BLOCKCHAIN/DISTRIBUTED-LEDGER IN DER AUTOMATISIERUNG EINE LÖSUNG SUCHT PROBLEME?

DR. MICHAEL KREUTZER, ATHENE UND FRAUNHOFER SIT

AUTOMATISIERUNGSREGION RHEIN MAIN NECKAR - AUTOMATISIERUNGSTALK VOM 27.10.21

Fraunhofer SIT

AGENDA

- **In Aussicht gestellt (beispielhaft)**
- Zwei Prinzipien
- Was ist eine Blockchain
- Funktionsweise einer Blockchain
- Varianten von Blockchains
- Anwendungskriterien für Blockchains
- Revisited: In Aussicht gestellt (beispielhaft)

IN AUSSICHT GESTELLT (BEISPIELHAFT)

Die Blockchain könne

- Produktions– oder Lieferdaten insbesondere in Lieferketten,
- den Besitz,
- Stationen des Transports,
- Messwerte wie die Einhaltung der Kühlkette,
- Materialqualität und Produkteigenschaften,
- Informationen über Alterung und Verschleiß und
- Vertragsinformationen

unumkehrbar und für alle transparent dokumentieren und nachweisen.

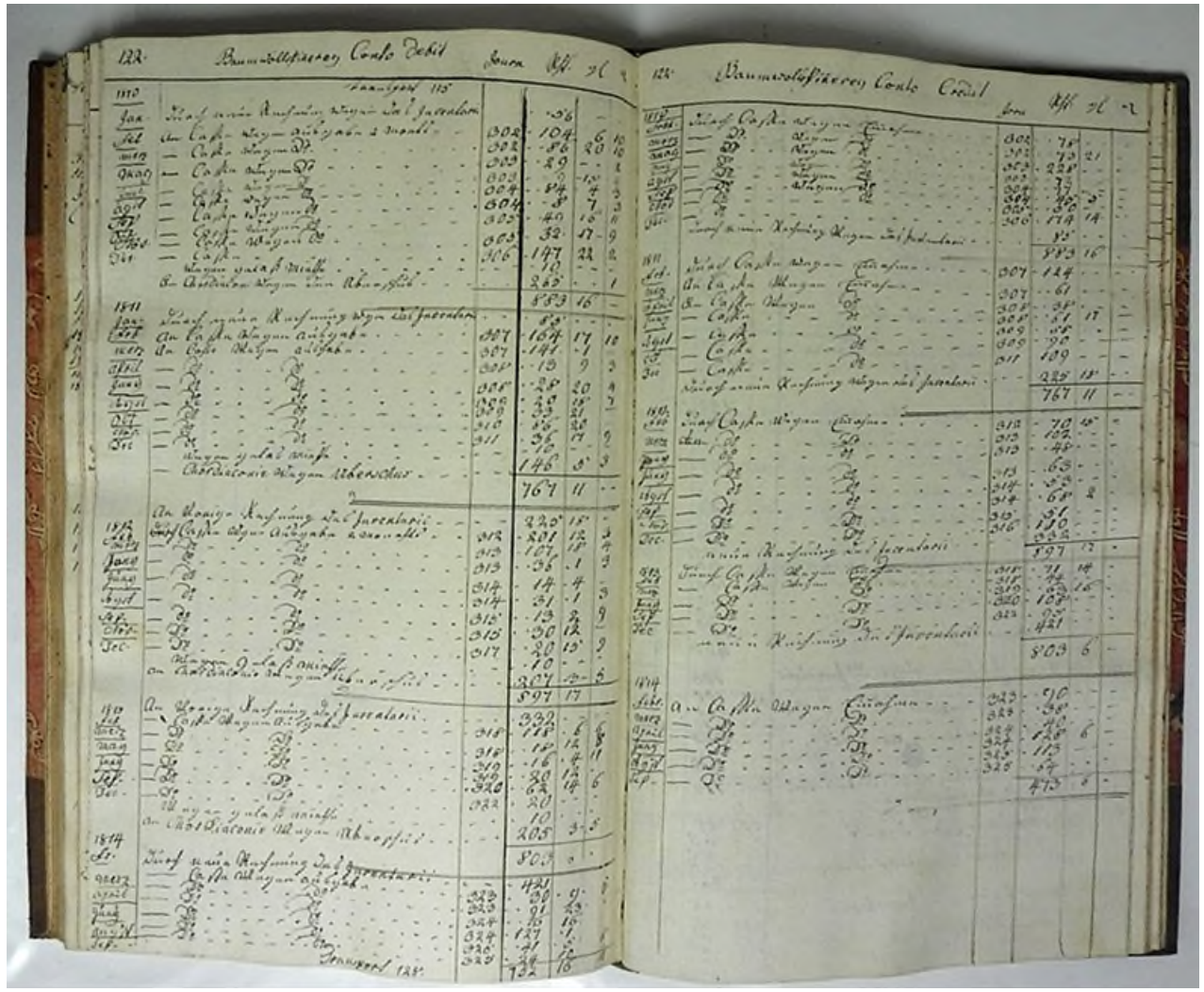
AGENDA

- In Aussicht gestellt (beispielhaft)
- **Zwei Prinzipien**
- Was ist eine Blockchain
- Funktionsweise einer Blockchain
- Varianten von Blockchains
- Anwendungskriterien für Blockchains
- Revisited: In Aussicht gestellt (beispielhaft)

1. PRINZIP: DAS HAUPTBUCH

Hauptbuch Schwesternhaus Kleinwelka

1786-1820 im Archiv der Kolonie Kleinwelka



Derbrauni, CC BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0>, via Wikimedia Commons

2. PRINZIP:
DEZENTRALITÄT - KOORDINATION UNTER PEERS

Beispiel: Höhenmessung Flugzeug

Messgerät 1: 2,521 ft
Messgerät 2: 2,522 ft
Messgerät 3: 1,017 ft
Messgerät 4: 2,519 ft
Messgerät 5: 2,2517 ft

Resultat des Quorums aller Messgeräte untereinander: ca. 2,520 ft.

Wert des fehlerhaften Messgeräts 3 wurde durch Quorumsentscheidung ignoriert.

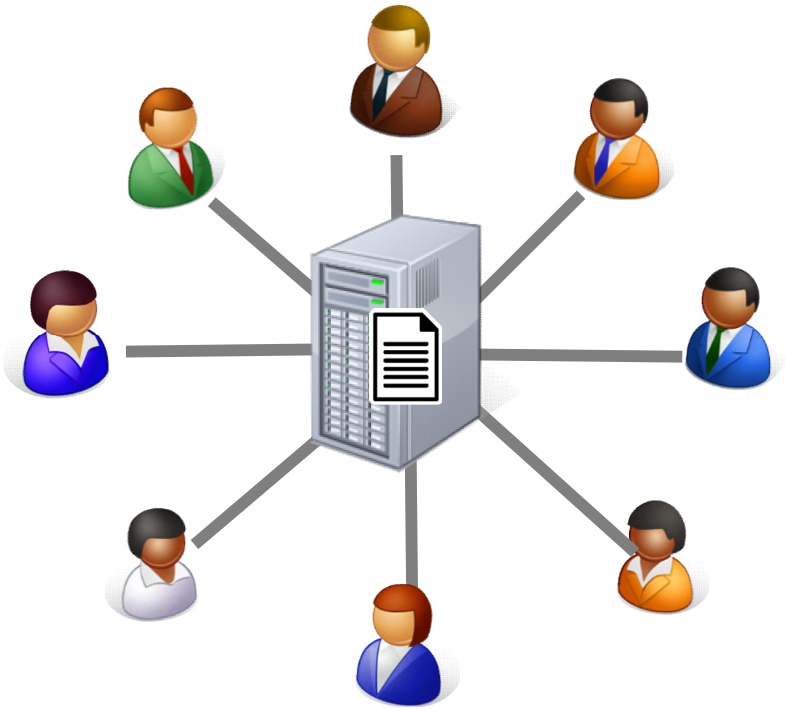
AGENDA

- In Aussicht gestellt (beispielhaft)
- Zwei Prinzipien
- **Was ist eine Blockchain**
- Funktionsweise einer Blockchain
- Varianten von Blockchains
- Anwendungskriterien für Blockchains
- Revisited: In Aussicht gestellt (beispielhaft)

EINE BLOCKCHAIN IST *KEINE* ZENTRALE STRUKTUR

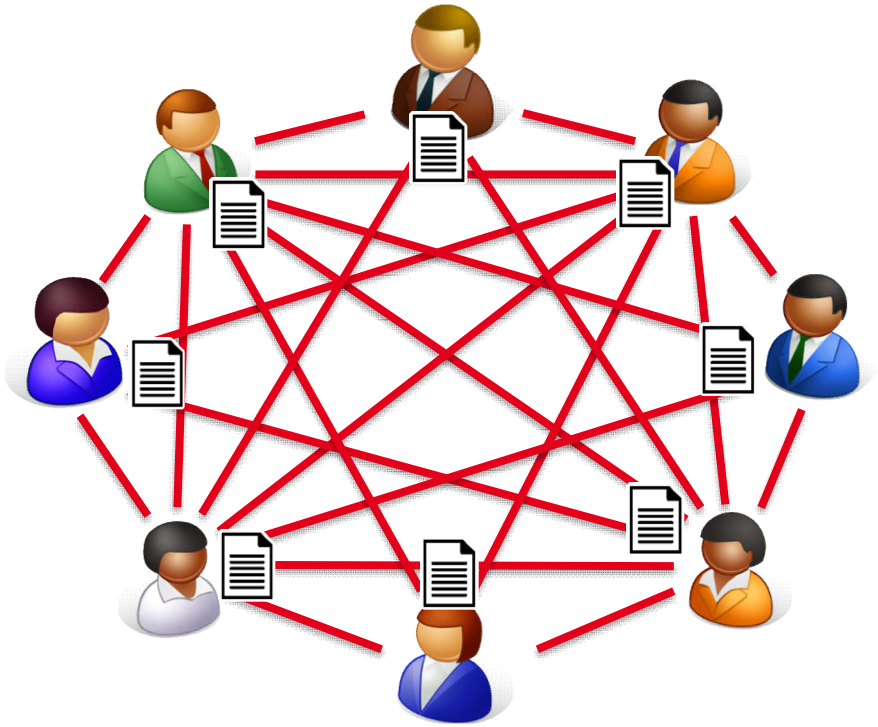
Zentrale Struktur:

- Zentrale Ablage von Daten
- Serversoftware an einer Stelle
- Einfache Wartung und Änderung
- Single Point of Failure



WAS IST EINE BLOCKCHAIN?

Eine Blockchain ist ein digitales, dezentrales append-only Register, bei dem alle Einträge in Blöcken strukturiert und kettenartig miteinander verbunden sind.



Dezentrale Struktur:

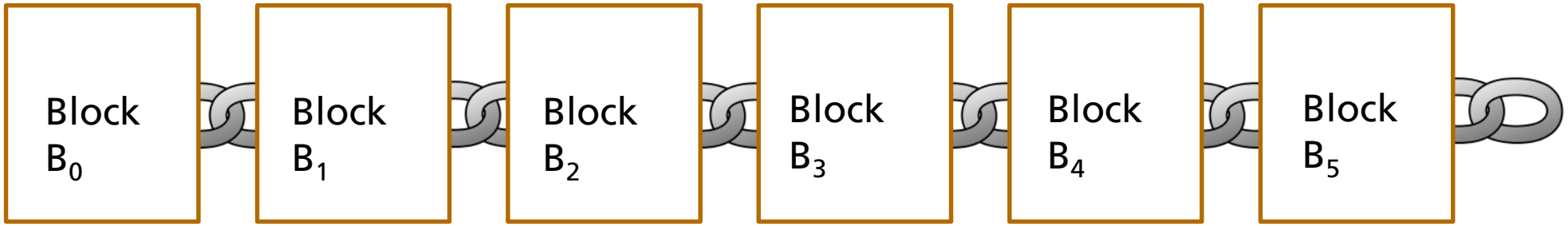
- Verteilte Ablage von Daten
- Gemeinsames Protokoll und Software bei Knoten
- Änderungen aufwändig
- Kein Single Point of Failure

WAS IST EINE BLOCKCHAIN?

Eine Blockchain ist ein digitales, dezentrales append-only Register, bei dem alle Einträge in Blöcken strukturiert und kettenartig miteinander verbunden sind.

Der Begriff wird verwendet als Bezeichnung für

- eine Kryptowährung (Bitcoin)
- eine Technologie
- eine Datenstruktur



AGENDA

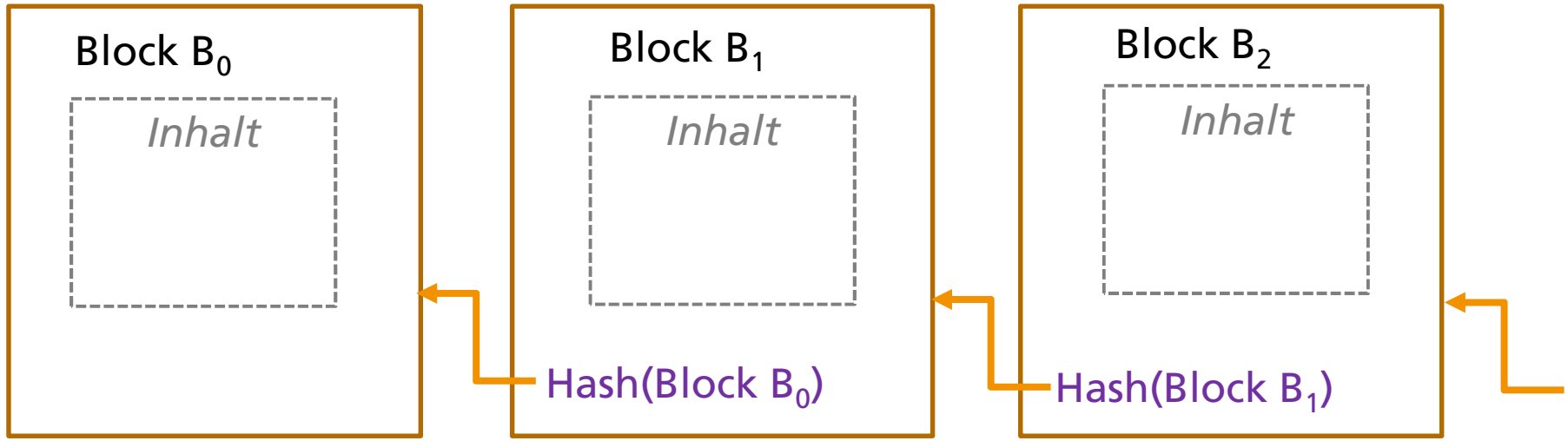
- In Aussicht gestellt (beispielhaft)
- Zwei Prinzipien
- Was ist eine Blockchain
- **Funktionsweise einer Blockchain**
- Varianten von Blockchains
- Anwendungskriterien für Blockchains
- Revisited: In Aussicht gestellt (beispielhaft)

FUNKTIONSWEISE VON BLOCKCHAIN

Verkettung durch Hash-Werte

- Alle Blöcke sind miteinander verkettet
- Unbemerktes Löschen/ Manipulieren von Blöcken nicht möglich

  ⇨ Irreversibilität, Integrität, Transparenz

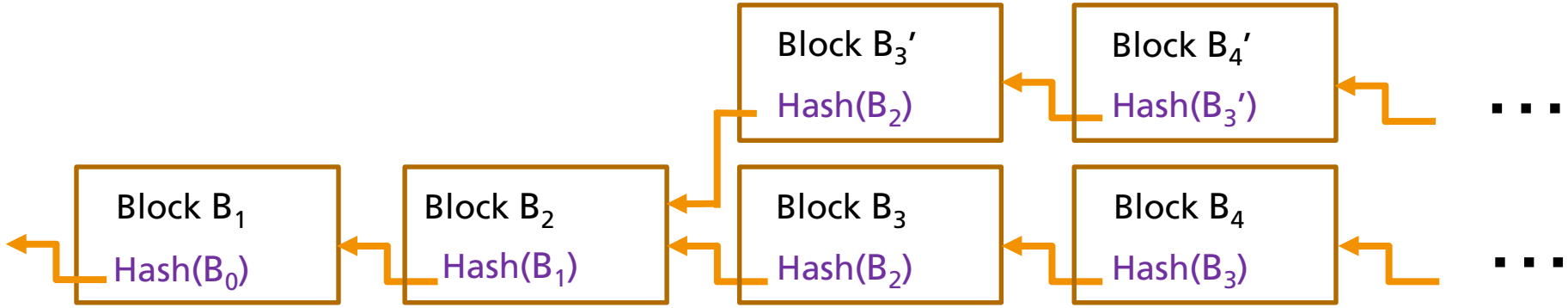


Inhalte

- Transaktionen
- Informationen
- Smart Contracts
- …

Funktionsweise von Blockchain

- Alle Transaktionen einsehbar und überprüfbar
  - Keine unbemerkte Manipulation von getätigten Transaktionen
  - Unautorisierte Transaktionen sind erkennbar
  - Kein „double spending“
- Problem: Dezentralität ermöglicht unterschiedliche Versionen der Blockchain im Netzwerk – welche ist die „Richtige“?
- Lösung: Mehrheitsentscheidungen durch Konsens-Mechanismen



Konsens-Mechanismus Proof of Work

Proof of Work

- Lösung rechenintensiver Aufgabe zur Erstellung neuer Blöcke notwendig

  (Bitcoin: Finde $Hash(B_{i-1}) \leq 2^{256}/2^{72}$)

- Erstellung gültiger Blöcke wird mit Anreiz (incentive) belohnt ⇨ „mining“

- „One-CPU-one-Vote“: Knoten stimmen mit CPU über gültige Version der Blockchain ab

  ⇨ Mehrheitskonsens ohne gegenseitiges Vertrauen

- Betrug ineffizienter als Wohlverhalten

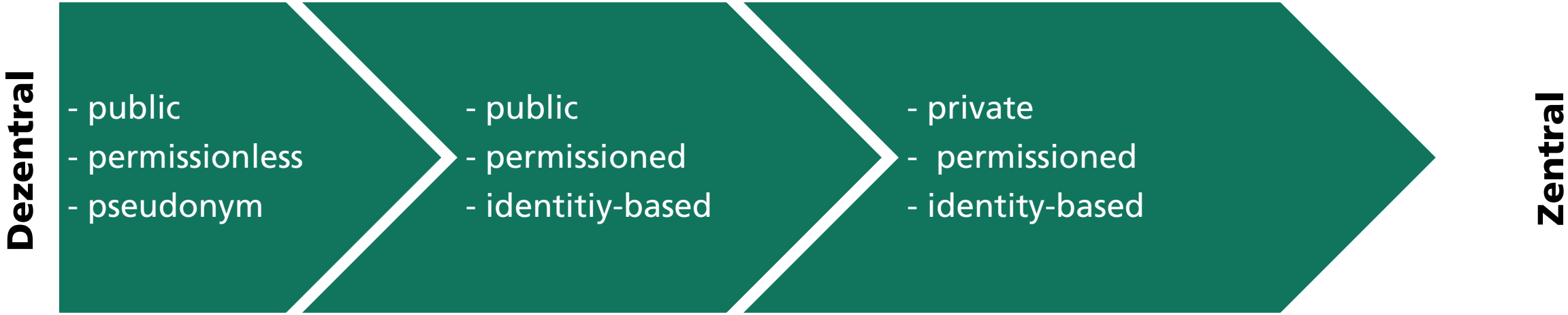
Mehrheit der Rechenpower entscheidet ⇨ ermöglicht 51%-Angriff

AGENDA

- In Aussicht gestellt (beispielhaft)
- Zwei Prinzipien
- Was ist eine Blockchain
- Funktionsweise einer Blockchain
- **Varianten von Blockchains**
- Anwendungskriterien für Blockchains
- Revisited: In Aussicht gestellt (beispielhaft)

Varianten von Blockchain

- public / private: Blockchain öffentlich einsehbar/ privat
- permissioned / permissionless: Anfügen neuer Blöcke bedarf Genehmigung / keiner Genehmigung
- identity-based / pseudonym: Teilnehmer treten über reale Identitäten/ pseudonym auf



Beispiele für Konsens-Mechanismen

Proof of Work	**Arbeitsnachweis** CPU-intensive Rechenaufgabe
Proof of Space	**Speichernachweis** Speicher-intensive Rechenaufgabe
Proof of Stake	**Anteilsnachweis** Das Recht zur Generierung neuer Blöcke haben Knoten mit vielen Coins
Delegated Proof of Stake	**Deligierter Anteilsnachweis** Coin Besitzer stimmen für Delegierte stimmen, die das Netzwerk für sie sichern
Practical Byzantine Fault Tolerance	**Redundante Abfragen:** Abstimmungsverfahren mit mehreren Runden

Beispiele für Konsens-Mechanismen

Proof of Work	**Arbeitsnachweis** CPU-intensive Rechenaufgabe
Proof of Space	tensive Rechenaufgabe
Proof of Stake	Generierung neuer Blöcke
Delegated Proof o Stake	Coin Besitzer stimmen für Delegierte stimmen, die das Netzwerk für sie sichern
Practical Byzantine Fault Tolerance	**Redundante Abfragen:** Abstimmungsverfahren mit mehreren Runden

Ressourcenverbrauch?

Angriffsmöglichkeiten?

Skalierbarkeit?

AGENDA

- In Aussicht gestellt (beispielhaft)
- Zwei Prinzipien
- Was ist eine Blockchain
- Funktionsweise einer Blockchain
- Varianten von Blockchains
- **Anwendungskriterien für Blockchains**
- Revisited: In Aussicht gestellt (beispielhaft)

Blockchain – was kann sie leisten, wo sind Grenzen?

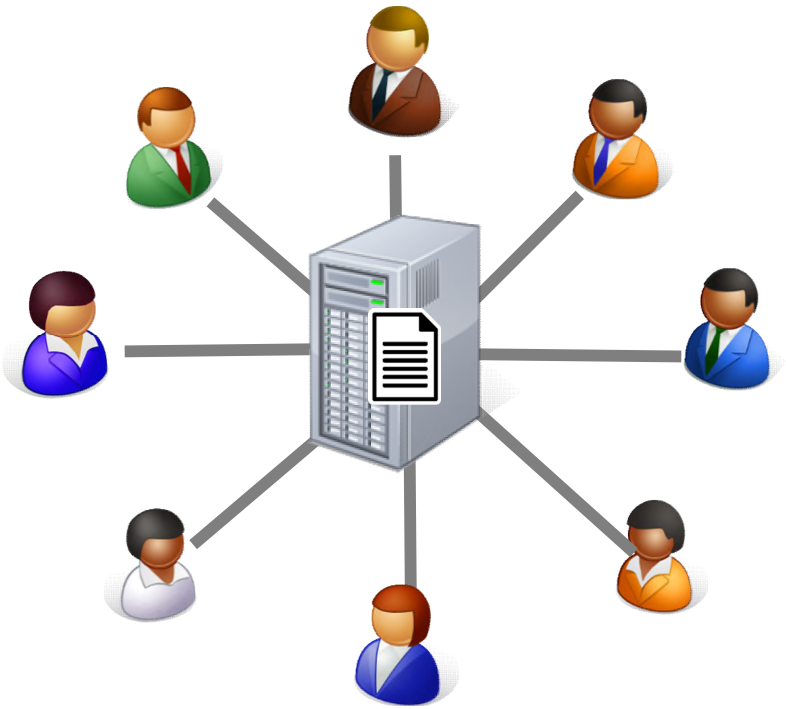
Leistung

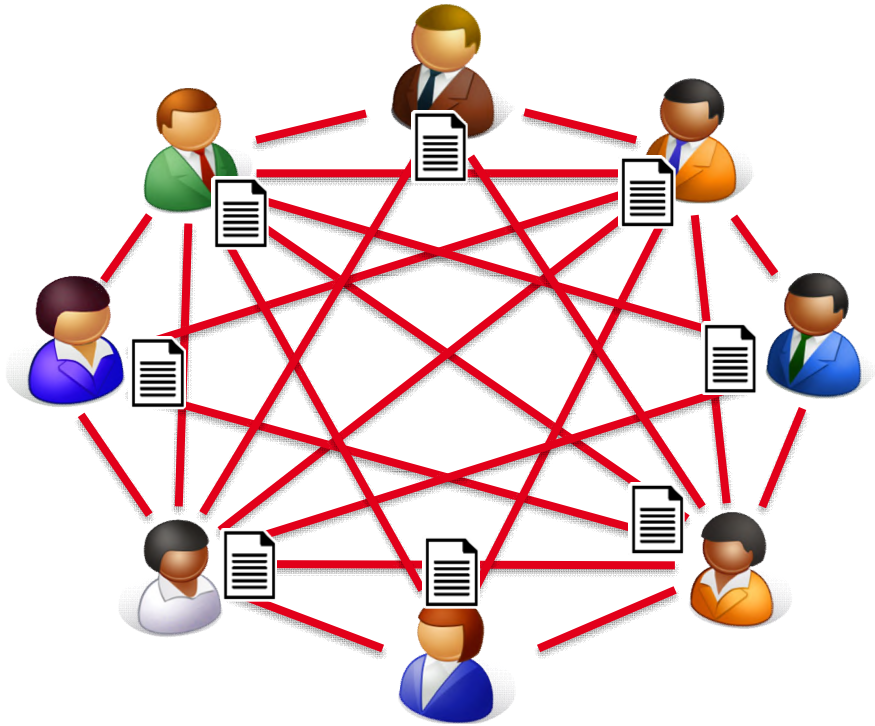
- Unabhängigkeit von zentralen Instanzen
- Integrität
- Irreversibilität
- Transparenz
- Konsensbildung ohne Vertrauen
- Kein Single Point of Failure

Grenzen

- Skalierbarkeit
- Mining-Aufwände (Energieaufwand, etc.)
- Verbindung von realer und digitaler Welt
- Irreversibilität
- Rechtliche und regulatorische Aspekte

BEISPIEL CLEARINGHOUSE





Anwendungskriterien für Blockchain

Ist Blockchain möglich?

- Es gibt ein Netzwerk
- Es gibt gemeinsame Objekte (Assets)
- Es gibt Transaktionen

Ist Blockchain sinnvoll?

- Notwendigkeit von Dezentralität, Integrität, Irreversibilität, dezentrale Konsensbildung ohne Vertrauen, etc. *in Kombination*?
- Günstigere Alternativen?
- Anforderungen an Skalierbarkeit?

Siehe auch: http://doyouneedablockchain.com/

AGENDA

- In Aussicht gestellt (beispielhaft)
- Zwei Prinzipien
- Was ist eine Blockchain
- Funktionsweise einer Blockchain
- Varianten von Blockchains
- Anwendungskriterien für Blockchains
- **Revisited: In Aussicht gestellt (beispielhaft)**

IN AUSSICHT GESTELLT (BEISPIELHAFT)

Die Blockchain könne

- Produktions– oder Lieferdaten insbesondere in Lieferketten,
- den Besitz,
- Stationen des Transports,
- Messwerte wie die Einhaltung der Kühlkette,
- Materialqualität und Produkteigenschaften,
- Informationen über Alterung und Verschleiß und
- Vertragsinformationen

unumkehrbar und für alle transparent dokumentieren und nachweisen.

BRAUCHE ICH DAFÜR EINE BLOCKCHAIN?

- **Firmeninterne Blockchains**

  Sobald nur eine Partei (die Firma) die Kontrolle über die Blockchain hat, braucht man keine mehr. Beispielsweise reichen Signaturketten völlig aus.

- **Blockchains für Lieferketten**

  Beispiel Automobilindustrie: Blockchain wäre insbesondere dann zu empfehlen, wenn alle großen Automobilhersteller und -zulieferer an ein und derselben Blockchain mitrechnen und sich gegenseitig nicht vertrauen! In diesem Fall prüfen sie gegenseitig die Signaturen etc.

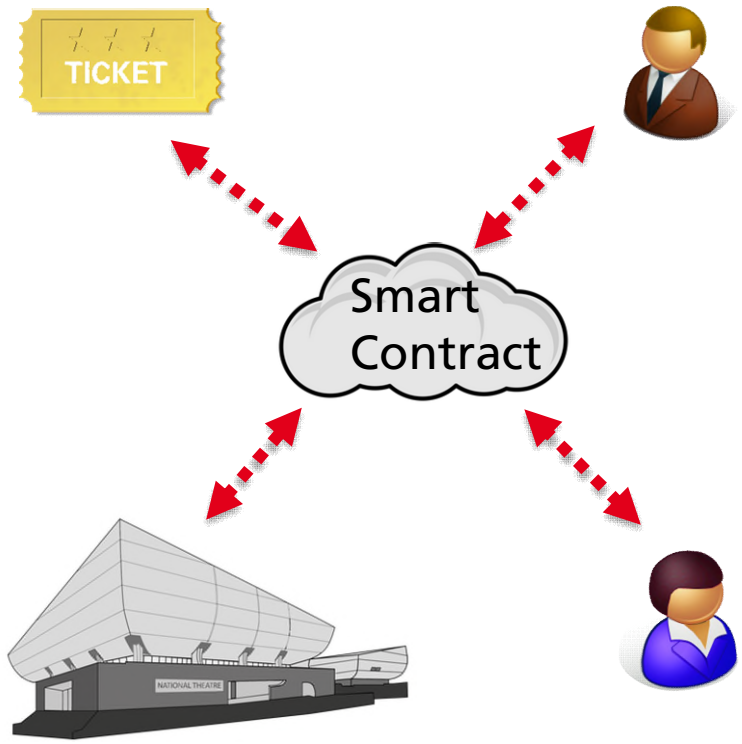
- Gilt auch für: Stationen des Transports, Messwerte wie die Einhaltung der Kühlkette, Materialqualität und Produkteigenschaften, Informationen über Alterung und Verschleiß

SMART CONTRACTS (BSP. ETHERUM)

- Knoten nutzen Etherum-Clients
- Verträge werden kodiert in spezielle Programmiersprachen (Solidity, Serpent, LLL) in der Blockchain eingetragen

- Automatisierte Erfüllung von Vertragsinhalten (`IF…THEN…ELSE`)

  über *Dapps* (Distributed Apps)



Weiterbildungsangebot des Fraunhofer SIT

- Online-Kurs „Einführung in Darknet und Kryptowährung“ im Lernlabor Cybersichereit
- Themen:
  - Darknet: technische und rechtliche Aspekte; Inhalte und BenutzerInnen im Tor-Netzwerk
  - Krypto-Währungen:
    - Kryptografie: Grundlagen zu Verschlüsselung und Hashes
    - Funktionsweise einer Blockchain
    - Kryptowährungen: Beispiele und praktische Verwendung
- Kursdauer: 14 Stunden an 4 Tagen
- Nächster Termin: 9.-12. Dezember 2021
- Infos: https://sit4.me/dnkw

Weitere IT-Security-Weiterbildungen am Fraunhofer SIT

- Unser Weiterbildungsangebot: https://www.sit.fraunhofer.de/de/weiterbildung

Titel	Datum
Einführung in Darknet und Kryptowährung	07.12. - 10.12.2021
Einführung in die Datenträger-Forensik (Grundlagenkurs)	30.11. - 02.12.2021
Digitale Forensik für interne Untersuchungen (Fortgeschrittenenkurs)	09.11. - 12.11.2021
Multimedia-Forensik für Ermittlungsverfahren	23.11. - 26.11.2021
Echtheitsprüfung für Digitalfotos und -videos	Dezember 2021 (TBA)
Grundlagen der Textdatenanalyse mit NLP und maschinellem Lernen	Anfang 2022 (TBA)
T.I.S.P. - Seminar	29.11. - 03.12.2021 21.03. - 25.03.2022
Cyber Range: Security Operation Center Basics	23.11. - 25.11.2021 13.12. - 15.12.2021

© Fraunhofer

HERZLICHEN DANK
FÜR IHRE AUFMERKSAMKEIT!

Dr. Michael Kreutzer

Internationalisierung und strategische Industriebeziehungen

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

Rheinstr. 75

64295 Darmstadt

michael.kreutzer@sit.fraunhofer.de

tel ++49 (0) 6151-869-348

fax ++49-(0) 6151-869-127

http://www.sit.fraunhofer.de/