

**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# BlockChain

**Idee, Konzepte, Mechanismen 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**  
(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

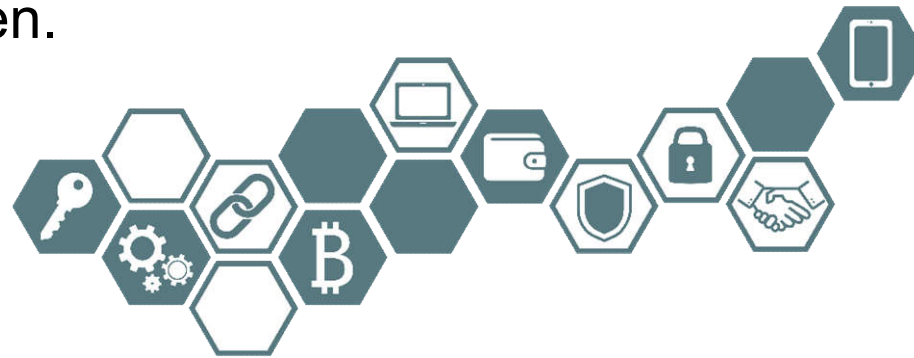
(Chancen, Sichtweiten, Tools)

- **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-Technologie

## → Verteilte Datenbank/Collaboration-Tool

### ■ BlockChains

- sind **fälschungssichere**, *kryptographische Verfahren*
- **verteilte, redundante** Datenstrukturen *Vielzahl von Teilnehmern gespeichert*
- in denen **Transaktionen** in der Zeitfolge protokolliert *Art der Verkettung*
- **nachvollziehbar, unveränderlich** und *jeder kann Kryptographie überprüfen*
- **ohne zentrale Instanz** abgebildet sind. *geeignete Konsensfindungsverfahren*

**BlockChain** → „**programmiertes Vertrauen**“

### ■ BlockChain-Technologie

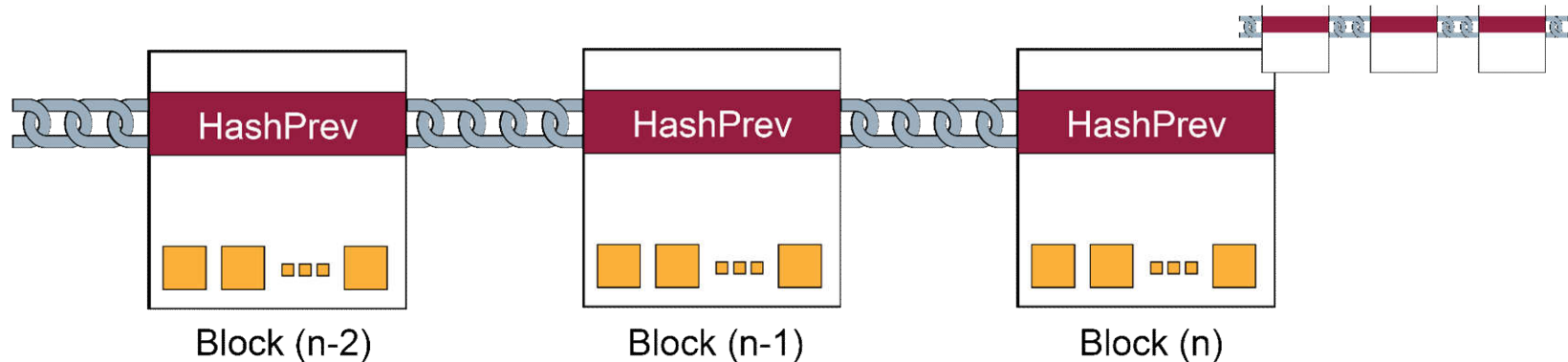
- Lassen sich **Eigentumsverhältnisse** (digital Assets)
- **direkter** und **effizienter** als bislang **sichern** und **regeln**,
- da eine **lückenlose** und **unveränderliche Datenaufzeichnung** hierfür die Grundlage schafft.
- Alle **Beglaubigungsprozesse** werden *schneller*, sicherer und *billiger*.

- **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** (*wie Datenbank*)



- 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 jedem Teilnehmer (Node) und damit verteilt und redundant vorhanden (**alle Nodes müssten Manipulationen werden**).
- Eine **Blockchain** kann sehr groß sein (z.B. Bitcoin etwa **115 G Byte** – Stand: Mai 2017)

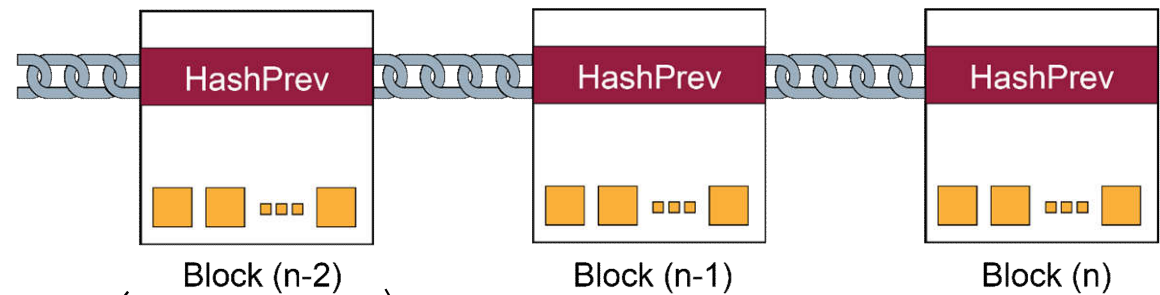


# Blockchain

## → 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  ...

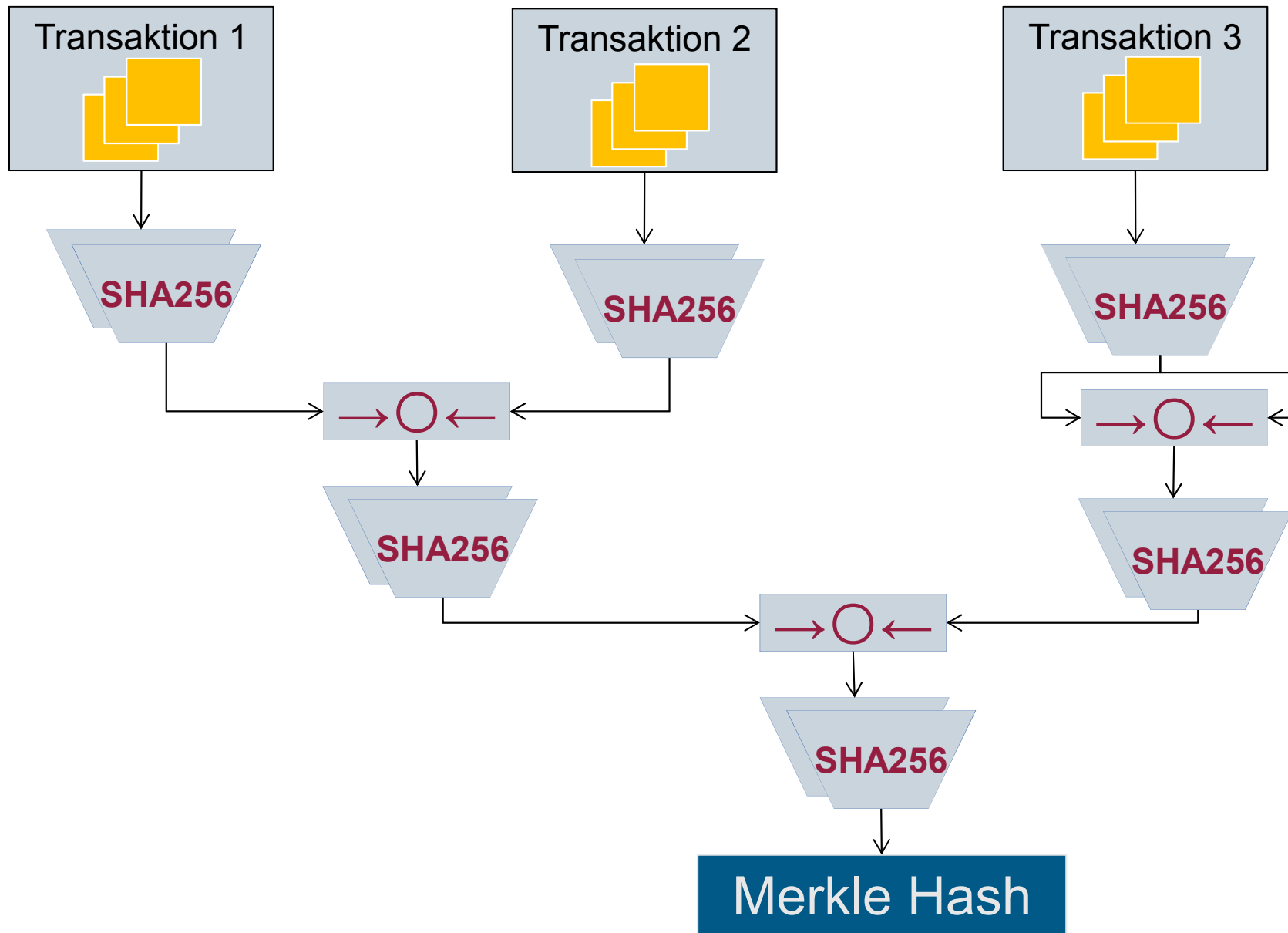
### Block Header

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

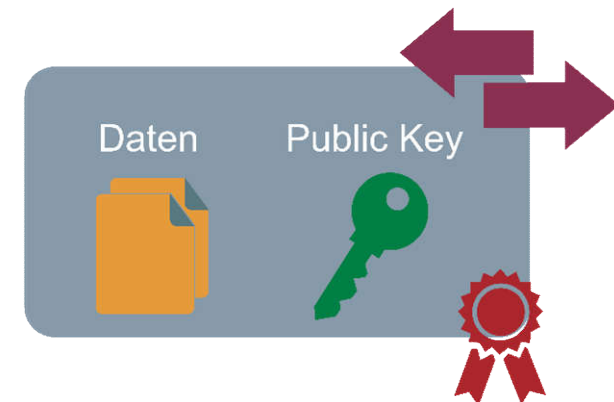
- Ein **Block** wird mit einem Hashwert geschützt (**Merkle Root Hash** - siehe nächste Folie) und mit dem Hashwert des vorherigen Block (**HashPrev**) verbunden

# Blockchain

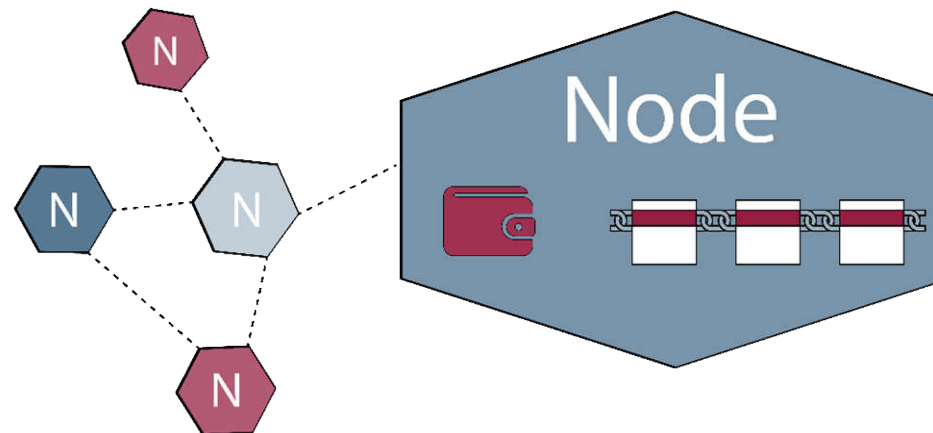
## → Merkle Hash (einfaches Beispiel)



- **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 von der erstellenden Node 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**.



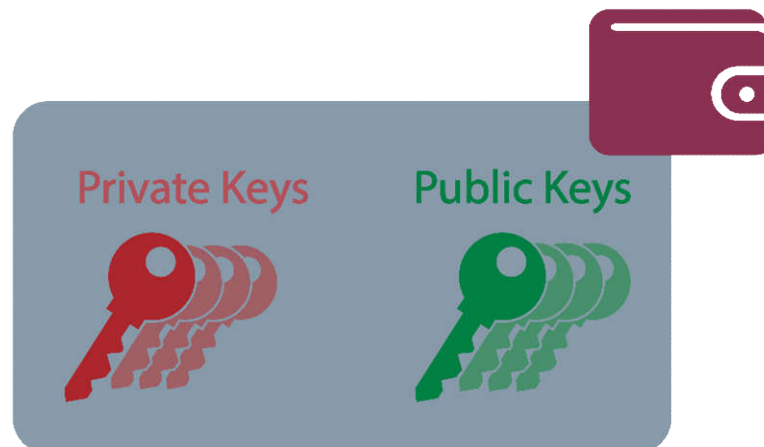
- Jeder, der an der „**Blockchain**“ teilnimmt, wird als „**Node**“ beziehungsweise „Teilhaber“ bezeichnet.
- Jede Node erhält eine **aktuelle Kopie** der **Blockchain**, die fortlaufend aktualisiert wird.
- Jede Node, die zu einer „**Blockchain**“ gehört, falls diese nicht eingeschränkt ist, hat im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



# Blockchain

## → Element: Wallet

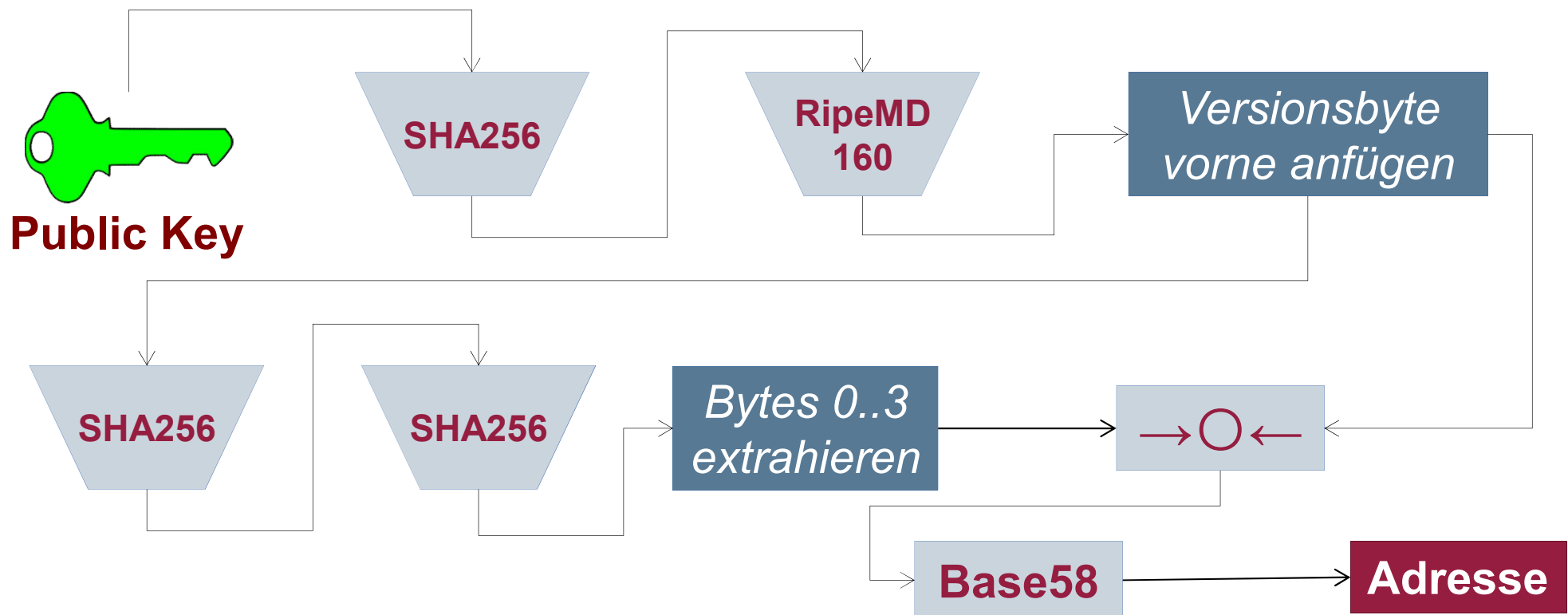
- Jede Node verfügt über eine „**Wallet**“.
- Eine **Wallet** ist dabei eine Datenstruktur, in der die eigenen **Private- und Public-Keys** der Node **sicher** gespeichert sind.
- Aus dem Public-Key wird mit Hilfe einer Funktion die **eindeutige Kennung (Adresse) einer Node** berechnet (siehe nächste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



# Wallets

## → Berechnung der BlockChain-Adresse

- Als **BlockChain**-Adresse wird nicht der öffentliche Schlüssel verwendet, allerdings berechnet sie sich daraus:

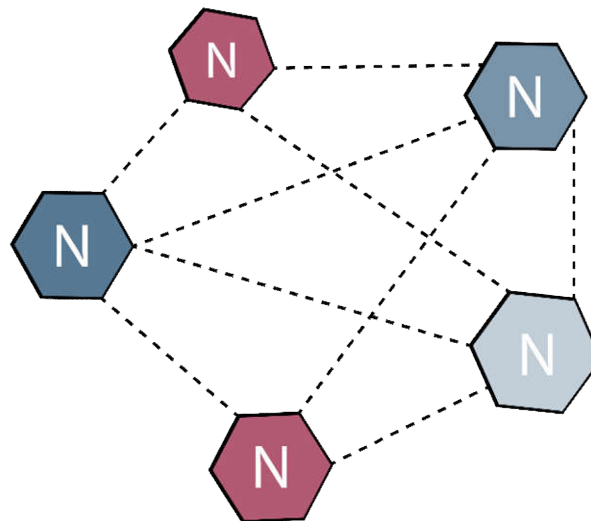


- Adressen sind pseudonym
- Pseudonymität kann nur selber aufgehoben werden, z.B. an **Schnittstellen zu Zahlungssystemen**

## → 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

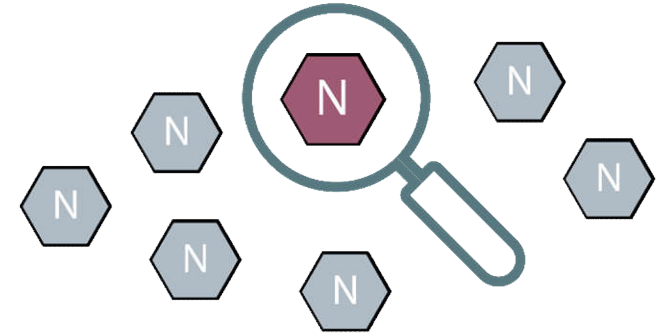


- Alle **Transaktionen** werden von den entsprechenden Nodes signiert, die für die **Daten** verantwortlich sind und an alle anderen Nodes über das Peer-to-Peer-Netzwerk verteilt.
- Ein **Konsensfindungsverfahren** bestimmt, welche Node einen neuen Block validieren und an die **BlockChain** „hängen“ 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 (jeder Teilnehmer) 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.





- 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
    - ...



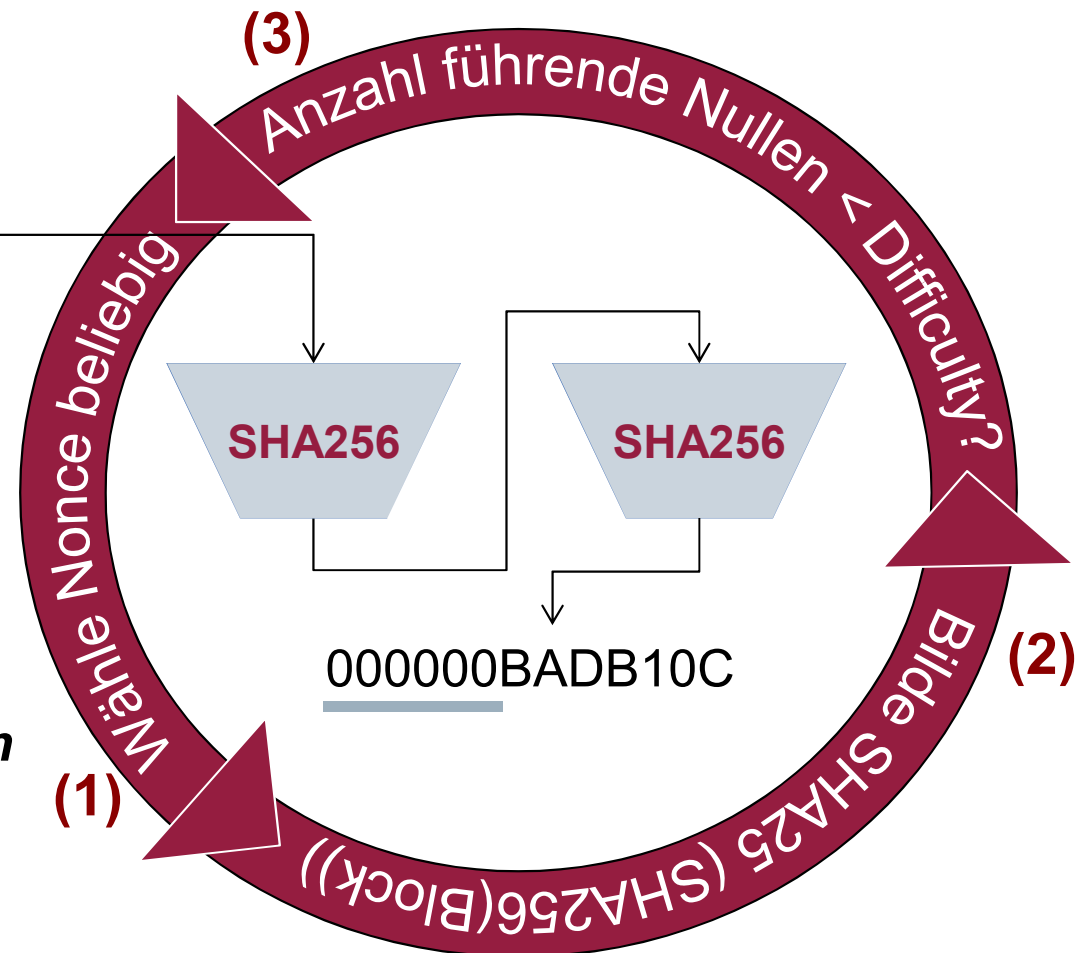
# Mining (Proof of Work)

## → 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



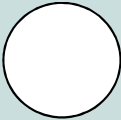



### Challenge

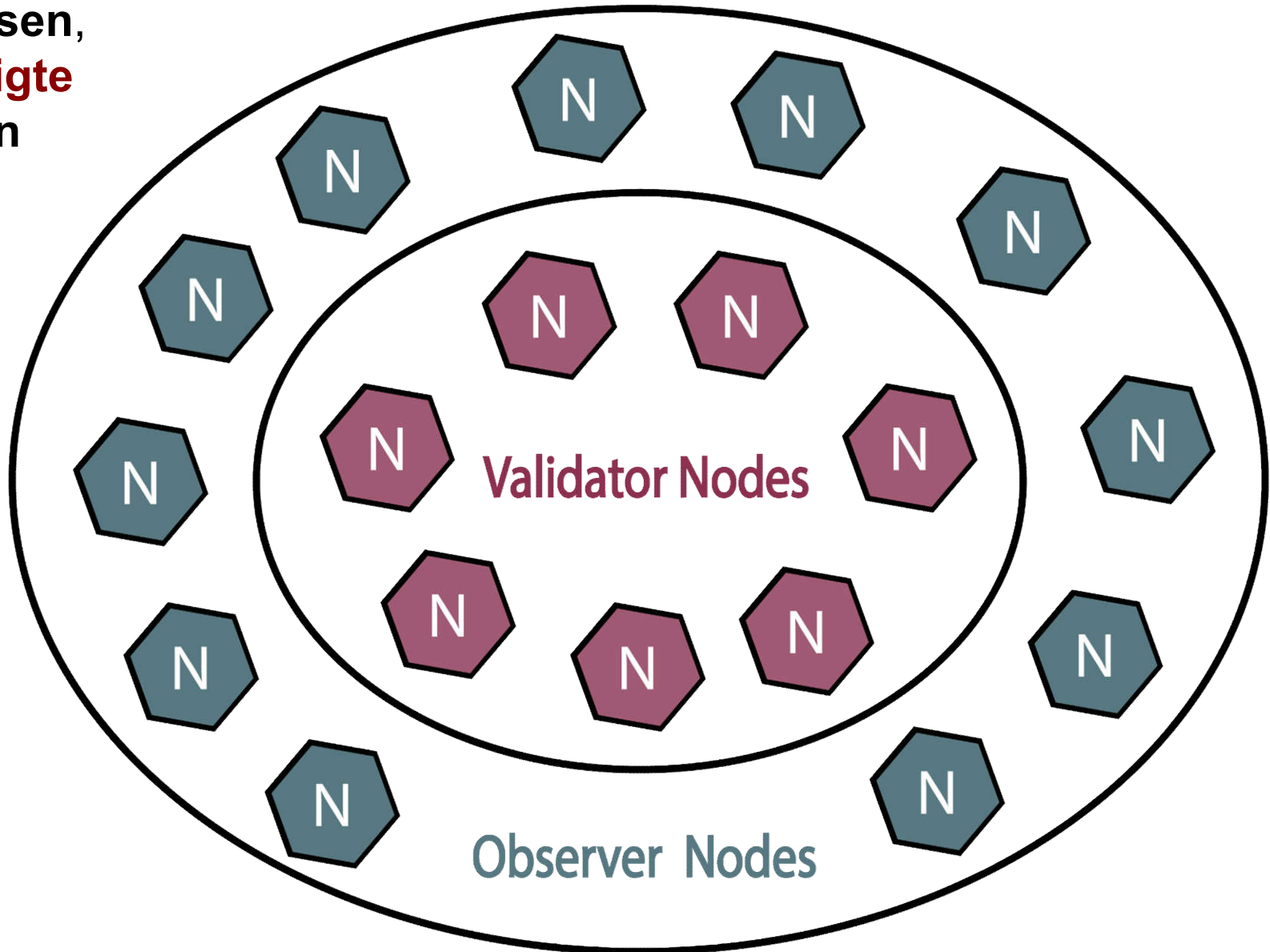
Ist die **Anzahl der führenden Nullen** größer oder gleich der **Difficulty**, gilt der Block als geschürft und wird im P2P-Netzwerk verteilt.

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

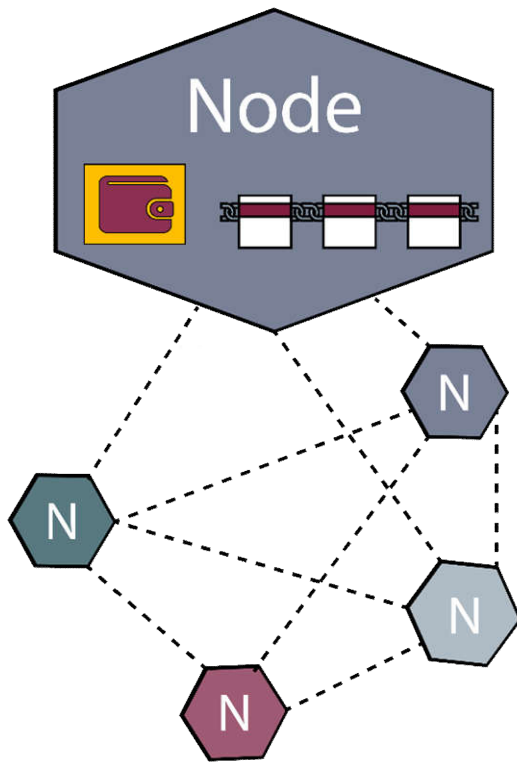
- **Die Challenge kostet sehr viel Energie:**
  - 2,8 Mio. US-Dollar pro Tag (Stromkosten)
  - 1,3 Giga-Watt
  - das sind ca. 10 US-Dollar pro **Transaktion**
- Solange eine **Node nicht die Mehrheit an Miner-Kapazitäten besitzt** (mehr als 50%), ist das Mining-Prinzip robust und nicht zu kompromittieren.
- **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.

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

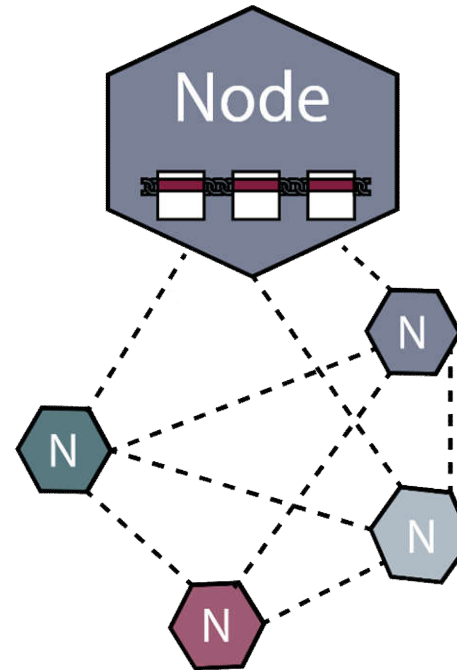
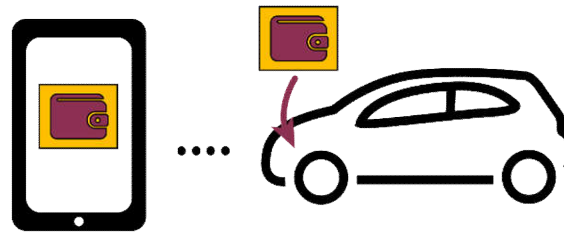
Jeder darf lesen,  
nur **Berechtigte**  
validieren



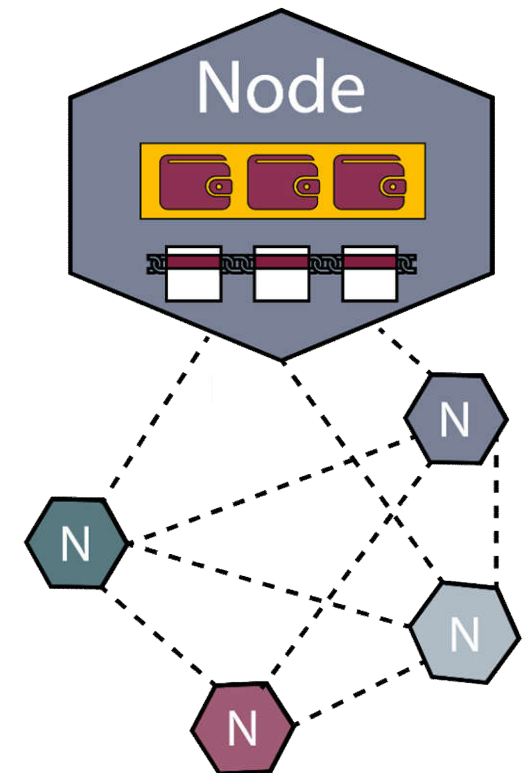
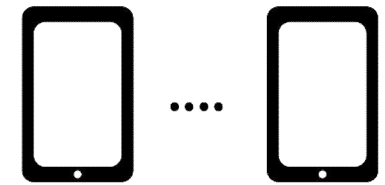
### Full Node



### Light Node



### Service Node



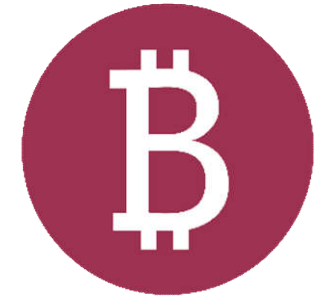
- **Übersicht**  
(Chancen, Sichtweiten, Tools)
- **Elemente, Prinzipien, Architekturen, ...**  
(Daten, Transaktionen, Block, ..., verteilt, Konsens, ...)
- **Anwendungen**  
(Bitcoin, Smart Contracts, Diamantenhandel, ...)
- **Sicherheitsherausforderungen**  
(Kryptosystem, Schlüsselspeicherung, Anzeige, ...)
- **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 = 4.750 \$, 16,65 Mio. Bitcoins, 78 Mrd. \$ Kapitalisierung – 17.10.17)



# 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

## → 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

## → Elektronische Auktion

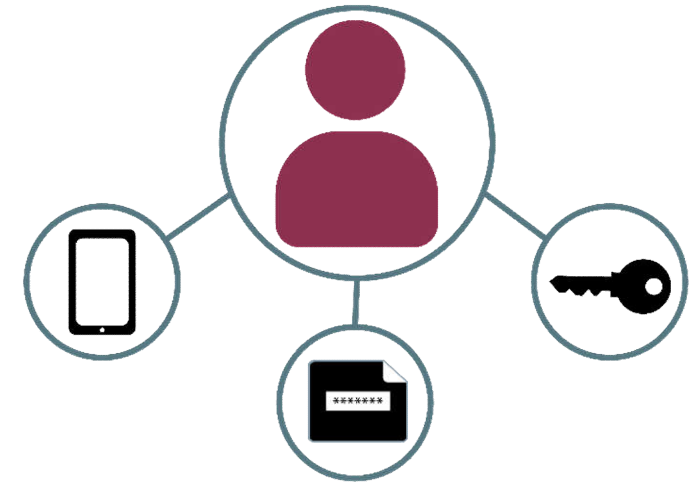


- **Idee:**
  - Einfache und sichere Auktion
- **Verfahren:**
  - Die **BlockChain** fungiert als eine private Handelsplattform.
  - Es können **Anfangsgebote für Objekte** durch Auktionäre gesetzt werden.
  - Interessierte können ihre Gebote einspielen.
  - Alle können immer den Verlauf der Auktion in der **BlockChain** beobachten.
  - Nach der Auktion wird die **BlockChain** geschlossen
  - ...

# BlockChain Anwendungen

## → Identity Management

- **Idee:**
  - Die **Identität** wird von jedem **Nutzer selber verwaltet.**
  - Identifikation von **Geräten im IoT** oder Identity & Access Management von Mitarbeitern im **Unternehmensumfeld.**

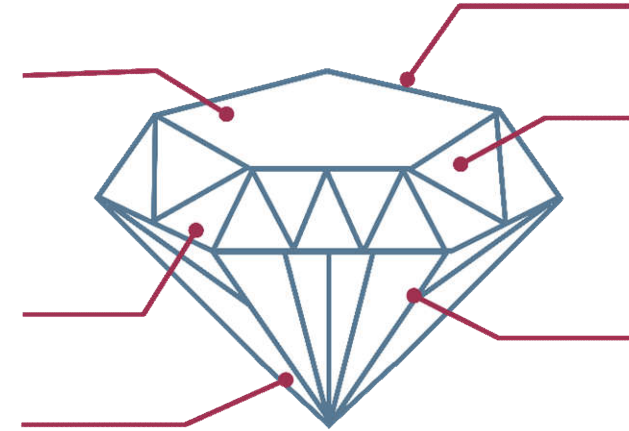


- **Verfahren:**
  - Eine bei Nutzer und Diensten etablierte „ID“- **BlockChain**“ bietet die Möglichkeit eines echten „**Bring Your Own Identity**“
  - Neuartiger Identitätsstandard, in denen der Nutzer selbst die vollständige Kontrolle über seine **persönlichen Daten** hat und souverän deren Weitergabe entscheidet.

# 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 **Hashfunktion** müssen dem **Stand der Technik** genügen und die passenden Schlüssellängen müssen verwendet werden.

Außerdem muss langfristig **Post-Quantum-Kryptoverfahren** berücksichtigt und genutzt werden.



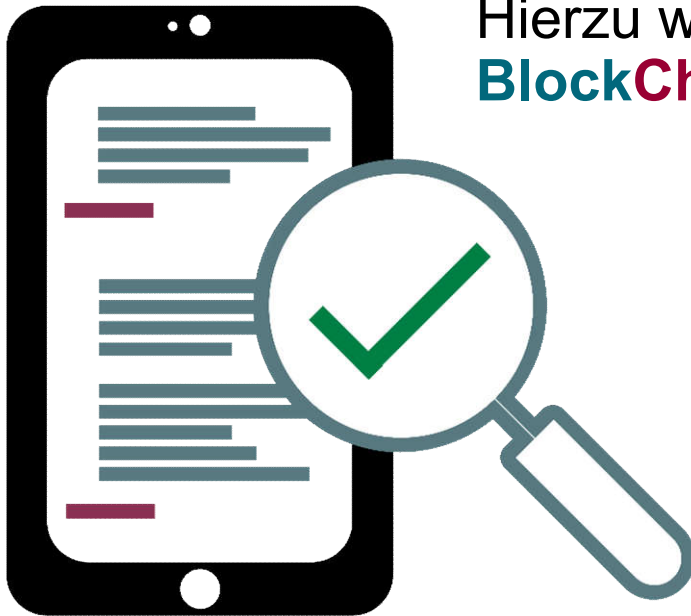
- Die Sicherheit der **BlockChain**-Technologie hängt auch von der **Geheimhaltung der privaten Schlüssel** der Public-Key-Verfahren ab.

Der Schutz des privaten Schlüssels sollte mit Hilfe von **Hardware-Security-Module** realisiert werden (SmartCards, Sec-Token, High-Level-Sicherheitsmodule).





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



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



- Außerdem müssen bei den Konsensfindungsverfahren die **Randbedingungen** überprüft werden, damit **keine Manipulation** durchgeführt werden kann (*Vertrauen ist gut, Kontrolle ist besser*).

- **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

- Lassen Sie uns die **passenden Anwendungen** auswählen und den **Digitalisierungsprozess** mit modernen und pragmatischen IT-Technologien **beflügeln**.
  
- **Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung!**

**BlockChain** → „**programmiertes Vertrauen**“



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# BlockChain

## Idee, Konzepte, Mechanismen 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**

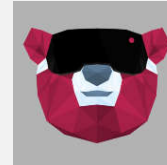


securityNews



- **7. Sinn im Internet (Cyberschutzraum)**  
[https://www.youtube.com/channel/UCEMkJW9dHcWfek\\_En3xhjg](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>