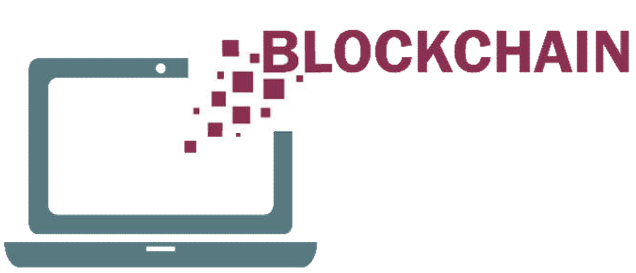


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

BlockChain - 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
→ Sicherheits- und Vertrauensdienst (1/2)

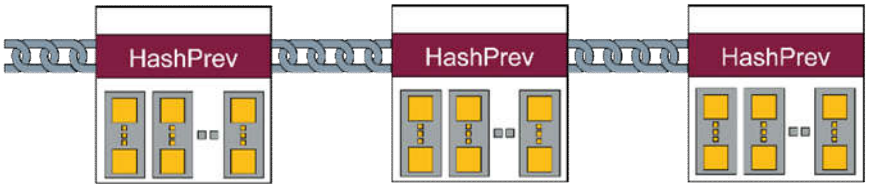
- Für einen **Informatiker** ist die **BlockChain** eine **einfache Datenstruktur**, die Daten sind in einzelnen „Blöcken“ verkettet und in einem ***verteilten Netz*** **redundant** (mehrfach) verwaltet.

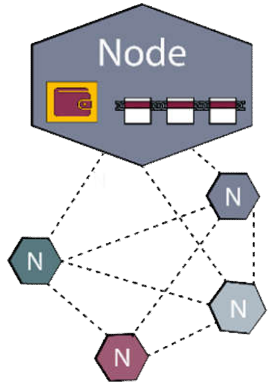
- Für die **IT-Sicherheitsexperten** hat die **BlockChain** den Vorteil, dass die **Daten** in den einzelnen „Blöcken“ **manipulationssicher gespeichert** werden können, das heißt, die Teilnehmer an der **BlockChain** sind in der Lage,
  → die **Echtheit**,
  → den **Ursprung** und
  → die **Unversehrtheit der gespeicherten Daten (Transaktionen)** zu überprüfen.

- Für den **Anwendungsdesigner** bedeutet die Nutzung der **BlockChain**-Technologie eine **vertrauenswürdige Zusammenarbeit** zwischen **verschiedenen Organisationen**.

BlockChain
→ Sicherheits- und Vertrauensdienst (2/2)

BlockChain

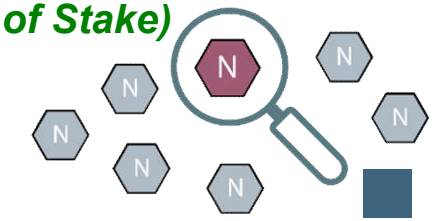




- **BlockChains**
  - sind **fälschungssichere**, *kryptographische Verfahren (Hashfunktionen / Public-Key-Verfahren)*
  - **verteilte**, **redundante** Datenstrukturen *Vielzahl von Teilnehmern gespeichert (jede Note hat die Blockchain gespeichert)*
  - in denen **Transaktionen in der Zeitfolge protokolliert** *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)*

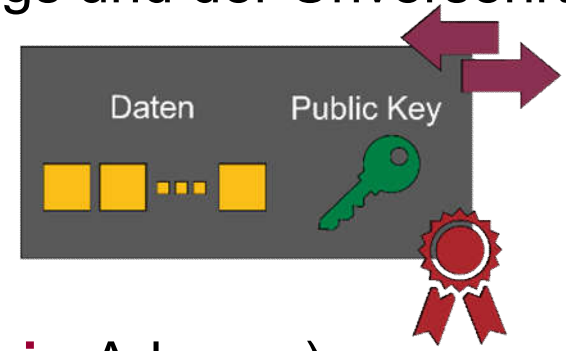


BlockChain → „programmiertes Vertrauen“

BlockChain
→ 1. Sicherheitsherausforderung

- 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

BlockChain
→ Kryptographische Verfahren (1/2)

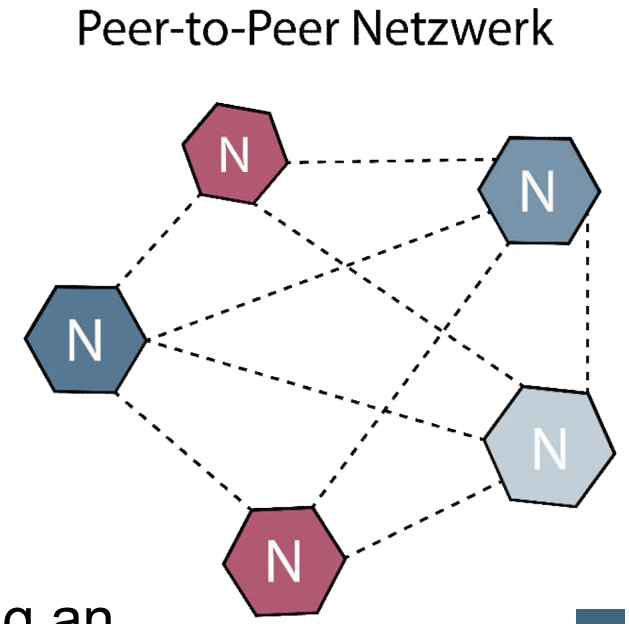
- **Kryptographische Verfahren** und **Schlüssellängen**, die für die nächsten 10 Jahre als sicher gelten:
  - **BSI – Technische Richtlinie** „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“
  - **SHA-2/SHA-3** mit einer Mindestschlüssellänge von 256 Bit
    Hashfunktionen
  - **RSA** 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 **BlockChain**s heutzutage (Bitcoin, Ethereum) nutzen kryptographische Verfahren, die diesen Richtlinien entsprechen

BlockChain
→ Kryptographische Verfahren (2/2)

- 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

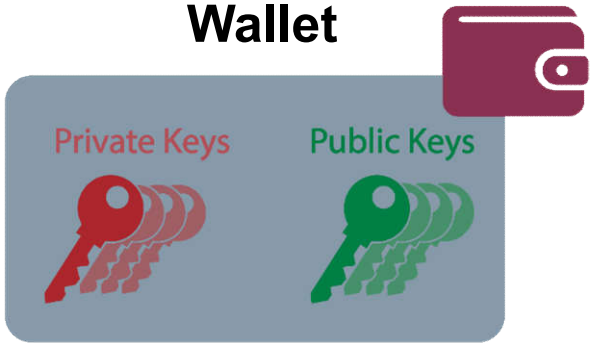


- Alle Teilnehmer müssen ihre **Transaktionen** an Adressen der neuen, **sicheren BlockChain** senden

- Die **Lebensdauer** einer **BlockChain** muss von Anfang an berücksichtigt werden.

BlockChain
→ 2. Sicherheitsherausforderung

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

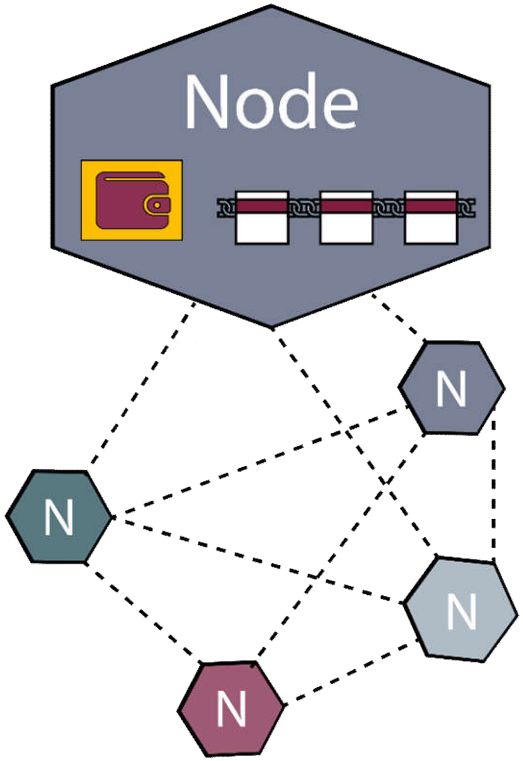


- Der **private Schlüssel muss** geheim bleiben
  - Wer immer den **privaten Schlüssel** einer **Wallet** besitzt, ist in der Lage, über die gesamten **Transaktionen** der **Wallet** zu verfügen

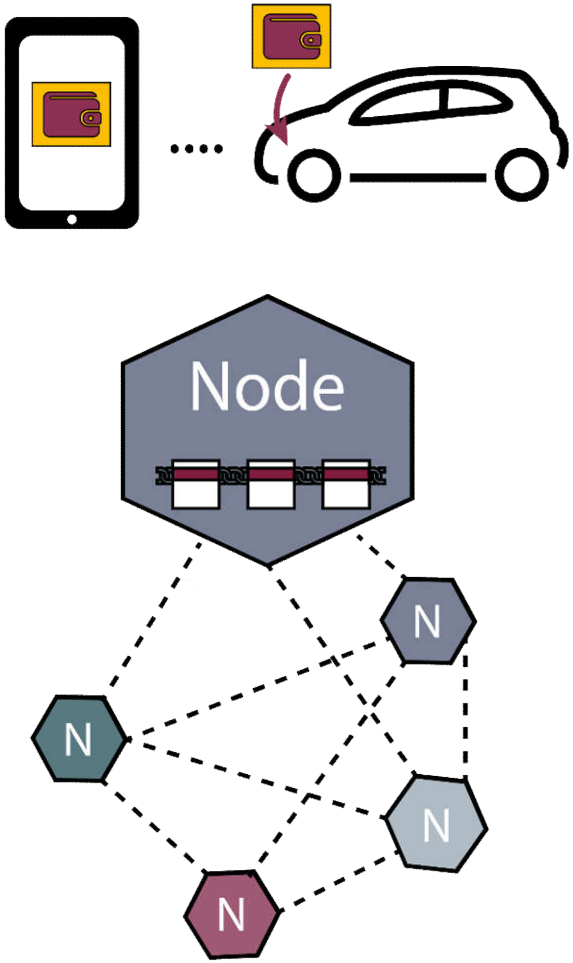
- Ein **Verlust** des **privaten Schlüssels** bedeutet gleichermaßen, dass sämtliche in der Adresse gespeicherten **Transaktionen** für immer „**verloren**“ sind

BlockChain
→ Verschiedene Arten von Nodes/Wallets

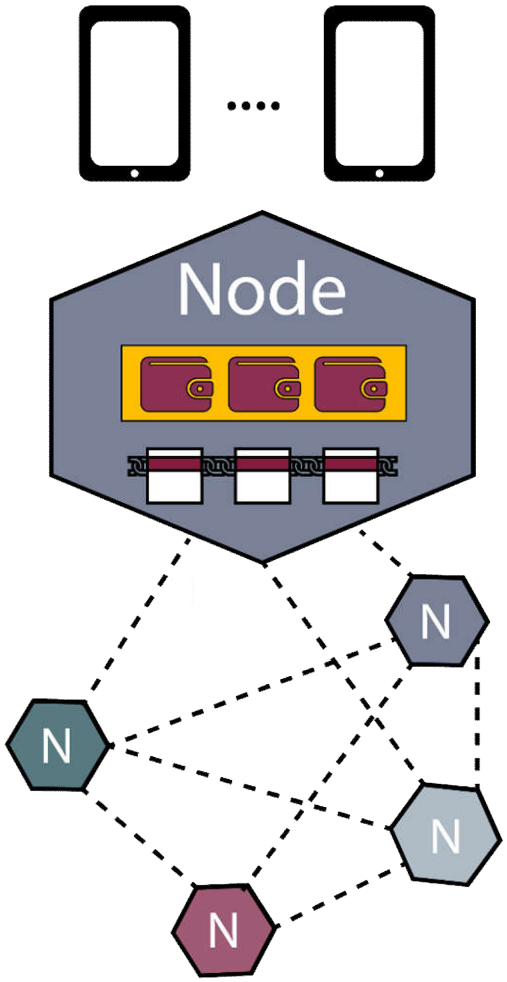
Full Node



Light Node



Service Node



Sicherheitsmodul: TPM, Smartcard, High-Level-SM

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**!

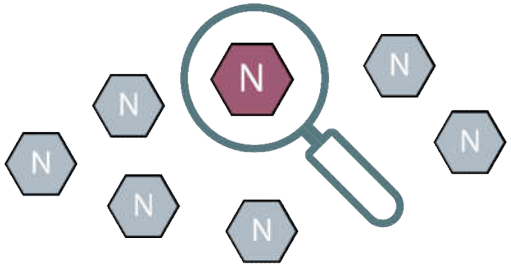
BlockChain
→ 3. Sicherheitsherausforderung

- 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).

BlockChain
→ Konsensfindungsverfahren (1/2)

- **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**



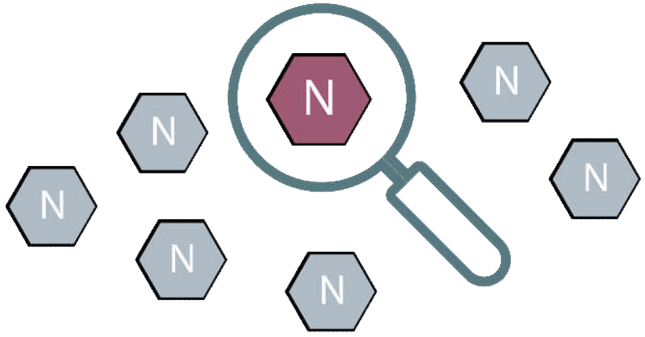
- Welches **Konsensfindungsverfahren** das beste ist, hängt auch von der Art der **BlockChain** ab
  - **Public** vs. **Private**, **permissionless** vs. **permissioned**

BlockChain
→ Konsensfindungsverfahren (2/2)

- **Proof of Work** ist das momentan am meisten verbreitete **Konsensfindungsverfahren**
  - bewährtes Verfahren, **robust** und **sicher**
  - **aber**: **skaliert** schlecht!
    Stetig steigender **Rechenaufwand** und **Energieverbrauch**

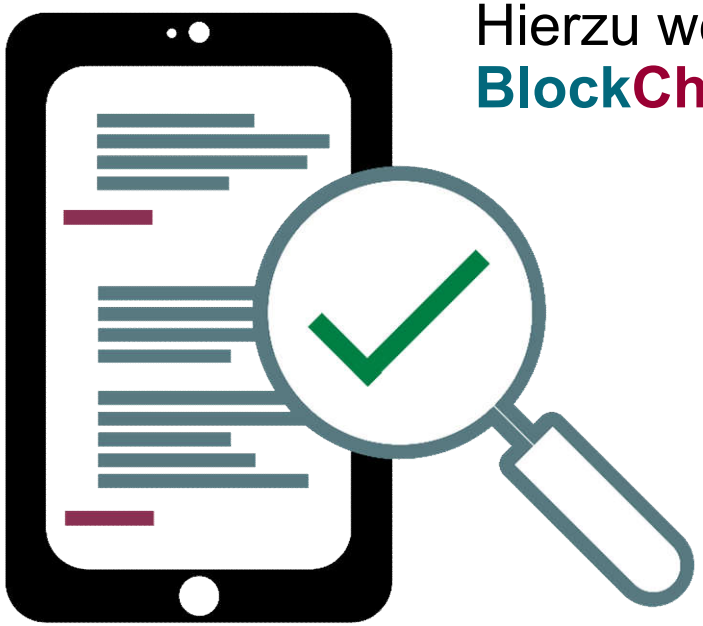
- **Proof of Stake** ist die zurzeit vielversprechendste Alternative für **BlockChain**s
  - Keine Probleme bei der **Skalierbarkeit**, geringer Energieverbrauch
  - Ist allerdings **noch nicht** so lang **erprobt**

- Es gibt noch **viele** weitere **Ansätze**



BlockChain
→ 4. Sicherheitsherausforderung

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

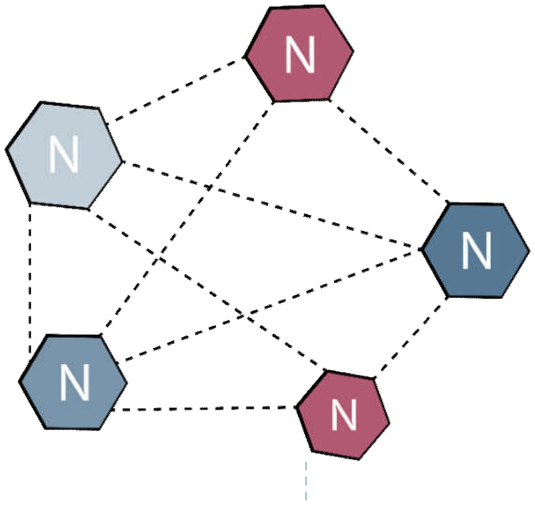


Hierzu werden einfache und vertrauenswürdige **BlockChain**-Viewer benötigt.

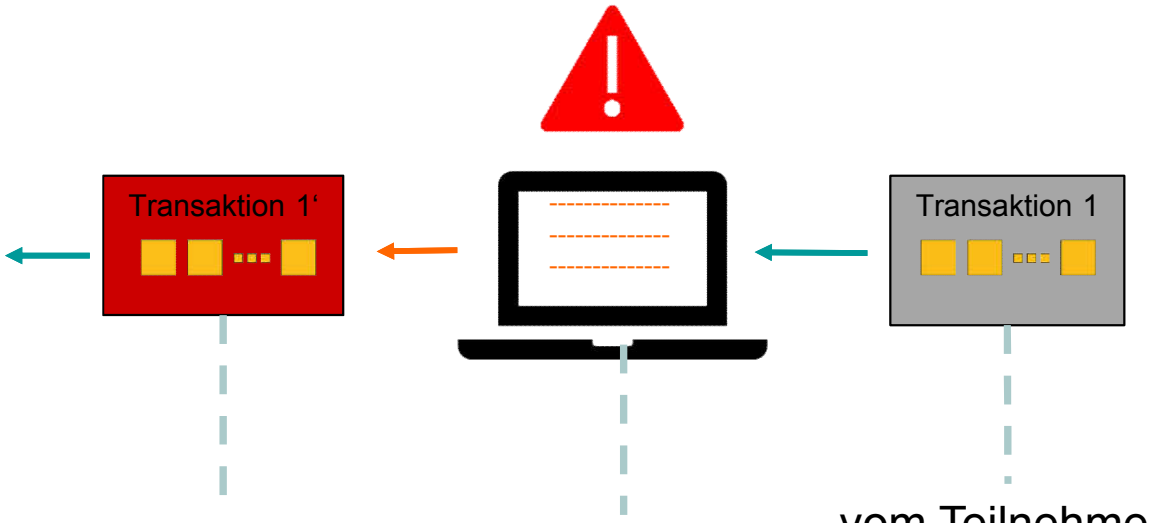
- Aber auch die **BlockChain**-Anwendung muss manipuliersicher sein, damit keine erfolgreichen Angriffe umgesetzt werden können.

BlockChain
→ Vertrauenswürdige Anwendung

- Alle **Sicherheit** der **BlockChain** bringt **nichts**, wenn die Anwendungs-software 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



manipulationssichere **BlockChain**

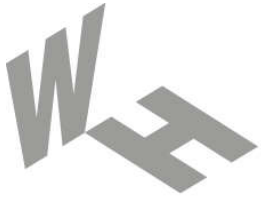


Manipulierte **Transaktion**

Manipulierte Software

vom Teilnehmer beabsichtigte **Transaktion**

Sicherheit der **BlockChain** | **Sicherheit** der **Anwendung**



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

BlockChain - Sicherheit

BlockChain → „programmiertes Vertrauen“

Prof. Dr. (TU NN)
Norbert Pohlmann

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

Anhang / Credits

Wir empfehlen

- **Kostenlose App securityNews**

- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/channel/UCEMkHjW9dHcWfek_En3xhjg
-
- **Cybärcast – Der IT-Sicherheit Podcast**
  https://podcast.internet-sicherheit.de/

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

Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

Google+
https://plus.google.com/107690471983651262369/posts

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/

Literatur

Artikel:

C. Kammler, N. Pohlmann: „Kryptografie wird Währung – Bitcoin: Geldverkehr ohne Banken“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 6/2013
https://norbert-pohlmann.com/app/uploads/2015/08/308-Kryptografie-wird-W%C3%A4hrung-Bitcoin-Geldverkehr-ohne-Banken-Prof-Norbert-Pohlmann.pdf

R. Palkovits, N. Pohlmann, I. Schwedt: „Blockchain-Technologie revolutioniert das digitale Business: Vertrauenswürdige Zusammenarbeit ohne zentrale Instanz“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 2/2017
https://norbert-pohlmann.com/app/uploads/2017/07/357-Blockchain-Technologie-revolutioniert-das-digitale-Business-Vertrauensw%C3%BCrdige-Zusammenarbeit-ohne-zentrale-Instanz-Prof.-Norbert-Pohlmann.pdf

Vortrag:

N. Pohlmann, Security Day 2017, Vortrag: „Blockchain – Idee, Konzepte, Mechanismen und Anwendungen“, Marl, 10.2017
https://norbert-pohlmann.com/app/uploads/2017/10/336-Blockchain-—-Idee-Konzepte-Mechanismen-und-Anwendungen-Prof.-Norbert-Pohlmann.pdf