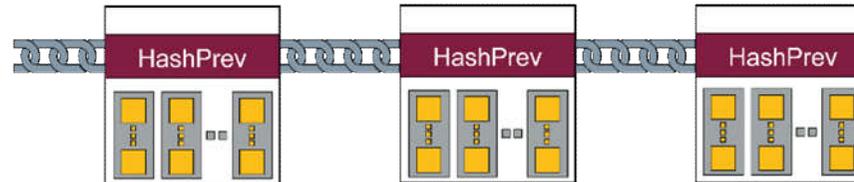
- Für einen **Informatiker** ist die **BlockChain** eine **einfache Datenstruktur**, die Daten sind in einzelnen „Blöcken“ verkettet und in einem **verteilten Netz redundant** (mehrfach) verwaltet.
Die Alternative wäre z.B. eine konventionelle Datenbank.
- Für die **IT-Sicherheitsexperten** hat die **BlockChain** 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 Zusammenarbeit zwischen verschiedenen Organisationen**.
Die Alternative wäre z.B. ein kostenintensiver Treuhänder.

BlockChain

→ Verteilte Datenbank/ Collaboration-Tool

BlockChain

■ BlockChains



- sind **fälschungssichere**, *kryptographische Verfahren (Hashfunktionen / Public-Key-Verfahren)*

- **verteilte, redundante** Datenstrukturen *Vielzahl von Teilnehmern gespeichert (jede Note hat die Blockchain gespeichert)*

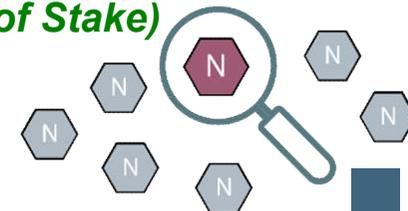
- in denen **Transaktionen in der Zeitfolge protokolliert** *Art der Verkettung (HashPrev)*



- **nachvollziehbar, unveränderlich** und *jeder kann Kryptographie überprüfen (Hashwert, Signatur)*



- **ohne zentrale Instanz** abgebildet sind. *geeignete Konsensfindungsverfahren (Proof of Work, Proof of Stake)*



BlockChain → „programmiertes Vertrauen“

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*.

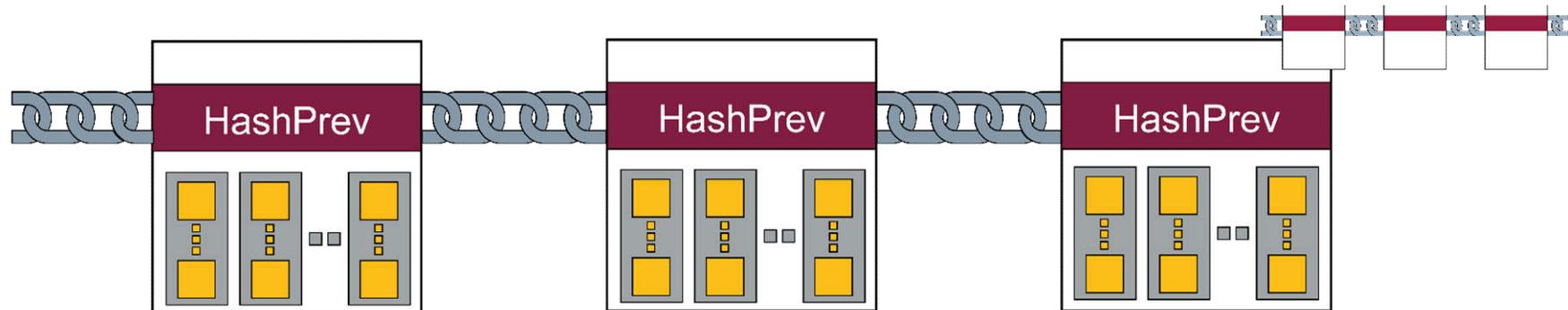
BlockChain → „Internet der Werte“

- **Übersicht**
(Chancen, Sichtweiten, Tools)
- **Elemente, Prinzipien, Architekturen, ...**
(Daten, Transaktionen, Block, ..., verteilt, Konsens, ...)
- **Anwendungen**
(Bitcoin, Smart Contracts, Diamantenhandel, ...)
- **Sicherheitsherausforderungen**
(Kryptosystem, Schlüsselspeicherung, Anzeige, ...)
- **Zusammenfassung**
(Chancen und Risiken)

Blockchain

→ Element: Daten

- Die **Blockchain** ist eine einfache Datenstruktur



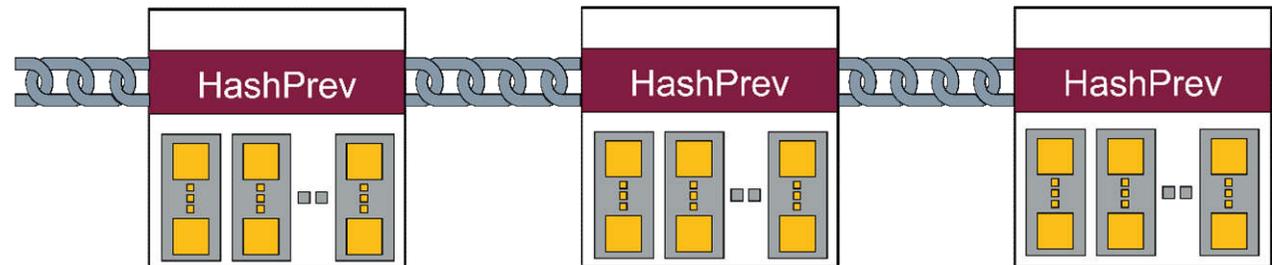
- Daten** werden in einzelnen, chronologisch **miteinander verketteten Blöcken** als **Transaktionen verwaltet**.
- Die **Daten** werden vor **Manipulationen gesichert** in der **Blockchain** gespeichert (siehe **Transaktionen**)!
- Die **Blockchain** ist bei jeder Node und damit verteilt und redundant vorhanden, d.h. es besteht eine sehr hohe Verfügbarkeit der Daten.
- Eine **Blockchain** kann sehr groß sein (z.B. Bitcoin etwa **146 G Byte** – Stand: Dezember 2017)

Blockchain

→ Element: Block

- Ein **Block** in einer **Blockchain** ist ein strukturierter Datensatz, der beliebige Transaktionen *mit Daten* enthalten kann.

- Block Header** sorgt für die **Verkettung** der Blöcke
- HashPrev**: *Hashwert* des Vorgängerblocks



Block

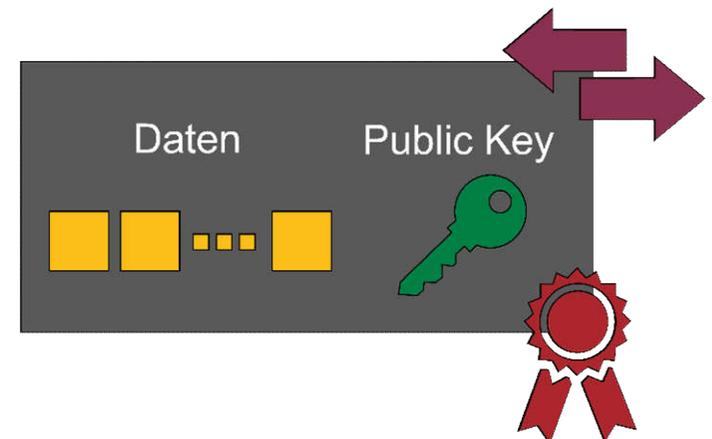
4 Byte	Magic Number
4 Byte	Blocksize
160 Byte	Block Header
1 – 9 Bit	Transaktionszähler
variabel	Transaktion 1 
variabel	... 
variabel	Transaktion n 

Block Header

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

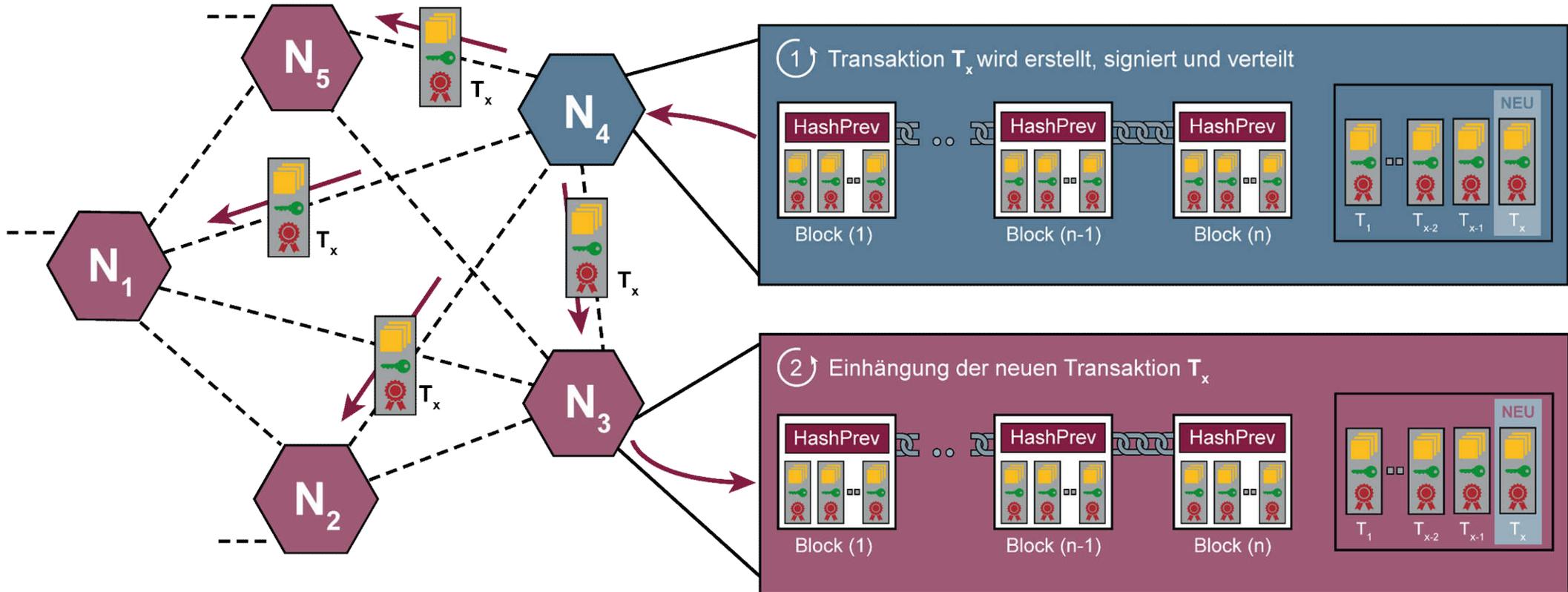
- Die Transaktionen in einem **Block** werden mit einem Hashwert geschützt (**Merkle Root Hash**).

- Transaktionen enthalten **Daten**, die in der Zeitfolge protokolliert (chronologisch), nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet sind.
- Die **Daten** können *Kontostände*, **Werte**, *Attribute*, **Quelltexte**, *Merkmale*, usw. (allgemein: **digital Assets**) sein
- Eine **Transaktion** enthält auch immer den **Public-Key (Adresse)** „der Node“, der die **Transaktion** erstellt und signiert hat.
- Jede **Transaktion**, die hinzugefügt werden soll, muss zunächst mit dem **Private-Key aus der Wallet signiert** und an alle Nodes über das **P2P-Blockchain-Netzwerk** gesendet werden.
- Jede **Node** im **P2P-Blockchain-Netzwerk** kann die **Identität** der Node, welche die **Transaktion** erstellt und abgesendet hat, und den Inhalt der **Transaktion verifizieren**.



Blockchain

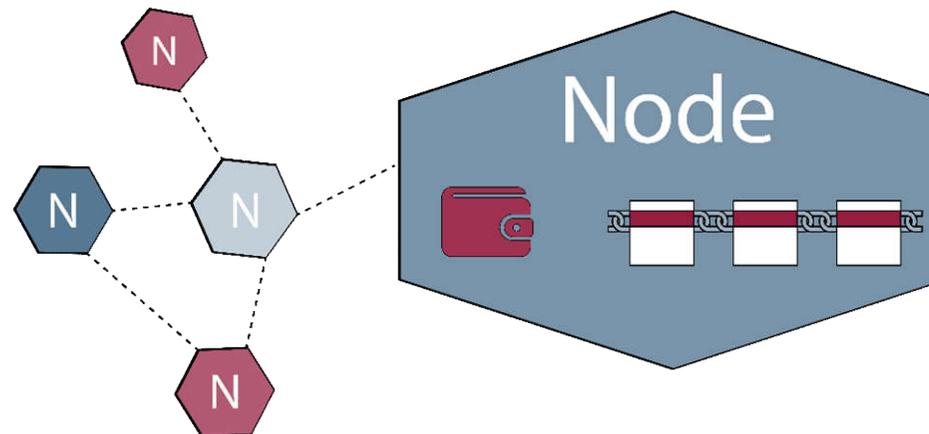
→ Element: Transaktion (2/2)



Blockchain

→ Element: Node

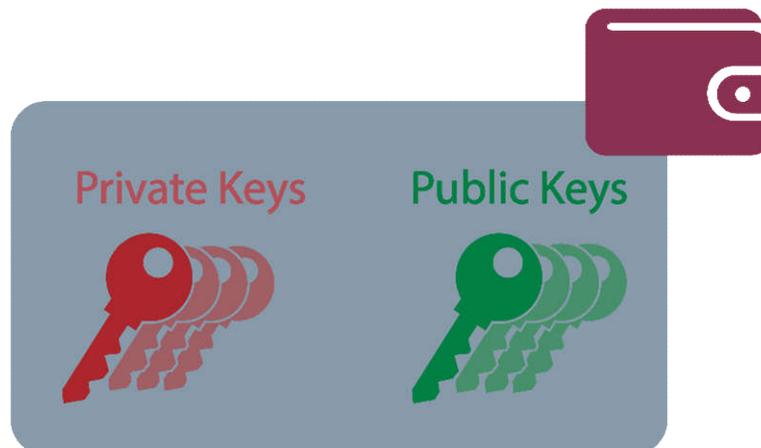
- Jeder, der an der „**Blockchain**“ teilnimmt, wird als „**Node**“ beziehungsweise „Teilhaber“ bezeichnet.
- Jede Node erhält eine **aktuelle Kopie** der **Blockchain**, die fortlaufend aktualisiert wird.
- Jede Node, die zu einer „**Blockchain**“ gehört, falls diese nicht eingeschränkt ist, hat im Prinzip die gleichen Rechte, die **Blockchain** zu speichern und neue Blöcke hinzuzufügen (validieren).
- Eine Node kann eine **Wallet** haben und **Transaktionen** mit **Daten** erstellen, signieren und im Peer-to-Peer-**Blockchain**-Netzwerk verteilen.



Blockchain

→ Element: Wallet

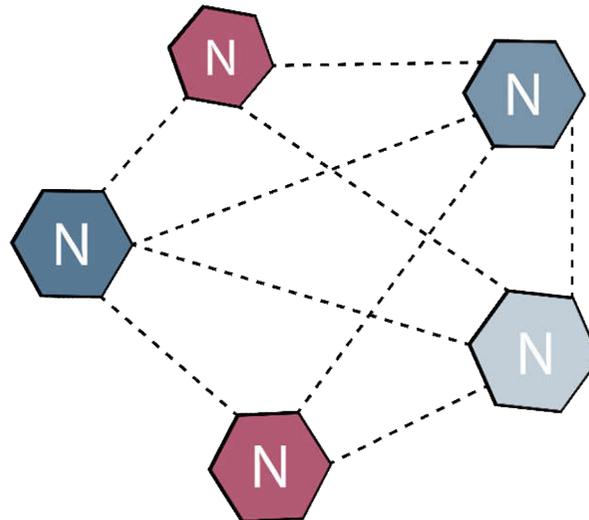
- Eine Node kann über eine „**Wallet**“ verfügen (siehe auch später).
- Eine **Wallet** ist dabei eine Datenstruktur, in der die eigenen **Private- und Public-Keys** *sicher* gespeichert sind.
- Aus dem Public-Key wird mit Hilfe einer Funktion die **eindeutige Kennung (Adresse)** berechnet.
- Mit dem **Private-Key** wird eine **Transaktion** signiert.
- Mit Hilfe des **Public-Keys** ist es möglich, zu **verifizieren**, dass die **Transaktionen von einer bestimmten „Node“** erstellt wurden.



→ Prinzip: Keine „zentrale Instanz“

- Eine **BlockChain** besitzt keine „zentrale Instanz“, sondern ist auf all ihren Nodes (Teilhabern) in einem Peer-to-Peer-**BlockChain**-Netzwerk verteilt.
- Jeder kommuniziert zum Beispiel über das Internet direkt miteinander.
- Damit gibt es **keinen „Single Point of Failure“** mehr und Logs beziehungsweise Backups müssen nicht besonders berücksichtigt werden, da die Datenstruktur (**BlockChain**) sich selbst regeneriert (*sehr hohe Verfügbarkeit und Ausfallsicherheit*).

Peer-to-Peer Netzwerk

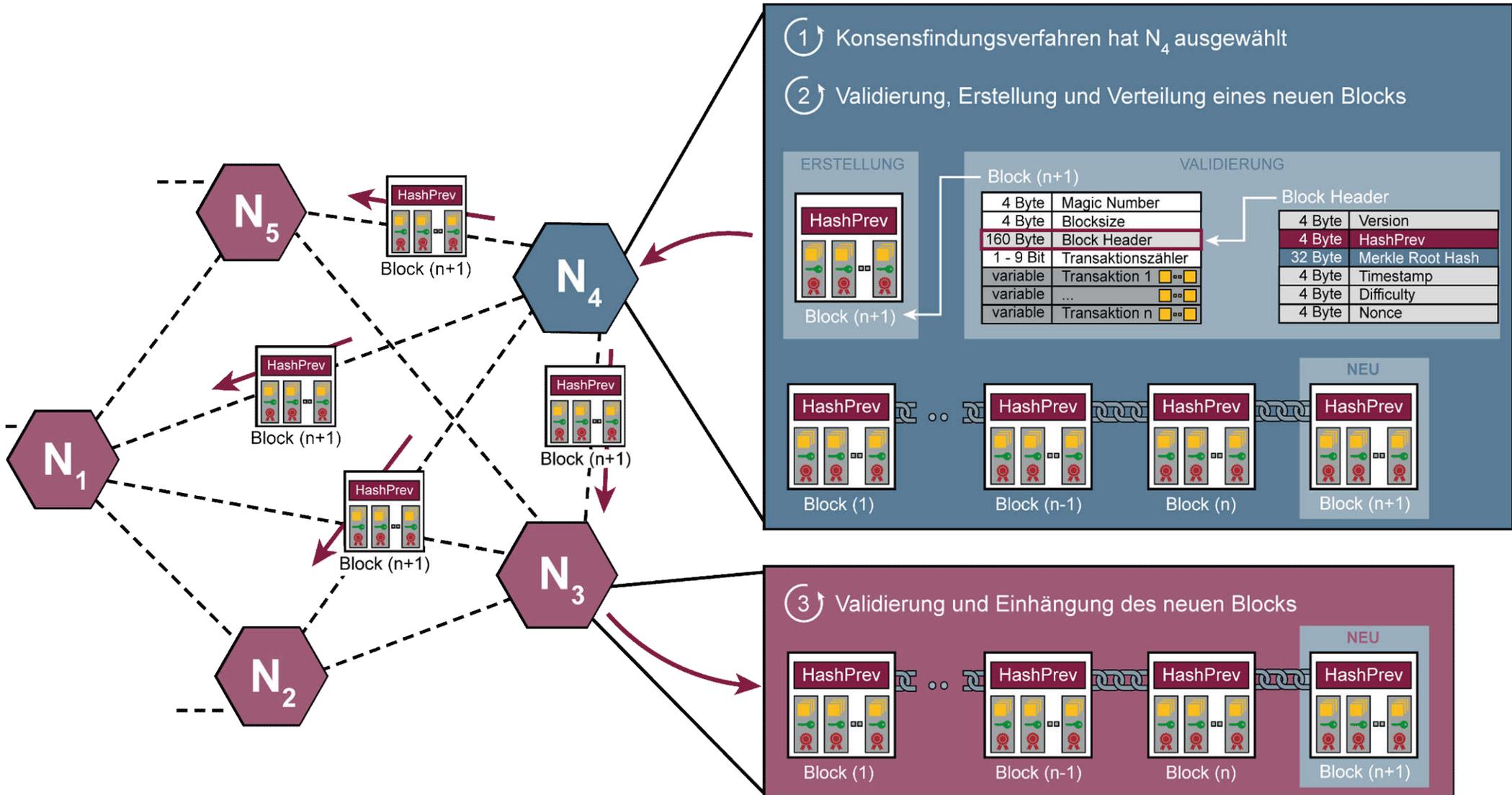


- Alle **Transaktionen** werden von den entsprechenden „Nodes“ signiert, die für die **Daten** verantwortlich sind und an alle anderen Nodes über das Peer-to-Peer-Netzwerk verteilt.
- Ein **Konsensfindungsverfahren** bestimmt, welche Node einen neuen Block validieren und an die **BlockChain** „hängen“ darf.
- Diese Node überprüft, ob die **Transaktionen** von **Semantik** und **Syntax** her richtig sind und ob die **digitalen Signaturen** des Initiators der **Transaktionen** mit der **Adresse** übereinstimmen.
- Dann wird ein neuer Block generiert (Hashwerte – HashPrev und Merkle Root Hash) und an alle Nodes verteilt. Jede Node hat dadurch jederzeit eine **Kopie** der aktuell gültigen **BlockChain**.
- Dieses Prinzip des **Distributed Consensus** macht die Konsistenzprüfung der **Transaktionen** vollkommen unabhängig von einer einzelnen vertrauenswürdigen Instanz. Für die Herstellung des Konsenses gibt es verschiedene Verfahren.



Blockchain

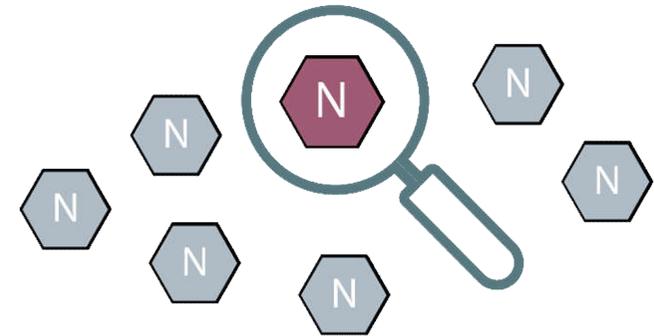
→ Validierung von neuen Blöcken (2/2)



BlockChain

→ 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
 - ...



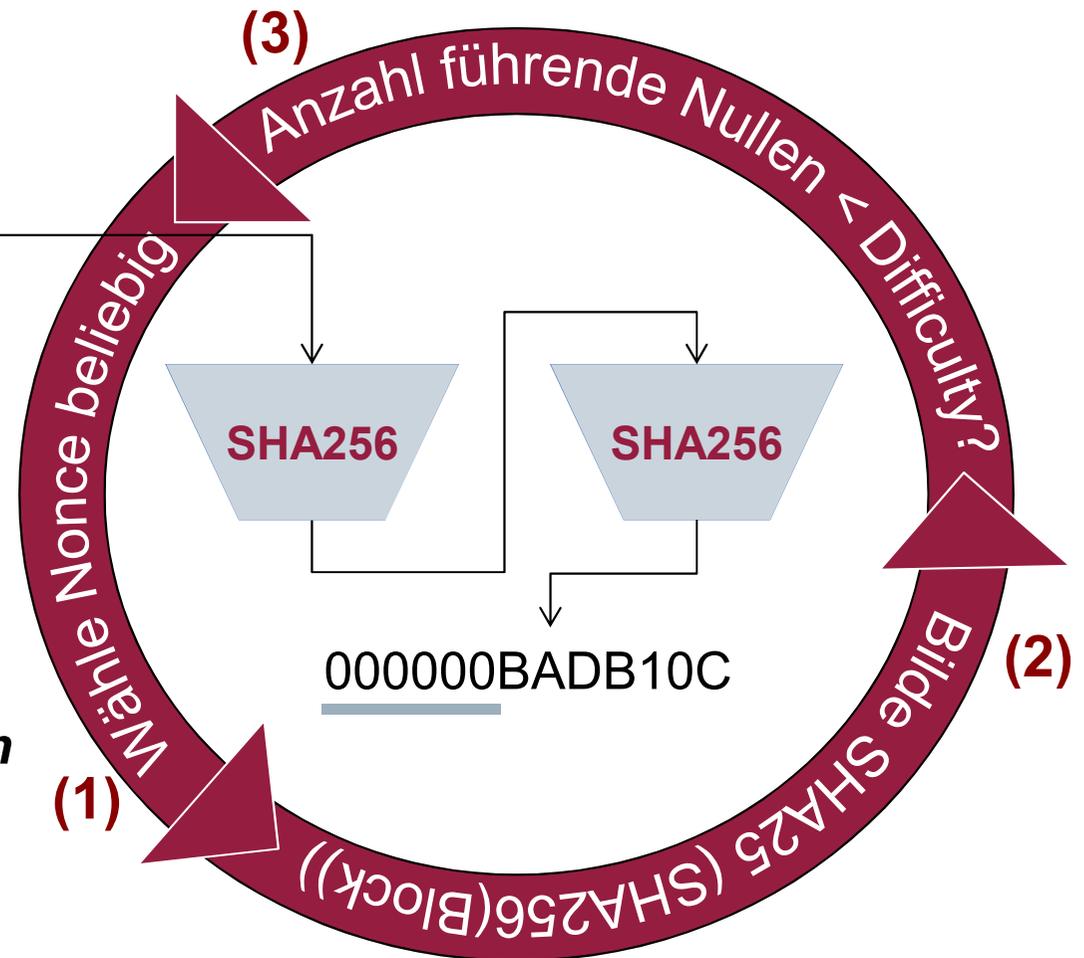
Mining (Proof of Work)

→ Gewinnen der Challenge

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

Block Header

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



Challenge

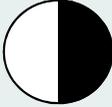
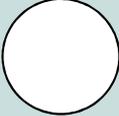
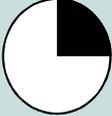
Ist die **Anzahl der führenden Nullen** größer oder gleich der **Difficulty**, gilt der Block als geschürft und wird im P2P-Netzwerk verteilt.

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

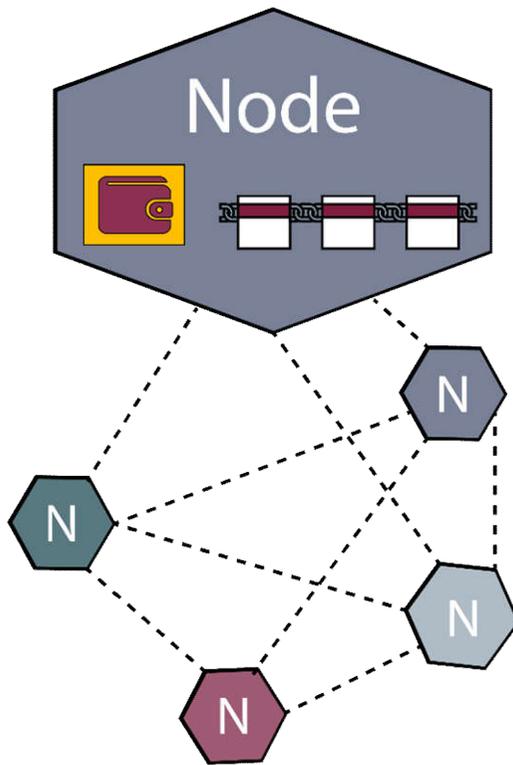
- **Die Challenge kostet sehr viel Energie:**
 - 2,8 Mio. US-Dollar pro Tag (Stromkosten)
 - 1,3 Giga-Watt
 - das sind ca. 10 US-Dollar pro **Transaktion**
- Solange eine **Node nicht die Mehrheit an Miner-Kapazitäten besitzt** (mehr als 51%), ist das Mining-Prinzip robust und nicht zu kompromittieren.
- **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

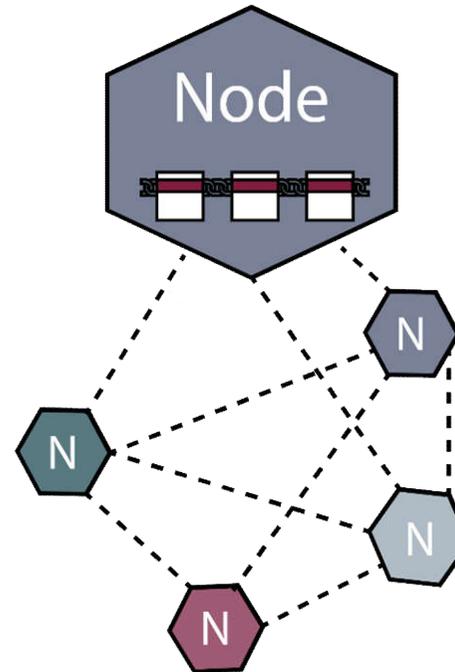
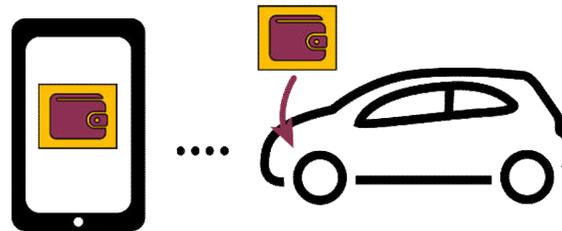
→ Berechtigungsarchitektur

		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> 

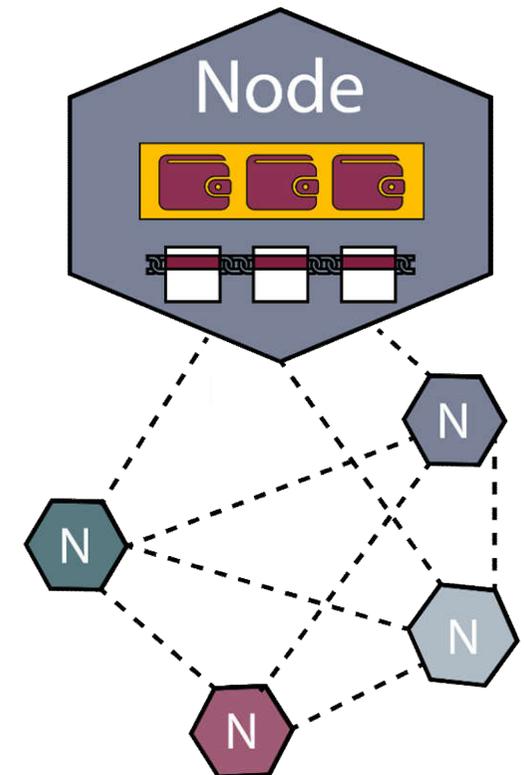
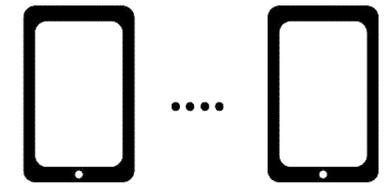
Full Node



Light Node



Service Node



- **Übersicht**
(Chancen, Sichtweiten, Tools)
- **Elemente, Prinzipien, Architekturen, ...**
(Daten, Transaktionen, Block, ..., verteilt, Konsens, ...)
- **Anwendungen**
(Bitcoin, Smart Contracts, Diamantenhandel, ...)
- **Sicherheitsherausforderungen**
(Kryptosystem, Schlüsselspeicherung, Anzeige, ...)
- **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 2017
- 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 = 6.538 €, 16,65 Mio. Bitcoins, 108 Mrd. € Kapitalisierung – 05.11.17)

BlockChain Anwendungen

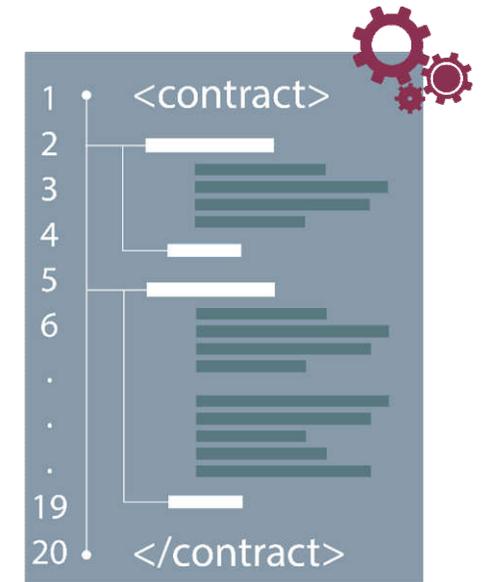
→ Smart Contracts

■ 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.



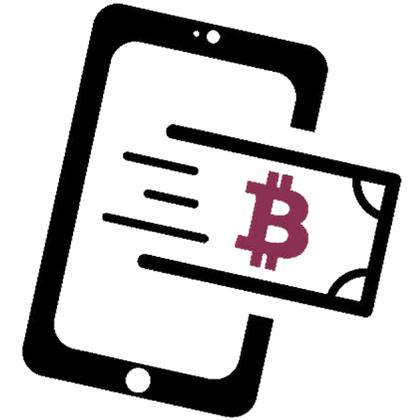
Beispiel:

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

Blockchain Anwendungen

→ Geld- und Wertpapiertransfer: USC

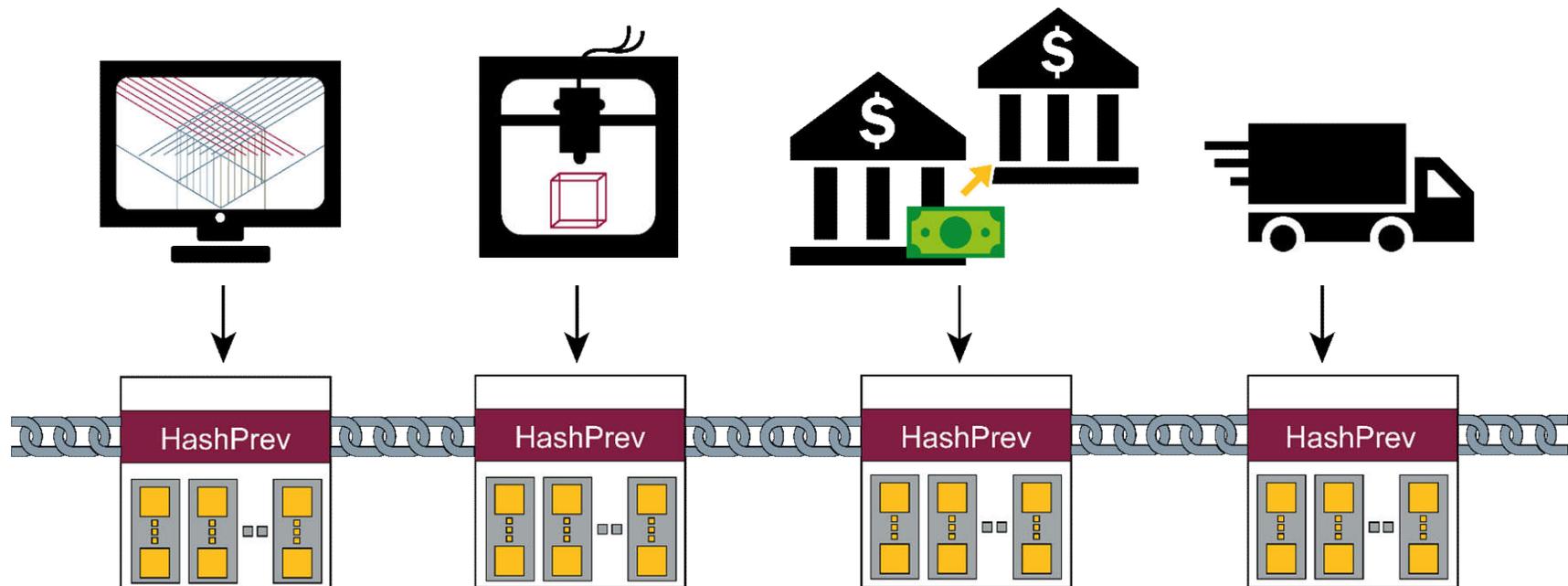
- **Idee:**
 - Eine **digitale Währung** (Utility Settlement Coin – USC), die für den Handel an der Börse mit dem Ziel genutzt werden soll, Clearinggesellschaften zu ersetzen (*UBS, Deutsche Bank, Santander, BNY Mellon, Icap*).
- **Hintergrund:**
 - Die Transaktionskette bei einem Wertpapierhandel z.B. mit einer Aktie, bis diese komplett in den Besitz des Käufers übertragen wurde, ist sehr komplex.
 - Auch wenn der Aktienhandel eigentlich in Sekundenschnelle abläuft, benötigt die vollständige Abwicklung dahinter bislang noch rund zwei Tage.
- **Verfahren:**
 - Das **Geld** und **Wertpapiere** werde sofort durch einen neu hinzugefügten Block ausgetauscht (*private permissioned Blockchain*).
 - Smart Contracts regeln dabei die automatische Überweisung der USC des Käufers an den Verkäufer.



BlockChain Anwendungen

→ Supply Chain

- **Idee:** Automatische Produktions-, Bezahl- und Lieferkette.
- **Ablauf**
 - Nach der Bestellung wird die **Konstruktion** des gewünschten Teils an die **BlockChain** gesendet (one time use only)
 - **Produktion:** Das Teil wird gedruckt (pay per use)
 - Nach dem Druck läuft die **Zahlung** automatisch.
 - Das gedruckte und bezahlte Teil ruft den **Versanddienst** automatisch.

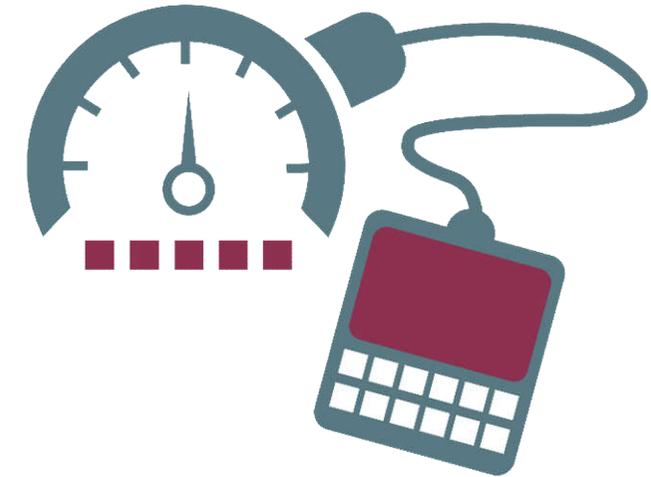


Blockchain Anwendungen

→ Manipulationssicherheit von Tachometern

■ Idee:

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



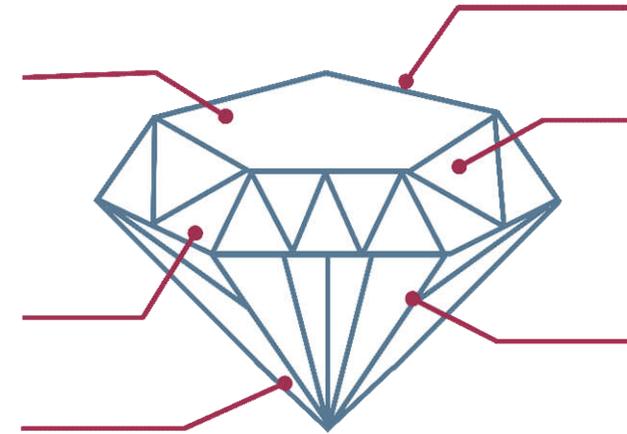
■ Verfahren:

- 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.



- **Übersicht**
(Chancen, Sichtweiten, Tools)
- **Elemente, Prinzipien, Architekturen, ...**
(Daten, Transaktionen, Block, ..., verteilt, Konsens, ...)
- **Anwendungen**
(Bitcoin, Smart Contracts, Diamantenhandel, ...)
- **Sicherheitsherausforderungen**
(Kryptosystem, Schlüsselspeicherung, Anzeige, ...)
- **Zusammenfassung**
(Chancen und Risiken)

- Das verwendete **Public-Key-Verfahren** und die **Hashfunktionen** müssen dem **Stand der Technik** genügen und die passenden Schlüssellängen müssen verwendet werden (*gilt für alle Sicherheitssysteme*).

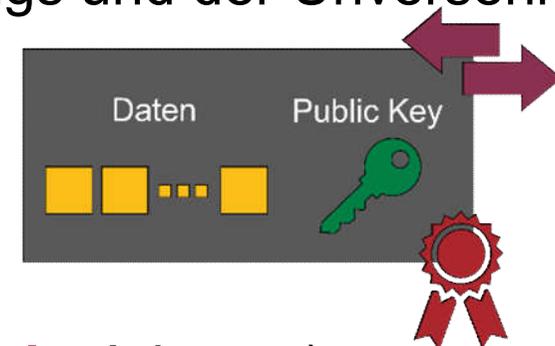
- **Public-Key Verfahren**

- Dient der **Signierung / Verifizierung** von Transaktionen
- Überprüfbarkeit der Echtheit, des Ursprungs und der Unversehrtheit der gespeicherten Daten (**Transaktionen**)



- **Hashfunktionen**

- Dienen der **Adresserzeugung** (**BlockChain**-Adresse)
- Notwendig für die **Verkettung** der **Blöcke** (**HashPrev**)
- Werden für die **Merkle Tree** der **Transaktionen** benötigt, um diese **verifizieren** zu können

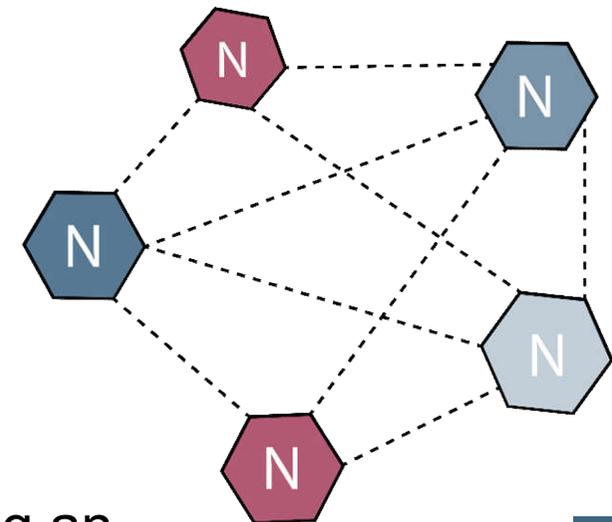


- **Kryptographische Verfahren und Schlüssellängen**, die für die nächsten 10 Jahre als sicher gelten:
 - **BSI – Technische Richtlinie**
„Kryptographische Verfahren: Empfehlungen und Schlüssellängen“
 - **SHA-2/SHA-3** mit einer Mindestschlüssellänge von 256 Bit
Hashfunktionen
 - **RSA** mit einer Schlüssellänge von mindestens 3.000 Bit
Public-Key Verfahren
 - **ECDSA** (elliptische Kurven) mit einer Mindestschlüssellänge von 256 Bit
Public-Key Verfahren
 - Außerdem müssen langfristig **Post-Quantum-Kryptoverfahren** berücksichtigt und genutzt werden (*noch länger als 10 Jahre*).
- Die größten **BlockChains** heutzutage (Bitcoin, Ethereum) nutzen kryptographische Verfahren, die diesen Richtlinien entsprechen

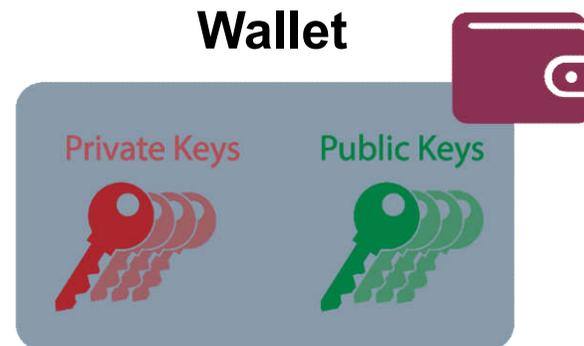


- Um **längerfristig** als **sicher** zu gelten, muss eine **BlockChain** ihre kryptographischen Verfahren **updaten**
 - Erweist sich aufgrund der dezentralen Strukturen als **schwierig**
→ Keine zentrale Instanz kann mehr verpflichtende Updates einspielen
- **Keine** einzige **Transaktion** in der Blockchain ist mehr **vertrauenswürdig**, wenn die kryptographischen Verfahren nicht mehr sicher sind
→ Ein **HardFork** ist erforderlich
 - Update, das **nicht abwärtskompatibel** ist
 - Alle Teilnehmer müssen dies akzeptieren, damit es sich durchsetzt
- Alle Teilnehmer müssen ihre **Transaktionen** an Adressen der neuen, **sicheren BlockChain** senden
- Die **Lebensdauer** einer **BlockChain** muss von Anfang an berücksichtigt werden.

Peer-to-Peer Netzwerk



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



- Der **private Schlüssel** muss geheim bleiben
 - Wer immer den **privaten Schlüssel** einer **Wallet** besitzt, ist in der Lage, über die gesamten **Transaktionen** der **Wallet** zu verfügen
- Ein **Verlust** des **privaten Schlüssels** bedeutet gleichermaßen, dass sämtliche in der Adresse gespeicherten **Transaktionen** für immer „**verloren**“ sind

Blockchain

→ Schlüsselspeicherung

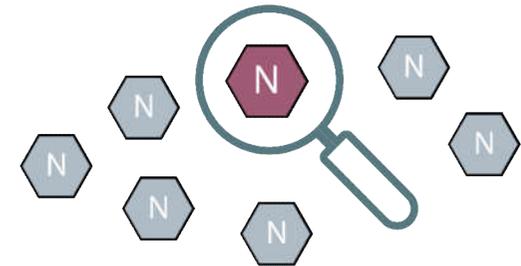
- Eine **sichere Schlüsselspeicherung** ist essentiell
 - Nutzer müssen sensibilisiert werden, was die **Wichtigkeit** der **Schlüsselspeicherung** anbelangt
 - Online **Wallets** bieten zwar Komfort, sind aber auch einfacher anzugreifen!
- **Gefahren** bei nicht ausreichendem Schutz des **privaten Schlüssels**
 - Der **private Rechner** des Nutzers wird **gehackt** (Malware)
 - IoT, z.B. Auto (Light Node) wird **gehackt**
 - 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!**



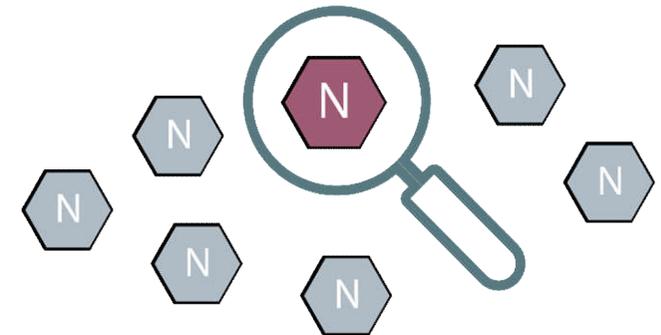
- Für die **BlockChain**-Anwendung muss ein passendes Konsensfindungsverfahren ausgewählt und genutzt werden.
- Außerdem müssen bei den Konsensfindungsverfahren die **Randbedingungen** überprüft werden, damit **keine Manipulation** durchgeführt werden kann
(*Vertrauen ist gut, Kontrolle ist besser*).



- Teilnehmer einer **BlockChain** müssen sich über einen wahren Zustand der **BlockChain** einig werden
- Es existiert keine zentrale Instanz mehr, die diesen Zustand vorgeben kann
- Nutzer der **BlockChain** stimmen ab, welcher **Block** als gültig angesehen werden kann und in die **BlockChain** als nächstes aufgenommen wird
- **Konsensfindung** bietet **Sicherheit** und **Vertrauen**
- Welches **Konsensfindungsverfahren** das beste ist, hängt auch von der Art der **BlockChain** ab
 - **Public** vs. **Private**, **permissionless** vs. **permissioned**



- **Proof of Work** ist das momentan am meisten verbreitete **Konsensfindungsverfahren**
 - bewährtes Verfahren, **robust** und **sicher**
 - **aber: skaliert** schlecht!
Stetig steigender **Rechenaufwand** und **Energieverbrauch**
- **Proof of Stake** ist die zurzeit vielversprechendste Alternative für **BlockChains**
 - Keine Probleme bei der **Skalierbarkeit**, geringer Energieverbrauch
 - Ist allerdings **noch nicht** so lang **erprobt**
- Es gibt noch **viele** weitere **Ansätze**



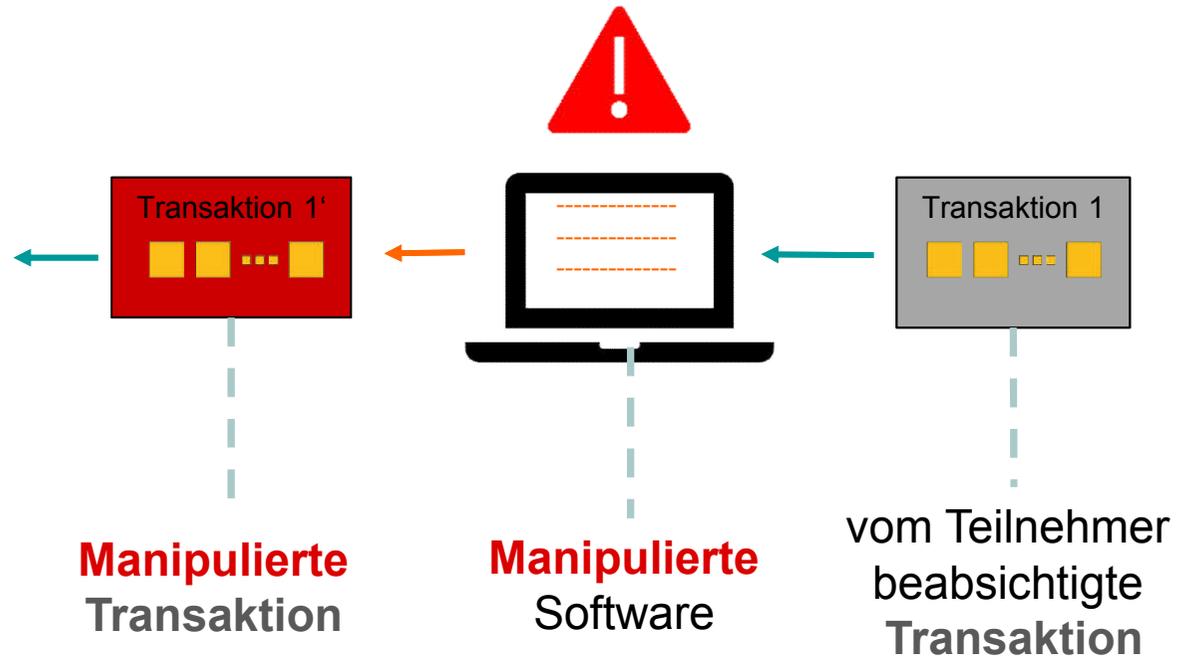
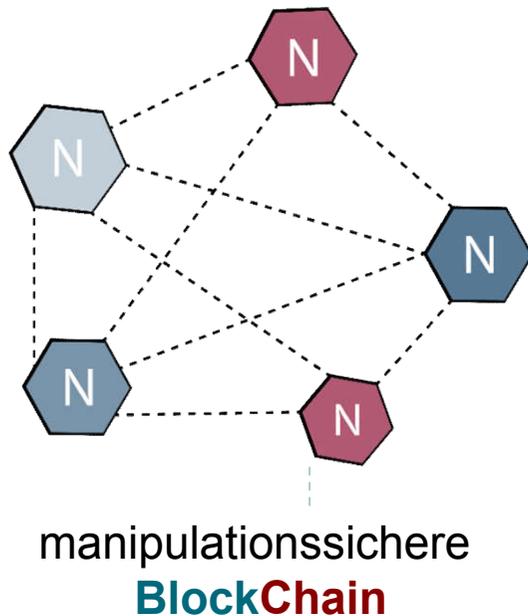
- Ein weiterer wichtiger Punkt ist die **vertrauenswürdige Anzeige** der Transaktionsdaten.



Hierzu werden einfache und vertrauenswürdige **BlockChain**-Viewer benötigt.

- Aber auch die **BlockChain**-Anwendung muss manipuliertsicher sein, damit keine erfolgreichen Angriffe umgesetzt werden können.

- Alle **Sicherheit** der **Blockchain** bringt **nichts**, wenn die Anwendungssoftware manipuliert werden kann, weil sie unsicher ist
- Während die **Blockchain** selbst nicht angreifbar ist, können **Hacker** die Anwendungssoftware manipulieren, mit der Teilnehmer der **Blockchain** Transaktionen tätigen

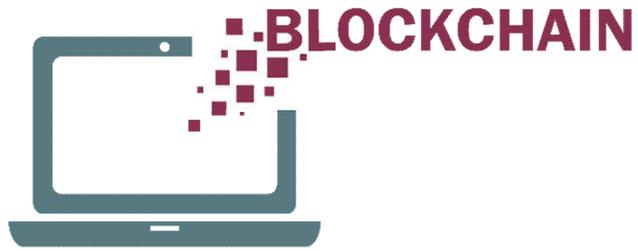


- **Übersicht**
(Chancen, Sichtweiten, Tools)
- **Elemente, Prinzipien, Architekturen, ...**
(Daten, Transaktionen, Block, ..., verteilt, Konsens, ...)
- **Anwendungen**
(Bitcoin, Smart Contracts, Diamantenhandel, ...)
- **Sicherheitsherausforderungen**
(Kryptosystem, Schlüsselspeicherung, Anzeige, ...)
- **Zusammenfassung**
(Chancen und Risiken)

BlockChain

→ Zusammenfassung

- **BlockChain-Anwendungen**
 - 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**
 - **Stand der Technik** (Post-Quantum-Kryptoverfahren)
 - **Sichere Speicherung von Keys** (Wallets)
 - **Vertrauenswürdige Anzeige-Komponente** von **BlockChain** Daten (*Trusted Viewer*)
 - **Vertrauensmodelle** (Validierungsalgorithmen)
 - **Rechtsrahmen** für neue Geschäftsmodelle und Ökosysteme



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Die **BlockChain**

Potenziale, Chancen und Risiken der Querschnittstechnologie

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/UCEMkJHjW9dHcWfek_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 Wahrung – 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 fur 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>