Blockchain Technologie aus unternehmerischer Perspektive

MTM-Verein, Uni Köln, 6.9.2017

Prof. Wolfgang Prinz, PhD

Fraunhofer FIT
RWTH Aachen

Fraunhofer FIT

Fraunhofer FIT - CSCW
Kooperative Lösungen für die Herausforderungen der Digitalisierung

Fraunhofer FIT

Fraunhofer FIT Blockchain Lab

Business Modell, Technology and Legal

Presentations and tutorials

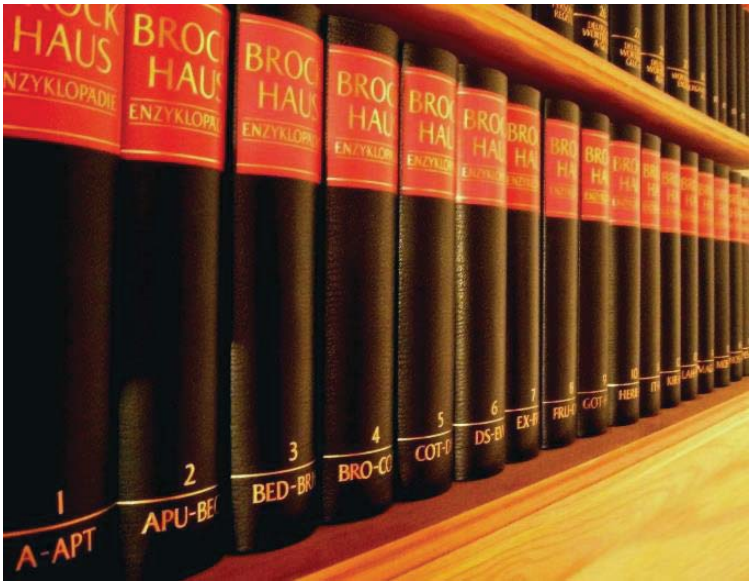
Demonstrators, concepts, POC and advanced solutions

Workshops on technical and business implications

Publications

Fraunhofer FIT

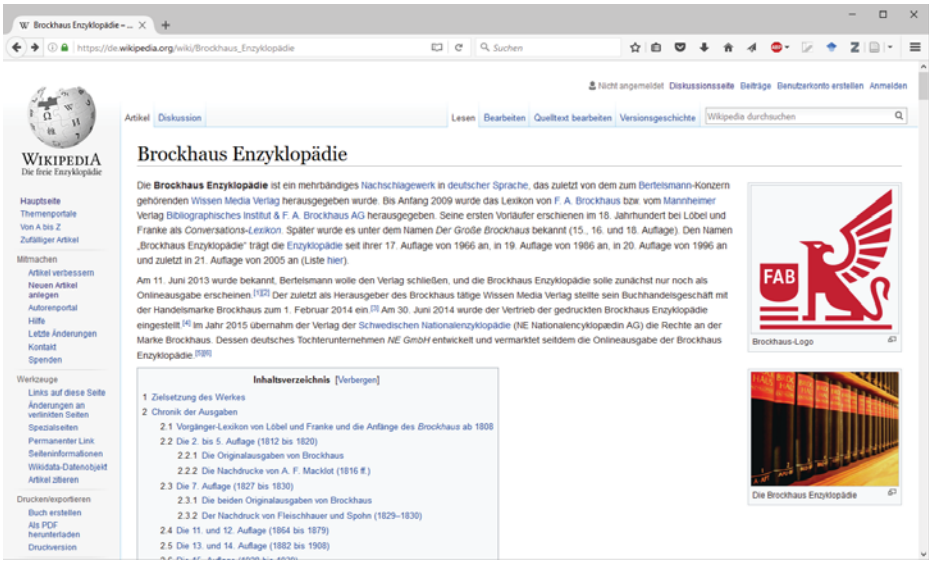
Brockhaus Enzyklopädie



https://upload.wikimedia.org/wikipedia/commons/c/c2/Draft01_wkp.png by Florian Hirzinger

Fraunhofer FIT

Wikipedia

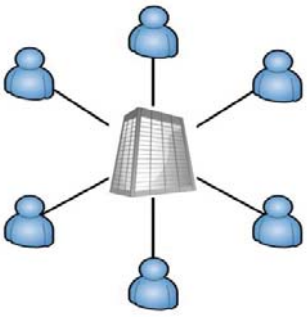


Fraunhofer FIT

Erste Generation des WWW:

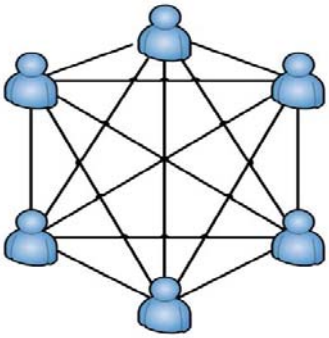
Dezentralisierte Informationserstellung im „Internet of Information“

Brockhaus Enzyklopädie



Zentralisierte Inhaltserstellung

Wikipedia

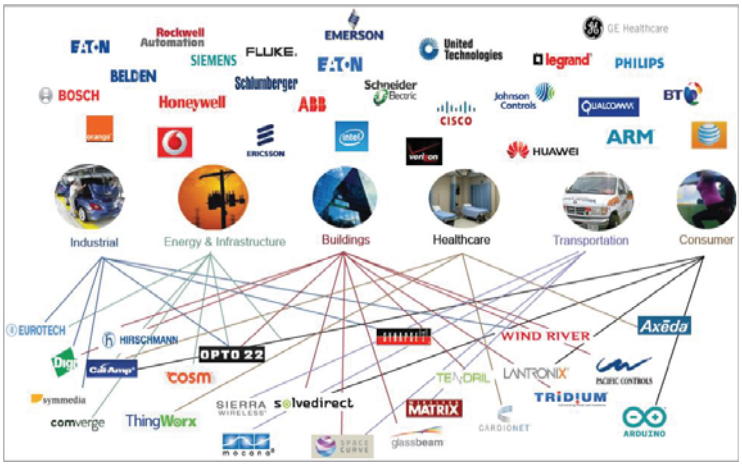


Dezentralisierter Inhaltserstellung

„Konsensbildung in einer Community“

Fraunhofer FIT

Zweite Generation WWW:
Verteilte Dienste im „Internet of Services“



Quelle: http://labs.sogeti.com/digital-disneyfication-m2m-internet-things-means/

Dritte Generation WWW:
Internet of Things

Quelle: http://www.innovationsmanagement.fraunhofer.de/?p=682

Wer garantiert mir eigentlich die Sicherheit einer Transaktion?

Warum wird Vertrauen, Kontrolle, Korrektheit immer noch hauptsächlich von Institutionen gewährleistet?

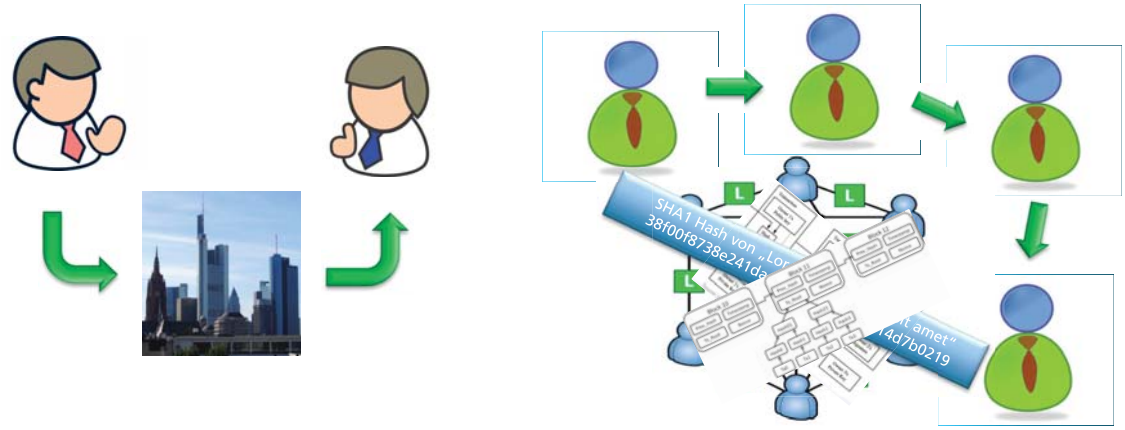
PayPal

TÜVRheinland®

Precisely Right.

Vierte Generation WWW ?:

Kontrolle und Vertrauen im „Internet of Value“

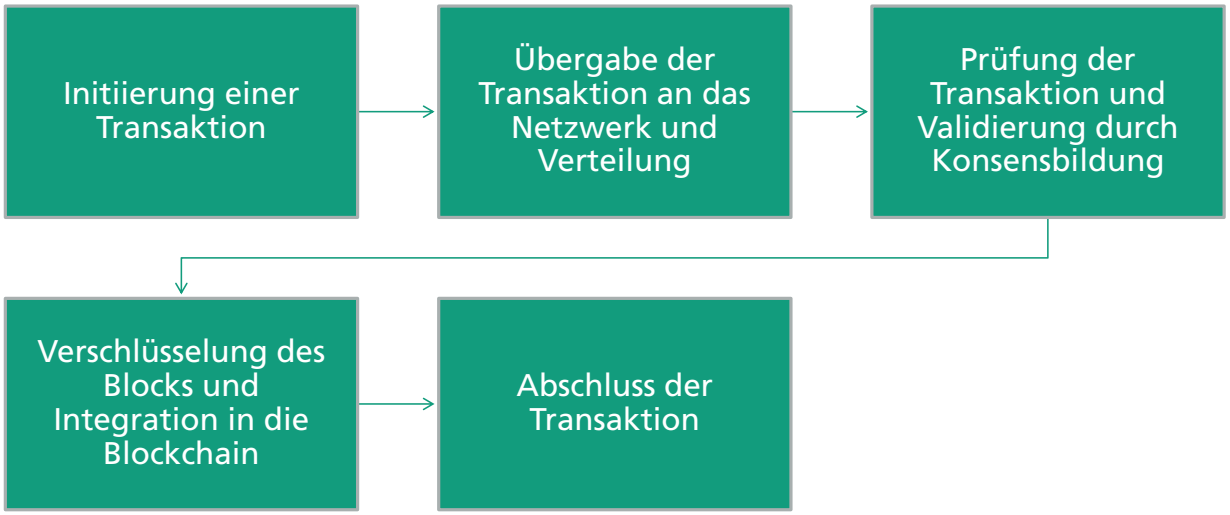


Institution ⟷ Algorithm

Wichtige Begriffe

Distributed Ledger	• Technologie zur verteilten Kontenverwaltung
Blockchain	• Neue Technologie zur dezentralen, nachvollziehbaren und irreversiblen Speicherung von Transaktionen
Bitcoin	• Kryptowährung auf Basis der Blockchain Technologie

Wie funktioniert es?



Authentisierung und Autorisierung in einer Blockchain

- Public / Private Key Mechanismen
  - Authentisierung gegenüber dem System
  - Identifikation der Transaktionspartner
  - Verschlüsselung
- Wie handhaben und verwalten wir die Schlüssel?
- Wie vermeiden wir den Verlust?

https://www.bitaddress.org

- Pseudoanonymization schützt nicht die Privatspähre!

Wann haben Sie eigentlich die letzte signierte/verschlüsselte Email verschickt?

Grundkonzepte hinter der Blockchain

Kryptografie – Hashwert

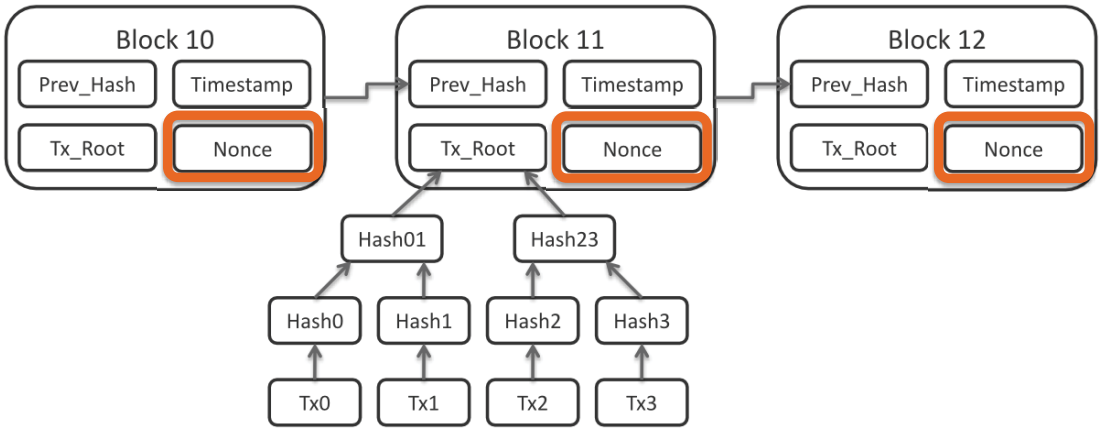
- Eine Hash-Funktion kann digitalen Daten beliebiger Größe in digitale Daten mit fester Größe umwandeln
- Selbst geringfügige Unterschiede in den Eingangsdaten erzeugen sehr große Unterschiede in den Ausgangsdaten
- Eine Wiederherstellung des ursprünglichen Textes aus dem Hashwert ist nicht möglich (nicht umkehrbar)

SHA1 Hash von „abc“
a9993e364706816aba3e25717850c26c9cd0d89d

SHA1 Hash von „abC“
57babce0612ae7c07c380ddd1fb9d6b4c0dc1033

SHA1 Hash von „Lorem ipsum dolor sit amet“
38f00f8738e241daea6f37f6f55ae8414d7b0219

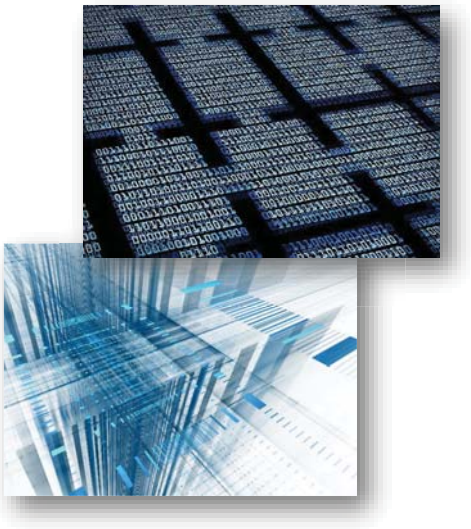
Hash-Funktionen und Merkle Tree



Smart Contracts verwandeln eine passive Blockchain in ein weltweit verteiles Computing Ecosystem

- **Technik**
  - Programmcode wird als ausführbares Skript in einer Transaktion gespeichert
  - Programmcode wird innerhalb einer Blockchain ausgeführt.
- **Konzept**
  - Realisierung eines neuen Ecosystems zur Abwicklung autonomer Transaktionen.
  - Blockchain wird Basis für IoT Lösungen.
- **Smart Contracts können aber auch zum Albtraum werden, durch**
  - komplexe Verwaltung, unkontrollierbare und irreversible autonome Aktivitäten

Was macht diese Technologie so attraktiv?



Verteilte Konsensbildung in einem Netzwerk
– keine zentrale Instanz

Abbildung von Werten und Rechten

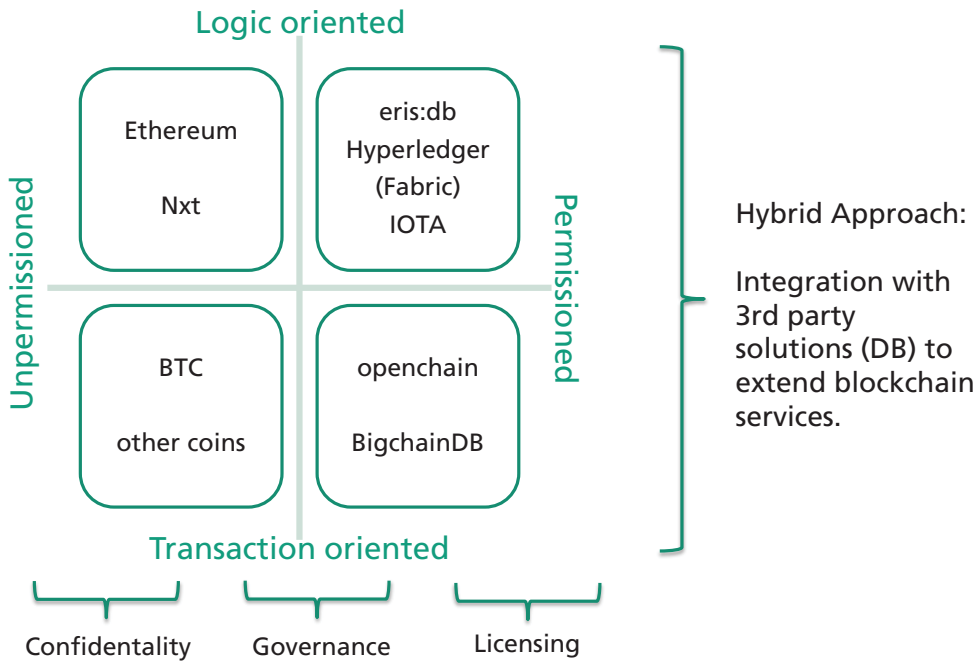
Nachvollziehbarkeit und irreversibles Protokoll des Transfers

Automatisierungspotenzial durch Smart Contracts

Blockchain als Basis für die 4. Generation eines Internets der Werte

Fraunhofer FIT

The Blockchain *Design Space*



Fraunhofer FIT

Validation von Transaktionen in einer Community Consensus building

Performanz

Proof of Work	Proof of Stake	Lottery Protocol	Explizite Validierungsknoten
• Validierung durch das Lösen eines mathematischen	• Validierung durch die Knoten, die den größten Anteil halten – „trust the bosses“	• Zufällig ausgewählte Knoten	• Ausgewählte Knoten haben das Recht zu validieren. z.B. BigchainDB, erisDB
• Erfordert Energie, hohe Rechenleistung, Zeit	• Schneller, verlagert das Vertrauen aber aus den Algorithmen in Institutionen	• Erfordert ein vertrauensvollen Lotterie Mechansimus – Hardware?	• Kontrollierter Zugang zur Blockchain

Offenheit, Öffentlichkeit

Fraunhofer FIT

Auf der Suche nach einem Use Case?

Wer verdient unnötig an meinem Prozess?

Wo bin ich der Vertrauensspender?

- Intermediär verdrängen
  - Können Sie einen Intermediär eliminieren, um Zeit oder Kosten zu sparen?
  - Kann die Aufgabe des Intermediärs über Konsensfindung übernommen werden?
  - Bin ich ein Intermediär?

Was können wir nicht vernetzt erledigen, weil uns der Intermediär fehlt?

- Neuen Intermediär finden
  - Unterschiedlichen Stakeholder ohne Vertrauensbeziehung
  - flexible und flüchtige Kooperationspartnern ohne stabile und sichere Transaktionsbasis.

Wo bin ich im Boot und wo bald der Steuermann gewechselt wird?

- Bin ich Partner eines solchen Prozesses?

Fraunhofer FIT

Auf der Suche nach einem Use Case?

Wo können Routineprüfungen den Prozesse umkrempeln?

- Aus Prozesssicht:
  - Ist eine hohe Datenintegrität erforderlich?
  - Sollen / können Prozesse autonom und nach festen Regeln ausgeführt werden? (Smart Contracts)

Suchen Sie einen prüf- und dokumentationsintensiven Prozess

Um sich das Leben einfach zu machen …

- Vermeiden Sie Prozesse, die einer strengen Regulierung unterliegen
- Fokussieren Sie nicht auf Kryptowährungen!

Lieferkettenverfolgung und Fälschungssicherheit

Everledger To Use Blockchain Technology For Insurance Purposes

2015-08-03 08:59 AM | Alex William

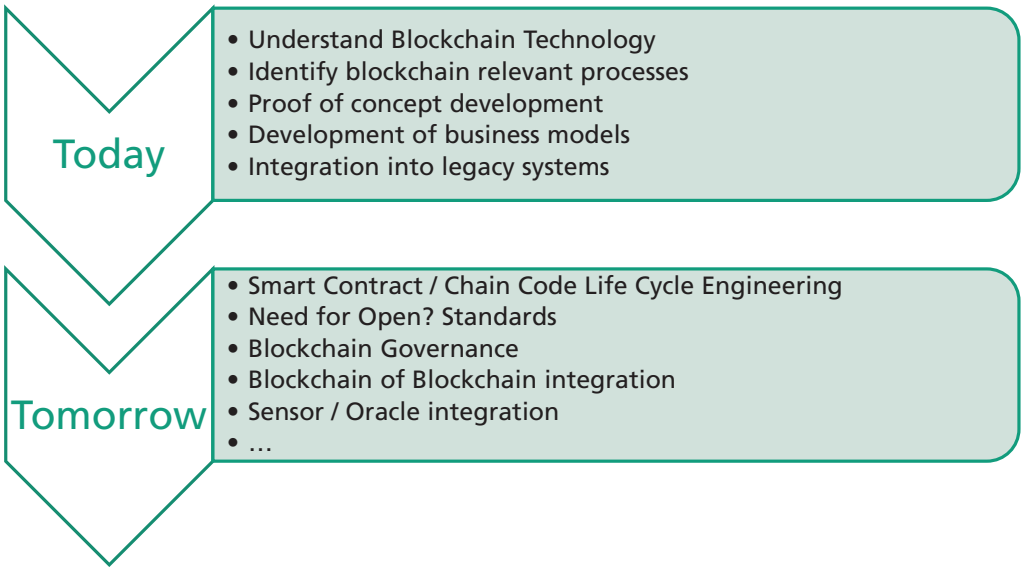
Everledger, a London- based startup that provides immutable ledger for diamond ownership and related transaction history verification for insurance companies has come up with a plan to ensure that the insured items are what they are said to be.

http://bitcoinvox.com/article/1845/everledger-to-use-blockchain-technology-for-insurance-purposes

Smart-Grids

Energie Schwarm		Blockchain
Dezentral	✓	P2P Netzwerk, kein zentraler Intermediär
Irreversible Protokollierung von Lieferung und Verbrauch	✓	Inherente Blockchain Eigenschaft in Kombination mit Orakeln
Abrechnung	✓	Smart Contracts
Bezahlung	✓	Cryptocurrency
Aushandlung / Preisfindung	✓	Smart Contracts
Skalierung und hohe Transaktionsfrequenz	?	Abhängig von der Infrastruktur
Eingriff durch Regulatoren	?	Rollen und Rechtekonzepte
Offen/Transparent <-> Zugangskontrolliert	?	Abhängig von der Infrastruktur

Trends?



Sensor / Oracle Integration

How do we deal with untrusted sensors / oracles?

Baseline of a blockchain is a transaction of values from Alice to Bob

What does that mean in the context of representing facts / certificates or sensor values in a blockchain?

- Is this fact just payload to a financial transaction?
- Financial transactions operate on a limited resource (amount of available currency)

Do we need sensor to sensor transactions, i.e. do we need two sensors for each sensor value who agree upon a fact?

Zusammenfassung

- Blockchains spannen einen sehr weiten Lösungsraum für unterschiedliche Anwendungen – nicht nur Cryptowährungen!
- Analysieren Sie Ihr Geschäftsmodell und Ihre Prozesse auf Blockchain-Potenzial.
- „Unchaining the blockchain“ in ihre einzelnen Bausteine ermöglicht die Konzeption neuer Lösungsansätze.

Empfehlung:
Analysieren Sie Ihre Prozesse auf Blockchain-Relevanz (Intermediär, Netzwerktransaktionen, etc.) und experimentieren Sie mit Prototypen und Demonstratoren.

Kontakt

Prof. Wolfgang Prinz, PhD
Fraunhofer FIT
Schloss Birlinghoven
53754 Sankt Augustin

Tel: 02241 – 14 2730
wolfgang.prinz@fit.fraunhofer.de

Visit our blockchain lab:
http://www.fit.fraunhofer.de/de/fb/cscw/blockchain.html