

8. Blockchain / Distributed Ledger Technology

■ Einführung

- Zielsetzungen
- Arten von Blockchains/DLT
- Anwendungen

■ Anwendungsfall Krypto-Währungen / Bitcoin

- signierte Transaktionen
- Blockkette / Ledger
- Double Spending Anomalie
- Konsensus-Verfahren: Proof of Work



Motivation

■ klassische Datenbanken mit Transaktionen

- dauerhafte Speicherung von Daten
- Fehlersicherheit / Korrektheit bei Systemausfällen
- Konsistenz / Korrektheit bei konkurrierenden Zugriffen
- aber zentralisierte Kontrolle (auch bei verteilter Implementierung) , zB. durch Unternehmen / Finanzinstitut

■ Probleme

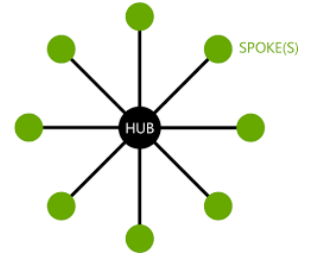
- Nutzer müssen Unternehmen (z.B. Bank) und anderen Transaktionspartnern (z.B. am Geldverkehr) vertrauen
- nicht-transparente Maßnahmen zum Schutz der Beteiligten und Angriffen



Generelle DB-Lösungen

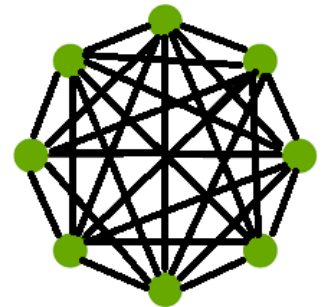
■ Lösung 1: zentralisiertes System (z.B. Bank) mit kompletter Kontrolle über Zustände und Zustandswechsel

- Nutzung eines zentralisierten DBS mit Transaktionskontrolle
- auch bei Einsatz von parallelen/verteilten DBS bleibt zentrale Kontrolle bzw. begrenzte Knotenautonomie (Verteilungstransparenz)



■ Lösung 2: Blockchain-Systeme / verteilte Ledger-Systeme (DLT: Distributed Ledger Technology)

- „Ledger“ (Buchführungssystem = Datenbank) zur Repräsentation des Zustandes
- verteilte Kopien mit Append-Only Änderungen
- globale Identität (Signatur) von Akteuren
- Transaktion für Zustandsübergänge (Synchronisation gegen Double Spending)



Blockchain: Begriff

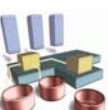
■ Blockchain = verteiltes System zur Verwaltung von Datensätzen mit dem Ziel, Konsens über den Zustand zu erzielen

■ Eigenschaften

- keine zentrale Instanz
- Teilnehmer ...
 - müssen andere Teilnehmer nicht kennen
 - müssen anderen Teilnehmern nicht vertrauen
 - können sich dennoch über einen Zustand einig sein

■ Prinzip

- Konsens über den initialen Zustand (z.B. leerer Zustand)
- P2P-Netz aus Teilnehmern (Netzwerkknoten)
- Transaktionen werden im Netzwerk angezeigt und weitergeleitet
- Verhindern der Manipulation von Existenz oder Inhalt bereits ausgeführter Transaktionen



Zielsetzungen

- mit Blockchain/DLT sollen mögliche Probleme zentraler Systeme lösen
- keine Abhängigkeit von „trusted third parties“
 - auch kein Vertrauen gegenüber anderen Teilnehmern erforderlich
- gleichberechtigter Zugriff auf Daten für alle Teilnehmer
- Daten können nicht manipuliert /gelöscht werden
- besserer Schutz gegenüber Angriffen
 - kein Single Point of Failure
- hohe Skalierbarkeit



Blockchain/DLT-Typen

- öffentliche vs. private Blockchains
- öffentliche Blockchains (z.B. für Kryptowährungen)
 - lassen beliebige Teilnehmer zu
 - maximale Transparenz, gesamter Ledger öffentlich
 - Pseudonymität der Nutzer suggeriert Privacy, aber oft Tracking-Angriffe möglich
 - sehr hoher Ressourcenbedarf
- private Blockchains (z.B. für Unternehmensanwendungen)
 - durch Eigentümer oder Konsortium kontrollierter Teilnehmerkreis (*permissioned* blockchains)
 - effizientere und kostengünstigere Realisierung von Transaktionen
 - typische Anwendung: Prozesse zwischen großen Organisationen abbilden, z.B für Lieferketten (supply chains)
 - Beispielrealisierung: Hyperledger (www.hyperledger.org)



Warum private Blockchains (DLTs)?

- Unternehmen wollen ihre Daten oft nicht veröffentlichen, sondern den Zugriff kontrollieren
- gemeinsame Geschäftsdaten können nicht einseitig verändert werden und werden doch automatisch synchronisiert
- Unveränderlichkeit vergangener Transaktionen bietet Grundlage für Audits
- Unterstützung komplexer Prozessmodelle / smart contracts



DLT: Anwendungen

- Krypto-Währungen (Bitcoin, Ether etc.)
- viele dezentrale, mit Smart Contracts realisierte, Anwendungen
- E-Voting-Systeme
- virtuelle Organisationen
- Crowdfunding
- Auditing: Aufzeichnung sicherheitskritischer Operationen
 - Zugriff auf bzw. Veränderung von Ressourcen (z.B. Daten, Dokumente)
 - Zugriff auf Gesundheitsakten, ...
- dezentrale Energieversorgung und –Abrechnung
- Lieferketten: Dokumentation der Teilschritte
- ...
- generell: Regeln eines gemeinsamen Prozesses automatisch Durchsetzen ohne auf zentrale Instanz zu vertrauen



8. Blockchain / Distributed Ledger Technology

■ Einführung

- Zielsetzungen
- Arten von Blockchains/DLT
- Anwendungen


■ Anwendungsfall Krypto-Währungen / Bitcoin

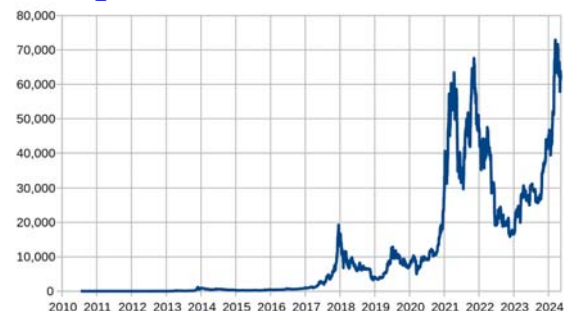
- signierte Transaktionen
- Blockkette / Ledger
- Double Spending Anomalie
- Konsensus-Verfahren: Proof of Work



Krypto-Währungen

■ Historie: Bitcoin

- 2008: Artikel von „Satoshi Nakamoto“ *Bitcoin – A Peer-to-Peer Electronic Cash System* <https://bitcoin.org/bitcoin.pdf>  **bitcoin**
- 2009 Open-Source-Software, eigentlicher Start
- starke Kursschwankungen
 - all-time high (2024): > 70 TE pro BTC (bitcoin) ,
 - März 2023 < 20 TE
- seit Jan. 2024 auch Börsenfonds (ETFs) in Bitcoin möglich



■ aktuell weit über 1000 Währungen

- fast keine staatliche Anerkennung (Ausnahme: El Salvador)
- viele Offerings mit betrügerischem Hintergrund
- weniger als die Hälfte überlebt ersten vier Monate
- Akzeptanz erfordert ausreichendes Vertrauen (durch sich gegenseitig kontrollierende Teilnehmer statt Zentralbank bzw. Staat)



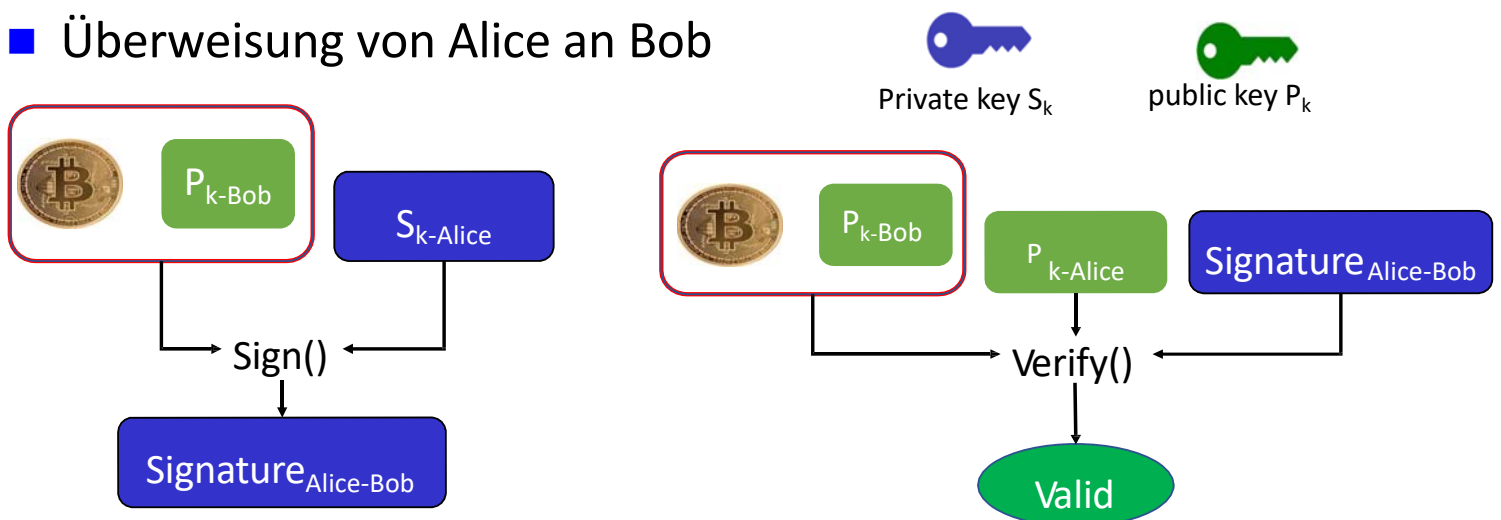
Krypto-Währungen: Bausteine

- Vernetzung der Teilnehmer: P2P-Netz statt zentrale Instanz
 - mehr als 19.000 Bitcoin-Knoten nach <https://bitnodes.io> (>1.600 in D)
- kryptographische Signaturen: Public-Key-Kryptosystem
 - öffentlicher Schlüssel = Kontonummer
 - privater Schlüssel = Verfügungsgewalt über Konto
 - Überweisung: Betrag + öffentlicher Schlüssel des Empfängerkontos, signiert mit privatem Schlüssel des Senders (=Transaktion)
 - Überweisung wird im Netz verteilt und kann von allen überprüft werden
- Buchführung: Transaktionen werden im Ledger voll repliziert auf allen Knoten verwaltet
- Bitcoin-Transaktionen
 - keine expliziten Konten: Guthaben = eingegangene Gutschriften, die noch nicht weiter überwiesen wurden

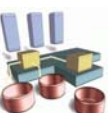
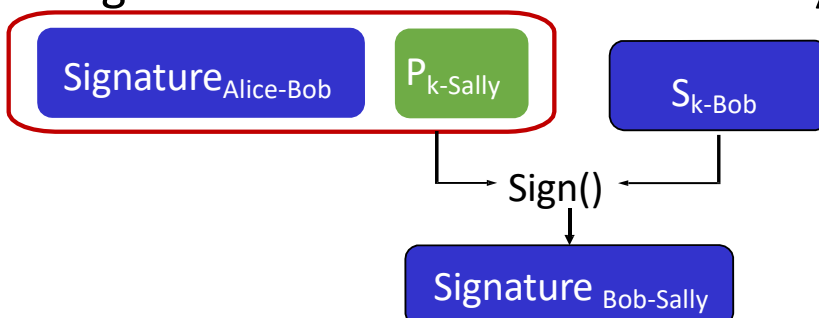


Digitale Signaturen und Bitcoin

- Überweisung von Alice an Bob



- Weitergabe der Bitcoins von Bob an Sally



Hashing H(x)

- Kombination von Signaturen und Public Keys über Hashing
 - Eingabe: String beliebiger Länge
 - Ausgabe fester Länge (z.B. 256 Bits)
 - effizient berechenbar
- Bitcoin nutzt SHA-256 (Secure Hash Algorithm)

$$\text{SHA256} \left(\text{Signature}_{\text{Alice-Bob}} \parallel P_{k\text{-Sally}} \right) =$$

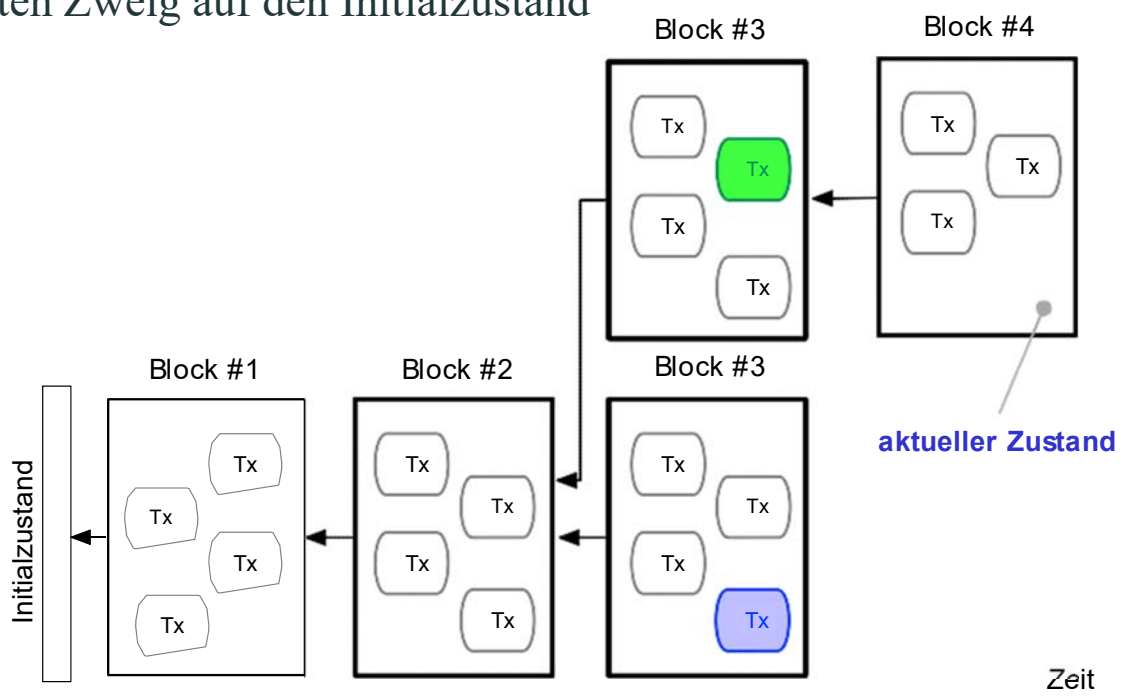
256-Bit (32-Byte) eindeutiger String

- Eigenschaften:
 - *kollisionsfrei*: keine zwei x, y so dass $H(x) = H(y)$
 - *sicher*: unmöglich x aus $H(x)$ abzuleiten (one-way hash function)



Blockchain-Elemente: Ledger

- Ledger = Blockkette (enthält Transaktions-Log)
 - jeder Knoten im Netzwerk verwaltet eigene Kopie des Ledgers
 - aktueller Zustand = Anwendung aller Transaktionen der Blöcke im längsten Zweig auf den Initialzustand



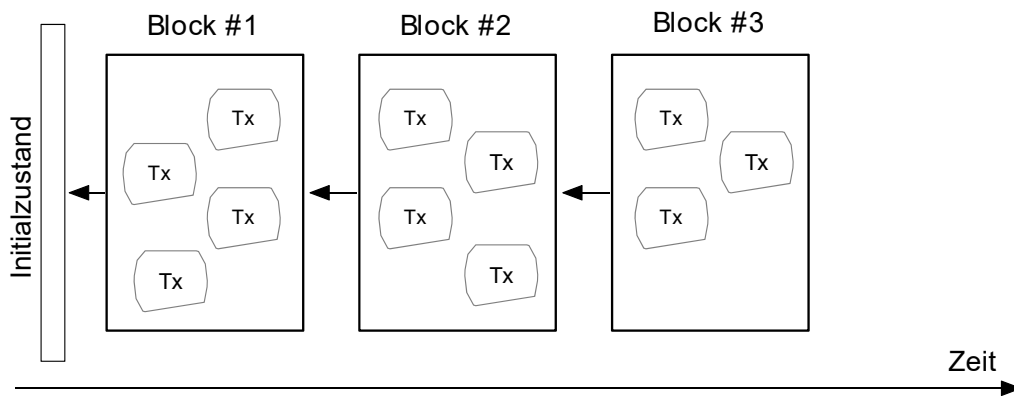
Blockchain-Elemente: Blöcke

■ Lösung:

- Zusammenfassung von Transaktionen zu Blöcken (**Block-**)
- Blöcke werden verkettet (**-chain**), d.h. ein Block basiert auf seinen Vorgänger
 - Block enthält kryptographisch sicheren Hashwert seines Vorgängerblocks

■ Blockinhalt: Transaktionsdaten, Zeitstempel, Hash des Vorgängerblocks (**unveränderlich**)

■ jeder Teilnehmer kann jederzeit neuen Block erstellen

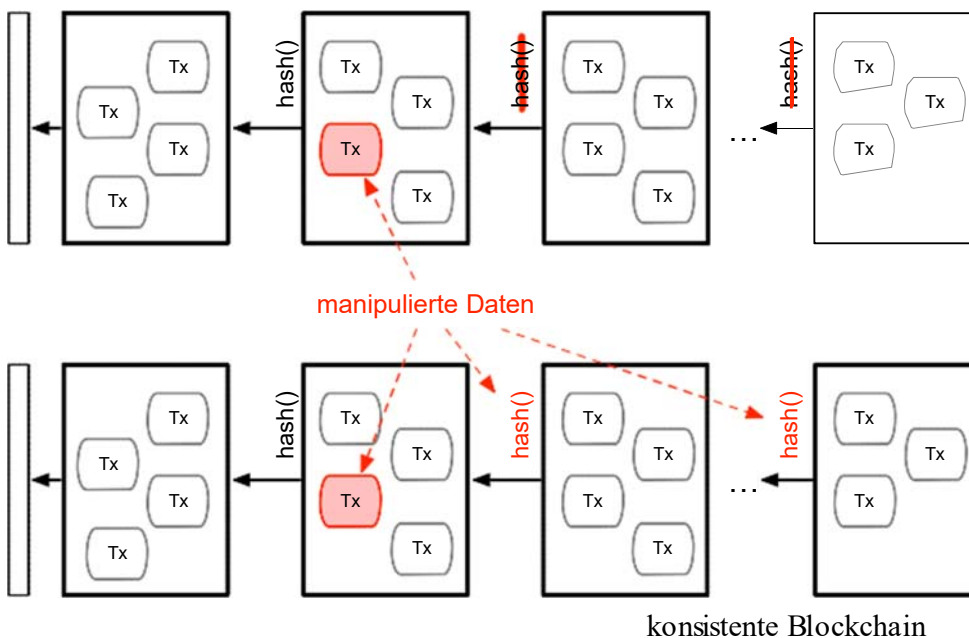


Blockchain: Manipulationssicherheit

■ Verkettung der Blöcke durch Hash-Zeiger

- Manipulation eines Blockinhaltes soll erkannt werden können
- alleine nicht ausreichend: Ersetzen einer Teilkette durch eine manipulierte Teilkette muss extrem schwer gemacht werden

Hash-Werte inkorrekt -> inkonsistente Blockchain

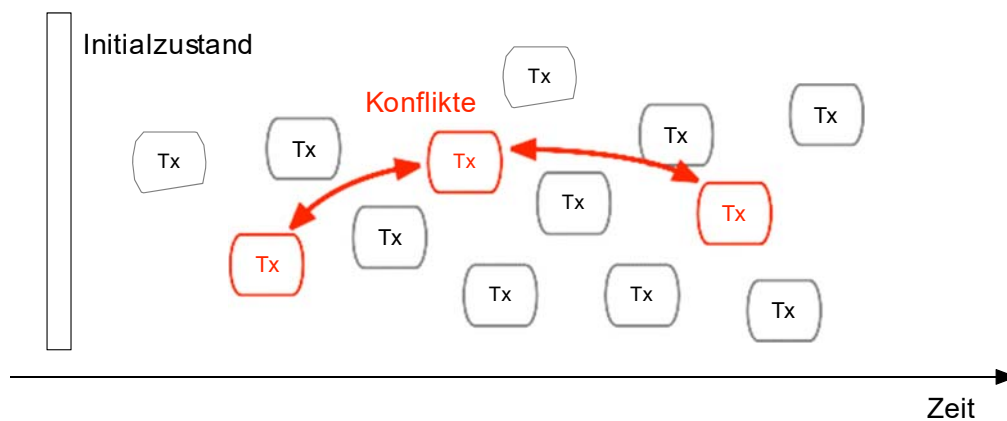


Probleme verteilter Transaktionen

■ Konsistenzprobleme

- (kurzzeitig) unterschiedliche Zustände der Knoten
- Reihenfolge der Transaktionen
- **Versuche doppelter Ausgaben**
- Konflikte / Abhängigkeiten zwischen Transaktionen

■ Notwendigkeit der Konsensusfindung



Mining / Konsens-Findung

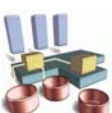
■ Miner sind Nodes, die das Konsens-Protokoll ausführen.

- werden dafür belohnt, da dies Dienstleistung für die Nutzer (Peers) ist
- Miner empfangen neue Transaktionen von Nutzern und bündeln sie in einem neuen Block. Neue Blöcke werden per Broadcast im Netz verteilt.
- da Miner parallel (konkurrent) arbeiten, können gleichzeitig verschiedene neue Blöcke im Netz kursieren (temporäre Inkonsistenz)

■ Eignung bekannter Konsensverfahren wie Paxos ...?

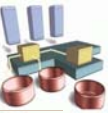
- keine Behandlung byzantinischer Fehler (böses Verhalten von Teilnehmern/Knoten, z.B. Austausch gefälschter Nachrichten)
- Knoten müssen bekannt und immer verfügbar sein

■ anderer Ansatz notwendig ->Proof of Work (PoW)

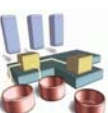
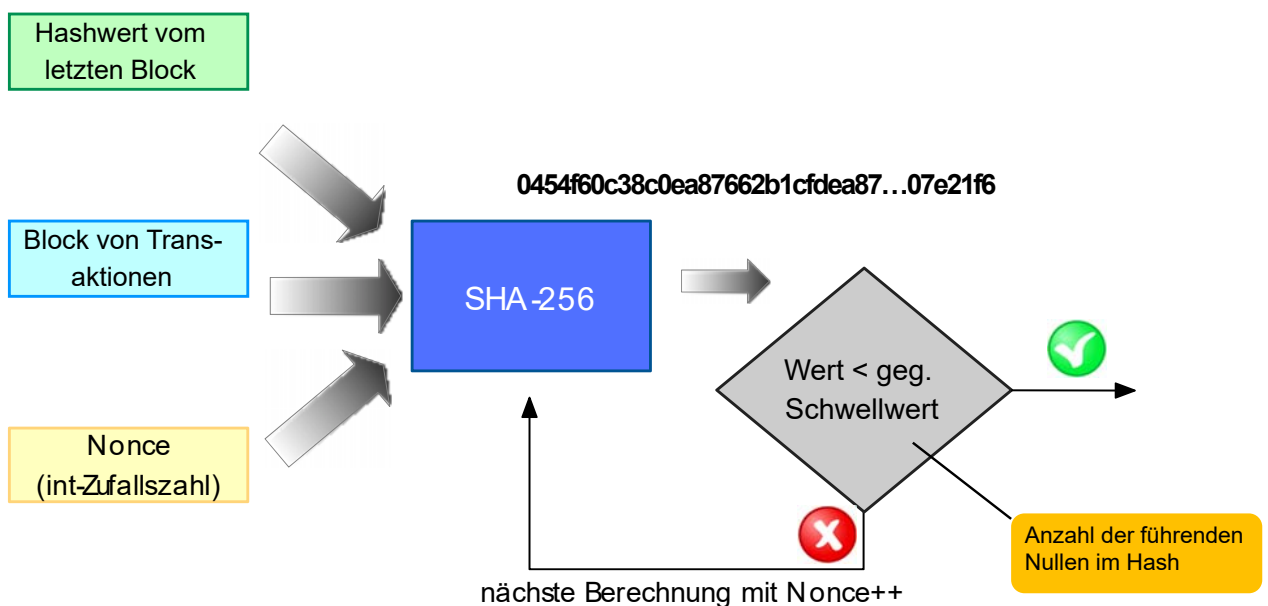


Proof of Work

- um einen neuen Block zu **signieren**, muss eine absichtlich sehr rechenaufwändige Aufgabe gelöst werden.
- Großteil des Netzwerks muss an der **längsten Block-Kette** mitgearbeitet haben → Peers übernehmen die längste Kette
- PoW Anforderungen:
 - aufwändige Berechnung (nur mit Brute Force) aber einfache und schnelle Validierung
 - muss abhängig vom zu erzeugenden Block sein (Vermeidung von Vorabberechnungsangriffen)
 - variabler Schwierigkeitsgrad
 - Anreizsystem: Mining selbst sollte lohnenswert sein: Belohnungstransaktion (Reward Transaction)
 - Teil des neuen Blocks (*Coinbase* in Bitcoin)



PoW: Hashcash von Bitcoin



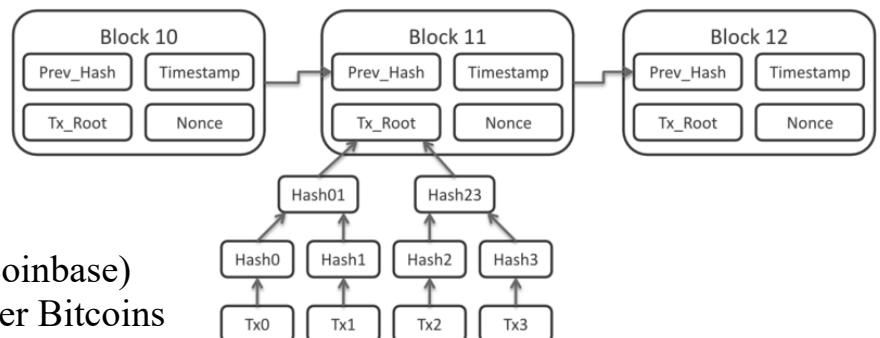
PoW: Ablauf

- wenn Knoten Aufgabe gelöst hat (Mining abgeschlossen):
 - füge Block von Transaktionen der Blockchain hinzu
 - Multicast (Flooding) der Lösung an andere Netzwerkknoten
 - Netzwerkknoten validieren und akzeptieren Lösung
- eingehende Blöcke werden nur akzeptiert, wenn Sie längste Kette korrekt erweitern
- in welchem Zweig der Blockchain sollte ein Miner arbeiten?
 - für Belohnung: Zweig muss Teil des aktuellen Zustands sein (=längster Zweig)
 - keine Koordination notwendig!
 - für von Mehrheit akzeptierte Blöcke erhält Miner geschürfte Bitcoins + Gebühren der enthaltenen Transaktionen



Bitcoin: Transaktionen und Blöcke

- Transaktionen
 - Inhalt: Senderadresse, Empfängeradresse, Betrag, Signatur
 - selbstgewählte Transaktionsgebühren
 - mit privatem Schlüssel des Senders signiert
 - im Netzwerk validiert und verbreitet
- Blöcke
 - feste Größe (z.B. 1 MB)
 - 1. Block = Genesis-Block
 - neue Blöcke durch Mining erzeugt
 - erste Transaktion eines Blocks (coinbase) enthält Überweisung neu erzeugter Bitcoins für Mining + Transaktionsgebühren (Reward)
 - Hashwert = paarweises Hashing der Transaktionen in *Merkle-Baum*, Hashwert des Wurzelknotens (Root-Hash) als Prüfsumme des Blocks
- Mining: PoW wie beschrieben (Nonce-Variation, Flooding)

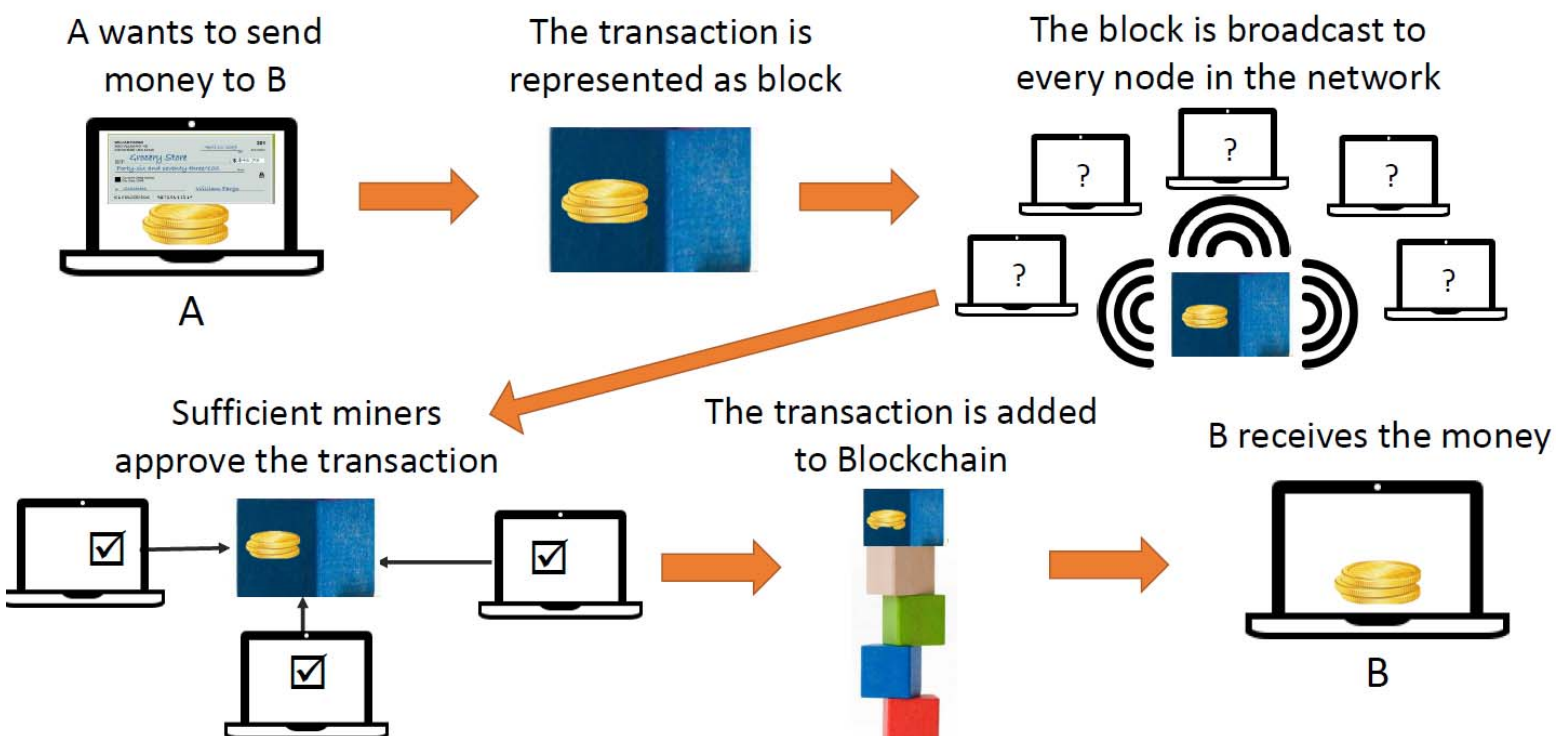


Netzwerkangriffe: 51%-Angriff

- Mehrheitsangriff: Angreifer kontrolliert über die Hälfte der Rechenleistung des Netzwerks
 - ermöglicht Double Spends, Rückgängigmachen von Transaktionen
 - Prinzip: eigene Blöcke schneller anlegen als der Rest des Netzes und nachträglich gültig machen
- nach Wikipedia:
 - 2014: Mining Pool GHash überschreitet kurzzeitig 50%-Marke
 - Attacken auf Bitcoin Gold (2018) und Ethereum Classic (2019)
- Gegenmaßnahmen
 - 51%-Angriff ist ein auffälliges Ereignis -> z.B. Hard Forks in Bitcoin
 - ersten Block einer verdächtigen Kette ungültig erklären
 - eingebaute Anreizmechanismen:
 - hohe Miningkosten im Falle einer Abwehr verloren
 - Senden anderer Transaktionen kann nicht verhindert werden



Gesamtablauf



Bitcoin: Fakten (Wikipedia)

- Größe Blockchain 562 GB (Juni 2024), Nov. 2020: 310 GB
 - seit April 2024: 3,25 neu erzeugte Bitcoins pro Block; halbiert sich alle 4 Jahre
 - Transaktionskosten: 1.000 Satoshi (= 10 μ BTC)
- max. 7 Transaktionen pro Sekunde (schlechte Skalierbarkeit)
 - ca. 10 Minuten pro Transaktion
- extremer Ressourcen/Energie-Bedarf
 - Schätzung: 120 Terawattstunden in 2023 (172 TWh in 2024) (0,5 % des Weltenergiebedarfs)
 - pro Transaktion: 1200 kWh (2021); Kreditkartentransaktion: 1,5 Wh
- energieeffizientere Konsensus-Ansätze existieren
 - z.B. “Proof of Stake” (seit 2022 in Ethereum System)



Zusammenfassung

- Blockchains/Distributed Ledgers: neues Paradigma für verteilte Daten- und Transaktionsverwaltung
- Popularität durch Kryptowährungen wie Bitcoin & Ether
- wesentliche Vorteile:
 - gleichberechtigte Datennutzung, keine Abhängigkeit von zentralen Institutionen, keine Veränderung bereits erfolgter Transaktionen ...
- technische Realisierung
 - Blockbildung und Verkettung durch Hashing verschlüsselter und signierter Transaktionen
 - vollständige Replikation der Blockchain
 - Validierung durch Mining und Konsensbildung
- Trend: private Blockchains für Unternehmensanwendungen mit besserer Leistungsfähigkeit und geringerem Ressourcenbedarf

