Bitcoin Protokoll

PC-Treff-BB VHS Aidlingen

Martin Schimpf

Datum

Quellen

- Grokipedia Fact-checked by Grok Bitcoin protocol
- Marc Friedrich Die größte Revolution aller Zeiten
- https://bitcoin.org/de/bitcoin-fuer-einzelpersonen

Grokipedia Fact-checked by Grok Bitcoin protocol

- Das Bitcoin-Protokoll ist die grundlegende Open-Source-Spezifikation von Regeln und Algorithmen, um über ein dezentrales Peer-to-Peer-Netzwerk digitales Geld zu übertragen, das
  - durch einen Proof-of-Work-Konsens zur Validierung von Transaktionen gesichert ist,
  - sicherstellt, das Geld nur einmal verwendet werden kann („double Spending“ verhindert)
  - und ein unveränderliches öffentliches Buchungsjournal führt
- ohne zentrale Behörden oder vertrauenswürdige Dritte zu benötigen. [1] [2]

Das Geldprotokoll

Bitcoin Protokoll

- Beschrieben im Whitepaper „Bitcoin: A Peer-to-Peer on Electronic Cash System" von 2208 vom Pseudonym Satoshi Nakamoto, definiert das Protokoll Schlüssel-Mechanismen
  - wie kryptografischem Hashing für Blockverknüpfungen,
  - digitalen Signaturen für Transaktionsautorisierung
  - und ein Schwierigkeitsanpassungsalgorithmus zur Regulierung des Mining-Tempos (zehnminütige Intervalle pro Block.)[1] [3]
  - Das Netzwerk startete am 3. Januar 2009 mit dem Mining des 1 Blocks (Genesis-Blocks)

https://www.house-of-satoshi.ch/wp-content/uploads/2023/11/Bitcoin-Genesis-Block-3.-Januar-1024x542.jpg

- Bitcoin als Alternative zur zentralisierten Währung mit Inflation und Rettungsaktionen

Bitcoin Protokoll

- Im Kern verwendet das Protokoll „unspend Transaktion Output“ (UTXO) für Buchhaltungssalden
- Programmierte, begrenzten Ausgabe von 21 Millionen Bitcoins
- Verringerung der Blockbelohnungen alle 210.000 Blöcke, die sich etwa alle vier Jahre halbieren (Block reward Halving)
- Förderung programmierter Knappheit und Anreize für langfristige Sicherheit durch den Wettbewerb der Bergleute (Miner). [1] [5]

Entwicklung 2009 - 2025

- release version 0.1 software on January 9, 2009
- genesis block on January 3, 2009, Zeitstempel: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"
- Dieser Block etablierte die grundlegende Blockchain-Struktur mit einer Blockbelohnung von 50 BTC und einem Proof-of-Work-Konsens unter Verwendung von SHA-256-Hashing.
- Der frühe Betrieb basierte auf CPU-basiertem Mining durch eine kleine Gruppe von Entwicklern, darunter Hal Finney, der am 12. Januar 2009 die erste Peer-to-Peer-Transaktion von 10 BTC von Satoshi Nakamoto erhielt und damit die Transaktionsübertragung des Netzwerks verifizierte. [10]

Genesis Block

Entwicklung 2009 - 2025

- Am 22. Mai hat Bitcoin seinen ersten dokumentierten realen Bezahlvorgang, als der Programmierer Laszlo Hanyecz 10.000 BTC für zwei Pizzen im damaligen Wert von etwa 41 $ gekauft hat
- Börsen wie Mt. Gox entstanden und erleichterten erste Preisfindung, wobei Bitcoin bis März 0,003 $ pro Einheit und bis Oktober 0,08 $ erreichte
- Von 2011 bis 2012 entwickelte sich die Mining-Hardware von CPUs zu GPUs und FPGAs mit der Folge, dass Netzwerk-Hash-Rate von Kilohashes auf Gigahashes pro Sekunde wuchs
- Die erste Halbierung erfolgte am 28. November 2012 im Block 210.000, wodurch die Blockbelohnung auf 25 BTC reduziert und die Ausgaberate gemäß dem vom Protokoll vorgegebenen 210.000-Block-Zeitplan, halbiert wird
- zunehmender Schwierigkeitsgrad biete Anreize für die Bindung von Minern. [13]

Entwicklung 2009 - 2025

- Transaction Volumen niedrig, im Schnitt unter 1,000 pro Tag, aber das peer-to-peer-Netzwerk wächst an Nodes, die Transaktionen verifizieren.
- Bis 2013-2016 revolutionierten anwendungsspezifische integrierte Schaltkreise (ASICs) das Mining mit der Folge, das die Hardware für die Hash-Leistung bei wenigen Herstellern konzentriert wurde.
- Die Hash-Rate stieg bis Ende 2016 von Terahashes auf über 1 Exahash pro Sekunde und steigerte so die Sicherheit gegen Angriffe,
- der Schwierigkeitsgrad wird wie im Protokoll festgelegt, alle 2016 Blöcke angepasst ,

  um Blockzeiten von ~10 Minuten aufrechtzuerhalten . [15]
- Protokollaktualisierungen konzentrierten sich auf Skalierbarkeit und Robustheit, wie z. B. P2P-Relay Verbesserungen, aber Kernregeln wie 1 MB Blockgröße und Versorgungsobergrenze blieben unverändert
- Satoshi Nakamoto stellte die Kommunikation im Dezember 2010 ein und übergab die

  Entwicklung an Open-Source-Mitwirkende wie Gavin Andresen.

Entwicklung 2009 - 2025

- Transaktionszahlen stiegen auf zig-Tausende monatlich bis 2016, was ein breiteres Experimentieren widerspiegelt trotz Volatilität und verstärkter behördliche Prüfung. [16]
- Wichtige Soft Forks und Upgrades (2017-heute)
  - Segregated Witness (SegWit), definiert in BIP 141, BIP 143, BIP 144 und BIP 145, aktiviert als eine Soft Fork am 24. August 2017 bei Blockhöhe 481.824. [17] Dieses Upgrade trennte Signaturdaten (Zeuge) aus Transaktionsdaten in Blöcken
  - Ermöglicht Zweit- Schichtlösungen wie das Lightning Network. [18]
  - erhöhte auch die effektive Blockkapazität wodurch bis zu etwa 4 Megabyte möglich sind im Vergleich zur vorherigen 1-Megabyte-Grenze
  - Weitere: Taproot

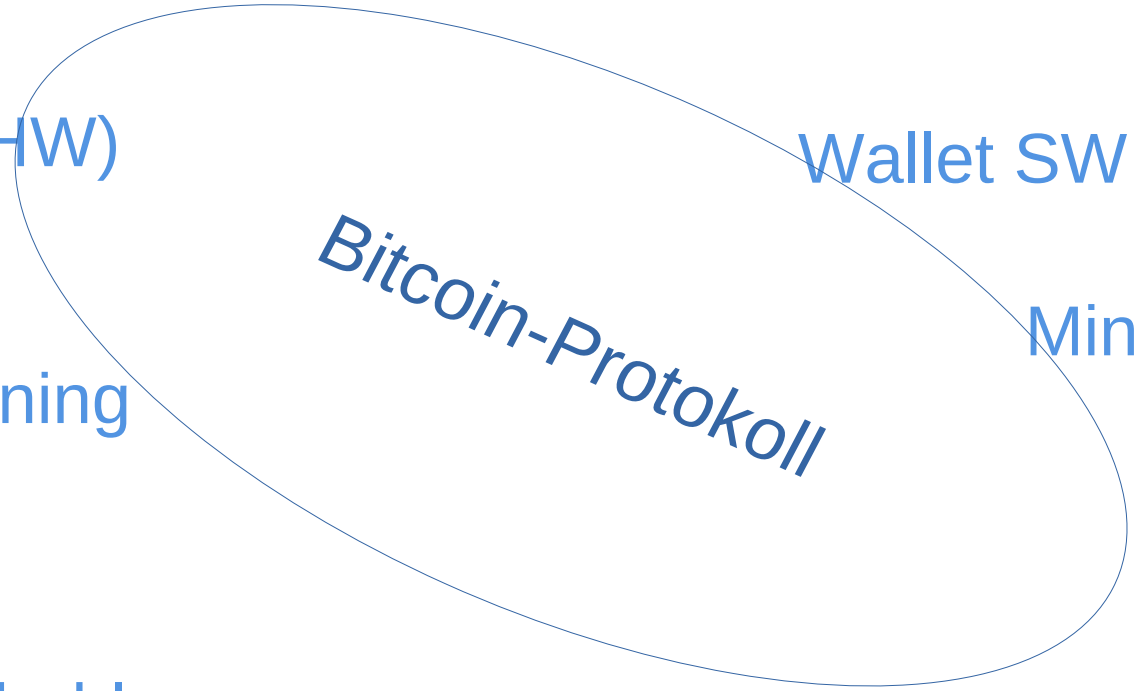
Inhalt

- Vorläufer
- Bitcoin Netzwerk
- Bitcoin
- Bitcoins transferieren
- Nodes
- Blockchain

Inhalt

- Mining
- Forks
- Bitcoin Governance und -Entwicklung
- Wallets

Elemente



Wallet (HW)

Wallet SW

Miner privat

Wallet Lightning

Nodes

Node reachable per Country

Miner professionell

Peer-to-Peer-Netzwerkprotokoll

- Peer-to-Peer-Netzwerkprotokoll
  - Das Bitcoin-Peer-to-Peer-(P2P)-Netzwerkprotokoll ermöglicht es einem dezentralen Netzwerk von Knoten, Blöcke und Transaktionen über TCP/IP-Verbindungen auszutauschen.
  - Dadurch wird die gemeinschaftliche Wartung der Blockchain ohne zentralen Koordinator gewährleistet.[28]
  - Knoten fungieren als vollständige Validatoren, die empfangene Daten unabhängig voneinander verifizieren, bevor sie diese weiterleiten.
  - Unterstützt werden Varianten
    - wie Archivierungsknoten (die die gesamte Blockchain speichern),
    - Pruned Nodes (die alte Blockdaten nach der Validierung verwerfen) u
    - und Simplified Payment Verification (SPV)-Clients (die nach Lightweight-Proofs fragen).[28]

Peer-to-Peer-Netzwerkprotokoll

- Peer-to-Peer-Netzwerkprotokoll
  - Das Protokoll verwendet standardmäßig Port 8333 für das Bitcoin-Mainnet, während das Testnet auf Port 18333 und das Regtest auf Port 18444 läuft.[6]
  - Die Peer-Erkennung beginnt mit Bootstrapping-Mechanismen, die in Implementierungen wie Bitcoin Core fest codiert sind, einschließlich DNS-Seeds wie seed.bitcoin.sipa.be, die Listen aktiver Knoten-IP-Adressen zurückgeben, gefiltert nach unterstützten Diensten (z. B. vollständigen Relay-Funktionen).[28]
  - Weitere Methoden umfassen fest codierte IP-Adressen im Client-Code und eine persistente Datenbank auf der Festplatte mit zuvor verbundenen Peers, die es ermöglicht, nach einem Neustart die Verbindung ohne vollständige Neuerkennung wiederherzustellen.[28]
  - Nach der Verbindung tauschen Knoten Adressen über addr- oder addrv2-Nachrichten (mit Unterstützung für jeweils bis zu 1.000 Einträge) als Antwort auf getaddr-Anfragen aus, wodurch die weitere Verbreitung bekannter Peers ermöglicht wird;

Peer-to-Peer-Netzwerkprotokoll

- Peer-to-Peer-Netzwerkprotokoll
  - DNS-Seeds bieten jedoch keine Authentifizierung, wodurch das Risiko der Einschleusung bösartiger Adressen besteht.[6][28]
  - Der Verbindungsaufbau beinhaltet einen Handshake, der damit beginnt, dass der initiierende Knoten eine Versionsnachricht sendet. Diese spezifiziert die Protokollversion (z. B. 70015 ab Bitcoin Core 0.18.0, wobei höhere Versionen Funktionen wie kompakte Blöcke ermöglichen), die unterstützten Dienste, einen Zeitstempel, die Adressen von Sender und Empfänger sowie eine Nonce zur Identifizierung der Verbindung.[6]
  - Der empfangende Knoten antwortet mit einer eigenen Versionsnachricht. Anschließend tauschen beide Knoten Versionsbestätigungsnachrichten (Verack) aus, um die Kompatibilität zu bestätigen.

Peer-to-Peer-Netzwerkprotokoll

- Peer-to-Peer-Netzwerkprotokoll
  - Verbindungen erfordern alle 30 Minuten Aktivität über Ping-/Pong-Nachrichten (auch bekannt als /page/Pong), um Timeouts zu vermeiden.[6][28] Neuere Upgrades, wie beispielsweise BIP 324 (eingeführt in Bitcoin Core v27.0 im April 2024), legen opportunistische Verschlüsselung auf der Transportschicht mithilfe eines Noise-Protokoll-Frameworks fest. Dadurch wird die Bandbreite leicht reduziert, während die Abwärtskompatibilität mit unverschlüsselten Version-1-Verbindungen erhalten bleibt.
  - Die Kernnachrichtensemantik bleibt jedoch unverändert.[29][30] Alle Nachrichten folgen einer festen Struktur: einem 24 Byte langen Header mit einer 4 Byte langen magischen Netzwerkkennung (z. B. 0xf9beb4d9 für das Mainnet), einem 12 Byte langen ASCII-Befehlsnamen (mit Nullbytes aufgefüllt), einer 4 Byte langen Little-Endian-Nutzlastlänge (bis zu 32 MiB) und einer 4 Byte langen Prüfsumme (die ersten 4 Bytes der Prüfsumme). SHA256(SHA256(payload))), gefolgt von der Nutzlast variabler Länge.[6]

Peer-to-Peer-Netzwerkprotokoll

- Peer-to-Peer-Netzwerkprotokoll
  - Zu den wichtigsten Nachrichtentypen gehören Bestandsmeldungen über inv (Auflistung von Objekt-Hashes wie Blöcken oder Transaktionen ohne vollständige Daten),
  - Anfragen über getdata (Angabe von Typen wie MSG_TX für Transaktionen oder MSG_BLOCK für Blöcke), Datennutzlasten wie tx für Transaktionen und block für vollständige Blöcke sowie Steuerungsmeldungen wie mempool (Ankündigung verfügbarer Transaktionen), feefilter (minimaler Gebührenschwellenwert für Relays) und reject (Fehlermeldungen).[6]
  - Compact Block Relay (BIP 152) optimiert die Weiterleitung von Blockgerüsten mit kurzen Transaktions-IDs mithilfe von cmpctblock, sendcmpct und verwandten Nachrichten, um die Latenz zu reduzieren.[6][31]

Peer-to-Peer-Netzwerkprotokoll

- Peer-to-Peer-Netzwerkprotokoll
  - Transaktionen und Blöcke verbreiten sich nach dem Gossip-Prinzip: Nach dem Empfang einer gültigen, unbestätigten Transaktion leitet ein Knoten diese per inv an Peers weiter, die bei Bedarf die vollständige Transaktion per getdata anfordern.
  - Blöcke verfahren ähnlich, wobei Knoten aktuelle Informationen bevorzugen und für die initiale Kettenfindung die Header-First-Synchronisierung (über getheaders/headers) nutzen.[6]
  - Peers, die sich durch ungültige Nachrichten oder Protokollverstöße verhalten, erhalten einen „Banscore“ und werden vorübergehend (standardmäßig 24 Stunden) getrennt, um die Netzwerkstabilität zu erhöhen.[28] B
  - bei diesem Design steht Robustheit im Vordergrund. Die Knoten halten typischerweise 8-10 ausgehende Verbindungen aufrecht und akzeptieren bis zu 125 eingehende Verbindungen, wobei die Anzahl dynamisch auf Basis der beobachteten Zuverlässigkeit angepasst wird.[28]

Vorläufer S. 286 ff

- Cypherpunks
  - Entwickler, Kryptographen, z.B. A Cypherpunks's Manifesto (1993) von Eric Hughes
- Ziel
  - sicheres, dezentrales, nicht vertrauensbasiertes Geldsystem
  - freies, offenes, digitales Währungssystem (z.B. Zugang für alle, unabhängig von Bonität)
  - Frei von staatlicher Kontrolle und der Notwendigkeit vertrauenswürdiger Drittparteien (keine Zensur, kein de-banking)
  - Sicherung der Privatsphäre / Anonymität wie bei Bargeld / (privacy) / Datenschutz / Schutz der privaten Kommunikation
  - Absicherung durch kryptographische Verfahren

Vorläufer S. 286 ff

- DigiCash von David Chaum 1980
  - Privatsphäre
  - Elektronisches Bargeld (z.B. CERN-Konferenz 1994)
- Hash Cash von Adam Back Ende 90-er Jahre
  - Ursprünglich zur Spam-Bekämpfung bei e-Mails gedacht
  - Grundstein für Proof-of-Work -Methode
- b-money von Wei Dai 1998
  - Geld durch Berechnung mathematischer Ressourcen
  - Grundlegende Prinzipien, die später in Bitcoin Verwendung fanden
- bit gold von Nick Szabo
  - Dezentrale Konsensmechanismen (Double Spending)

Double Spending – Blockchain S. 290 ff

- Digitale Währungseinheit darf nicht 2-mal ausgegeben werden
  - Physisches Geld hat diese Herausforderung nicht, da es nicht an 2 Orten gleichzeitig sein kann
  - Eine Datei, die eine digitale Münze repräsentiert, könnte aber an mehrere Empfänger gesendet werden
  - Aus diesem Grund verwendet Bitcoin ein öffentliches Buchungsjournal (Ledger), in dem alle Transaktionen aufgezeichnet und verifiziert werden und sicherstellt, dass jede Einheit nur einmal ausgegeben wird.
  - Genesis -Block:Erster Block der Blockchain „Block 1“, „Miner“ Satoshi Nakamoto, enthät 50 Bitcoin
  - „Software“ Bitcoin 1.0 veröffentlich auf Sourceforge 09.01.2009,12.01.2009 Beginn Bankenkrise
  - Alle10 Minuten wird ein neuer Block angefügt, bis Block 22,000 einziger Miner, bis Block Block 54.316 dominierender Miner, 50 Bitcoin Belohnung bis zum 1, Halving 2012
  - Schätzung: Satoshi Nakamoto besitzt ungefähr 1.125.150 Bitcoin

Blockchain = Buchungsjournal mit allen Transaktionen

Bitcoin Eigenschaften S. 300

- Dezentral: Peer-to-Peer Netzwerk mit 1000-en von Knoten weltweit, historische Verfügbarkeit 99,985 %,
- 21.000.000 Bitcoins – fest!
- Open Source – transparent, „Don’t trust, verify“, gilt für Software + Transaktionen in der Blockchain (Finanzamt)
- Neutral + demokratisch – Zugang für jeden (unabhängig von regulatorischen Zwängen oder Geschäftsbedingungen von Banken
- Zensurresistenz – Dystopien wie Social Scoring, Debanking etc.
- Unveränderbarkeit – gewährleitet Unveränderlichkeit und Unverfälschtheit (SHA-256-Hash)
- Pseudonymität – Identität muß nicht offengelegt werden – Transaktionen zwischen Bitcoin – Adressen, nicht Idenditäten
- Überprüfbar und sicher – Blockchain und Kryptographie

Bitcoin Einstieg s.307 ff

- Ausführungen beziehen sich auf Hardware-Wallet, nicht Börsenkonto
- Börsenwallet (Börsenkonto) gehören die Satoshies der Börse; bei Pleite (FTX) weg, keine Einlagensicherung
- Wie bei normalem Geld, ist erst abgehobenes Geld eigenes Geld, vorher gehört es der Bank
- Bankkonto stark reguliert, zB KyC, Identitätscheck
  - Wer regulatorische Kriterien nicht erfüllt, bekommt kein Konto
  - Bankensystem : Zentrales Netz, alle Punkte mit einer Quelle verbunden
- Bitcoin, dezentral, vermascht

Bitcoin Netz schrittweise verstehen S.326

Überweisung:

- Bob öffnet seine Wallet und gibt Annes Public Adress in das Empfängerfeld ein
- Die Wallet erstellt eine Transaktion und signiert Sie mit Bobs private Key
- Wenn die erzeugte Transaktion Bobs Mitteln entspricht, wird Sie von BTC – Netzwerk als gültig akzeptiert
- Die BTC kann nun von dem abgerüfen werden, der den private Key zu dieser öffentlichen Adresse besitzt
-
-

Ablauf

Bitcoin Netz schrittweise verstehen S.330/331 Abb.

- Wallet
  - Speichert Private Key, der Zugang zu einer Adresse in der Blockchain gibt, in der BTC aufgezeichnet sind.
  - Speichert keine Bitcoin
- Seed
  - „Samen“: Ausgangspunkt für Private Key, Public Key und Public Adress
  - HD Wallet Abb S.328
  - Private Schlüssel werden nicht weitergegeben, nur Public Keys und Adressen
  - 24 englische Wörter (Mnemonic Code)
  - Werden bei Inbetriebnahme der Wallet erzeugt per Zufalsgenerator
  - Serie von Wörtern + Reihenfolge
  - In BIP 39 (Bitcoin Improvement Proposal) festgelegt

- BIP 39

Bitcoin Netz schrittweise verstehen S.335/334 Abb.

- Seed
  - Mit der Seed kann die Wallet auf andere Geräte übertragen bzw wiederhergestellt werden
  - Von einem selbst oder von einem anderen → muß geheim bleiben
  - 24 aus 2028 Wörtern in der richtigen Reihenfolge zu erraten, ist ebenfalls unmöglich
  - Seed Phrase ist der „Hauptschlüssel“, aus dem alle weiteren privaten Schlüssel abgeleitet werden

- Hierarchie: Seed → Private Key → Public Key → Adresse

Bitcoin Netz schrittweise verstehen S.336 ff

- Transaktion
  - Wohin gehen die Bitcoins → Empfängeradresse (text, QR-Code etc)
  - Wallet: Funktion Senden
  - Die Transaktion beinhaltet
    - Absenderadresse
    - Zieladresse
    - Betrag
    - Prio
  - Validierung durch Benutzer auf Wallet
  - Wallet: Signieren
    - Mit Private Key und Hash auf alle Daten
  - Senden

Bitcoin Netz schrittweise verstehen S.336 ff Abb. 338

- Transaktion
  - Senden
    - Transaktion wird dem Bitcoin-Netzwerk gemeldet und als unbestätigt in der Wallet angezeigt, solange Sie nicht von einem Miner in die Blockchain eingetragen wurde. Die Dauer ist abhängig von der gewählten Prio und Auslastung des Netzwerks. Transaktion wird danach als bestätigt angezeigt.
  - Miner überprüfen die Transaktion und bündeln sie zusammen mit anderen Transaktionen in einem Block.
  - Der Miner, der zuerst das Proof-of-Work-Problem löst, darf den Block zur Blockchain hinzufügen und erhält die Blockbelohnung sowie die Transaktionsgebühren.
  - Die Nodes verifizieren die Gültikeit des neuen Blocks und propagieren Ihn in das Netzwerk. Nicht regelkonforme Blöcke werden nicht akzeptiert.
  - Der Block wird im Node in die bestehende Blockchain eingefügt. Damit ist der Block offiziell, und damit auch die Transaktion.

Bitcoin Netz schrittweise verstehen S.339

- Überweisung im Bitcoin Netzwerk

Transaktions-Hash	36dfeat0397af...
Transaktions-Hash der Transaktion mit der die Bitcoins ursprünglich empfangen wurden	A0efbd2a016ee ...
Betrag	1,51 BTC
Wechselgeldadresse UTXO „unspent Transaction Output“	Bei eiiner Zahlung nicht verwendetes Guthaben wird mit einer neuen Bitcoin-Adresse auf die Wallet zurücküberwiesen.
Empfängeradresse abgeleitet aus öffentlichem Schlüssel des Empfängers	bc1qar0srr7s
Signatur des Senders	
Öffentlicher Schlüssel des Senders	

- Da es unwahrscheinlich ist, das immer nur passende Beträge überwiesen werden, wird jede Überweisung im Bitcoin Netzwerk über 2 Transaktionen abgewickelt:
  - Der gewünschte Überweisungsbetrag
  - Rücküberweisung des Wechselgeldes unter neue Adresse → Einzahlung direkt aus dem Bitcoin-Netzwerk

Bitcoin Netz schrittweise verstehen S.343

- Transaktionsgebühr
  - In der Wallet kann die Prio festgelegt werden, mit der die Transaktion ausgeführt werden soll
  - Abhängig von der Auslastung des Netzwerks
  - Hoch: Transaktion wird zügig ausgeführt
  - Niedrig: Ausführung der Transaktion wenn möglich
  - Gebühr wird nicht im Voraus ausgewiesen, nur als Differenz zwischen überwiesenem Betrag und Wechselgeld
  - Man kann auch fest Beträge eingeben in der Wallet
  -
  -

Bitcoin Netz schrittweise verstehen S.343

- Nodes
  - Jeder Node hält die Blockchain
  - Kommunizieren über Peer-to-Peer Netzwerk
  - Server auf dem ein Bitcoin-Client läuft (die Bitcoin-Software)
    - Führt das Bitcoin-Protokoll autonom aus → Befolgt die Regeln des Netzwerks
    - Gibt Informationen weiter, wenn protokollkonform → neue Transaktionen und Blöcke mit alten Transaktionen → Hält eine einzelne Kopie der Blockchain und aktualisiert sie ständig → es gibt keine zentrale Blockchain → keine Vertrauen auf eine Zentral Stelle, da im Design gar nicht vorhanden.
    - Je nach Konfiguration und Auslastung des Netzwerks unterhält 1 Node eine feste Anzahl von aktuell 8 ausgehenden Verbindungen sowie eine variable Anzahl von bis zu 117 eingehende Verbindungen.[114] (aus https://de.wikipedia.org/wiki/Bitcoin)

Bitcoin Netz schrittweise verstehen S.343

- Um sich mit dem Bitcoin-Netz zu verbinden, benötigt die Bitcoin-Software[115] die Kenntnis von IP-Adressen anderer Bitcoin-Nodes.
- Für die initiale Suche nach anderen Nodes (Bootstrapping) wird das Domain Name System verwendet. Der Bitcoin-Client löst einen Domainnamen auf, um die IP-Adressen mehrerer anderer Bitcoin-Nodes zu erhalten. Die für das Bootstrapping verwendeten Domainnamen sind in der Bitcoin-Software fest integriert und die Services werden von Mitgliedern der Bitcoin-Community betrieben.
- Bereits verbundene Bitcoin-Nodes tauschen bekannte IP-Adressen untereinander aus. Schlägt das Bootstrapping fehl, greift der Bitcoin-Client auf eine mitgelieferte Liste von Bitcoin-Nodes zu.
- (aus https://de.wikipedia.org/wiki/Bitcoin)

Bitcoin Netz schrittweise verstehen S.343

- Mempool (Memory Pool)
  - Sammelt alle neuen Transaktionen, die noch nicht ausgeführt sind → Warteschlange für transaktionen, die von Minern noch in Blöcke aufgenommen werden müssen
  - Miner arbeiten die Transaktionen entsprechend der Proirität und damit entsprechend der Höhe der Transaktionsgebühr ab
  - Ändert sich ständig, da neue Transaktionen hinzukommen und bestätigte Transaktionen aus dem Mempool entfernt werden
  - Mempool groß → hohes Transaktionsvolumen → Bitcoin-Netzwerk langsam
    Mempool klein → Bitcoin-Netzwerk schnell
  -
  -
  -

Bitcoin Netz schrittweise verstehen S.348

- Blockchain → Wiki
  - Textdatei
  - Funktion einer Datenbank
  - Ungefähr 700 GB → Statistiken z.B. bei https://ycharts.com/indicators/bitcoin_blockchain_size
  - Die Blockchain (deutsch „Blockkette“) ist das Journal, in dem alle Bitcoin-Transaktionen verzeichnet werden. Sie besteht aus einer Reihe von Datenblöcken, in denen jeweils eine oder mehrere Transaktionen zusammengefasst und mit einer Prüfsumme versehen sind. Neue Blöcke werden in einem rechenintensiven Prozess erschaffen, der sich Mining nennt, und anschließend über das Netzwerk an die Teilnehmer verbreitet.[119] https://de.wikipedia.org/wiki/Bitcoin

Bitcoin Netz schrittweise verstehen S.348

- Blockchain → Wiki
  - Die Transaktionen eines Blocks werden durch einen Merkle-Baum paarweise miteinander gehasht und nur der letzte Hashwert, der Root-Hash, als Prüfsumme im Header des Blocks vermerkt.
  - Die Blöcke werden dann mithilfe dieses Root-Hashes verkettet. Jeder Block enthält im Header den Hash des gesamten vorherigen Blockheaders, so ist die Reihenfolge der Blöcke eindeutig festgelegt. Außerdem ist dadurch auch das nachträgliche Modifizieren vorangegangener Blöcke bzw. Transaktionen praktisch ausgeschlossen, da die Hashes aller nachfolgenden Blöcke in kurzer Zeit ebenfalls neu berechnet werden müssten.
  - Der erste Block in der Blockchain ist vorgegeben und wird Genesisblock genannt.
  - Beispiel S. 351 → 6 Blöcke für die absolute Sicherheit

Blockchain

Merkle-Baum

https://de.wikipedia.org/wiki/Hash-Baum#/media/Datei:Hash_Tree.svg

https://de.wikipedia.org/wiki/Hashfunktion

- Eine Hashfunktion oder Streuwertfunktion ist eine Abbildung, die eine große Eingabemenge, die Schlüssel auf eine kleinere Zielmenge, die Hashwerte, abbildet.
  - bei kryptologischen Hashfunktionen: Chaos oder Lawineneffekt – Die Hashfunktion soll eine gute Diffusion besitzen; ähnliche Quellelemente (Eingabewerte) sollen zu völlig verschiedenen Hashwerten führen. Im Idealfall verändert das Umkippen eines Bits in der Eingabe durchschnittlich die Hälfte aller Bits im resultierenden Hashwert.
  - bei kryptologischen Hashfunktionen: Konfusion – Vom Hashwert sollen keine Rückschlüsse auf den Eingabewert gemacht werden können.
  - bei kryptologischen Hashfunktionen: Unumkehrbarkeit – Es soll kein praktisches Verfahren möglich sein, das aus einem Hashwert den Eingabewert bestimmt.
  - Hash 256 https://emn178.github.io/online-tools/sha256.html
  -

Bitcoin Netz schrittweise verstehen S.356

- Blockchain → Wiki
  - Sicherheit
    - Opensource
    - Viele Nodes, die einzeln einer Änderung des Protokolls zustimmen müssen
    - Die Mehrheit der Nodes müssen einzelnen Transaktionen zustimmen, bevor sie verifiziert ist.

Bitcoin Netz schrittweise verstehen S.356

- Bitcoin Mining → Wiki
  - Seitenerschaffungsabteilung → Schürfen
  - Status: Überweisung überprüft und validiert, jedoch noch nicht in die Blockchain eingetragen
  - Herausforderung: Die Blockchain muß nun so aktualisert werden, dass jeder Node im Netzwerk die gleichen Version besitzt und damit überall im >netzwerk die gleichen Kontostände angezeigt werden. (Double Spending → kein Node kann die Blockchain fortschreiben.
  - erfordert einen Konsens-Mechanismus → Proof-of-Work (POW)
  - Kernidee: Miner müssen Rechenleistung erbringen, um Transaktionen zu validieren und neue Blöcke in die Blockchain anzuhängen.
  - Hierfür wird Hardware, Energie und Zeit benötigt

Physischer Prozess, als Komponente des realen Gegenwerts von Bitcoins

Bitcoin Netz schrittweise verstehen S.356

- Bitcoin Mining → Wiki
  - Prozess stellt sicher, dass jede Transaktion dem Protokollverlauf entspricht und jede Transaktion eindeutig und unwiderruflich ist.
  - Blöcke anhängen ist kostspielig → man schätzt, ein Angreifer müsste mehr als die Hälfte der Rechenleistung des Netztwerkes besitzen, um die Blockchain zu manipulieren.
  - Dezentralisierung: Keine Autorothät besitzt die Kontrolle. Jeder Teilnehmer kann Miner werden → Kein Single-Point-of Failure (SpoF) → Miner-HW → Wiki
  -

Bitcoin Netz schrittweise verstehen S.356

- Bitcoin Mining → Wiki
  - Prozess
    - Alle Transaktionen („mit gültigem Überweisungszettel“, bereits durch Mehrzahl der Nodes geprüft) werden in MEM-Pool gesammelt
    - Miner konkurrieren um nächsten Block
    - Sie wählen eine bestimmte Menge an Transaktionen aus und fügen sie zu einem Block zusammen.
    - Proof-of-Work: Erzeugen eines Hashwertes mit vom Netzwerk bestimmten Schwierigkeitsgrad aus Transaktionen und Daten des letzten gültigen Blocks in der Blockchain (Nonce finden) → Lotterie, da die Nonce (Number used once) per Ausprobieren gefunden werden muss

Bitcoin Netz schrittweise verstehen S.359

- Bitcoin Mining → Wiki
  - Prozess
    - Sobald eine gültige Nonce dem Header hinzugefügt wurde, ist der Block gültig und wird
      - vom Miner der Blockchain des Miners hinzugefügt, der Miner erhält BTC für seine Arbeit
      - Dem gesamten Netzwerk bekannt gemacht
      - Von allen Minern und Nodes überprüft und Ihrer Blockchain angefügt
      - Danach ist die Transaktion gültig
      - (nach 6 Blöcken gilt die Transaktion als sicher)
      - Löst 2 Problem
        - kein Double-Spending
        - Byzanthinische Generäle

Bitcoin Netz schrittweise verstehen S.362

- Bitcoin Mining → Wiki
  - Prozess
    - Byzanthinische Generäle
      - Konsens: Nur gemeinsamer Angriff oder Rückzug führt zum Sieg
      - Auswirkungen von Entscheidungen von Verrätern müssen minimiert werden
      - Bitcoin:
        - Miner = Generäle, deren Konsensentscheidungen mit Kosten verbunden sind
        - Validierung durch Mehrheit der Nodes und Festhalten in einer unveränderbaren Blockchain. Einfache Überprüfung durch Anwendung derselben Hashfunktion, die zum Nonce geführt hat.

Bitcoin Netz schrittweise verstehen S.362

- Bitcoin Mining → Wiki
  - Difficulty Adjustment
    - Nach 2016 Blöcken, ungefähr alle 2 Wochen wird der Schwierigkeitsgrad um den erforderlichen Hash zu finden, überprüft
    - Ziel: Alle 10 Minuten ein neuer Block, unabhängig davon, wieviel Rechenleistung dem Block hinzugefügt oder entzogen wurde
  - Hashrate
    - Hash-Berechnungen im Netzwerk pro Sekunde → verfügbare Rechenleistung im Netz
    - KH/s, …. 31.10.25 $1x10^{9}$ TH/s ($1x10^{21}$) → Statistiken → entspricht der Wahrscheinlichkeit für einen Miner, einen gültigen Block zu finden
    -

Bitcoin Netz schrittweise verstehen S.365

- Block → Wiki
  - Body enthält Transaktionen („Überweisungszettel“)
  - Header
    - Versionsnummer
      - Zur Unterscheidung einzelner Blöcke; wichtig bei Protokolländerungen
    - Hash des vorhergegangene Blocks
      - Verknüpft den Vorgänger-Block mit dem neuen Block (Blockchain)
    - Merkle-Root-Hash
      - Hash auf die im Block enthaltenen Transaktionen
      - Würde eine Transaktion nachträglich verändert, stimmte der neue Hash nicht mehr mit Hash im Header überein → Block ungültig
    - Timestamp
      - in Sekunden nach dem 1.1.1970, Entstehungszeitpunkt des Blocks
    -

Bitcoin Netz schrittweise verstehen S.365

- Block → Wiki
  - Schwierigkeitsziel
  - Anzahl führender Nullen vor einem Blockhash
  - Block-Hash
  - Zentrales Konzept
    - Aus Hash des Vorigen Blocks
    - Merkle-Root Hash
    - Zeitstempel
    - Schwierigkeitsgrad
    - Nonce (number used once, „endgültige Nummer“
    - 64-stelliger Hexadezimal Code mit einer bestimmten Anzahl führender Nullen
    - Die Anzahl der führenden Nullen wird durch den Schwierigkeitgrad (Difficulty Adjustment) vorgegeben
    - Der Schwierigkeitsgrad wird alle 2016 Blöcke angepasst, um das Ziel zu erreichen, alle 10 Minuten einen neuen Block aufzunehmen.

Bitcoin Netz schrittweise verstehen S.365

- Block → Wiki
  - Block-Hash
    - Nonce
      - Die Elemente des Headers sind festgelegt (Merkle-Root-Hash kann verändert werden, in dem neue Transaktionen oder deren Reihenfolge verändert wird)
      - Ein Hash auf den Header würde immer den selben Hash ergeben, der in der Regel nicht dem vorgegebene Schwierigkeitsgrad entspräche
      - Deshalb kann der Miner eine bleliebige Zahl wählen (in der Regel 0) und erhöht sie schrittweise, bis er einen Hash gefunden hat, der dem geforderten Schwierigkeitsgrad entspricht.
      - Prozess rein zufällig → Lotterie
  -

Bitcoin Netz schrittweise verstehen S.362

- Bitcoin Mining → Wiki
  - Block Reward
    - Bitcoin-Supply-Schedule
      - Gesamtmenge 21 Mio BTC
      - 1. Blockbelohnung 50 BTC
      - Alle 210.000 Blocke (= 4 Jahre) wird die Belohnung halbiert
      - 2024 3,125 BTC
      - + Transaktionsgebühren
    - Orphan-Block
      - Wenn 2 Miner fast gleichzeitig einen Block finden
      - Blockchain wird in 2 Teile aufgeteilt
      - Weitere Blöcke werden angefügt, bis einer der beiden Ketten längere ist als die andere
      - Die kürzere wird aufgelöst und in den MEM-Pool zurückgespielt.

Bitcoin Netz schrittweise verstehen S.362

- Softfork oder Hardfork
  - Softfork
    - Von der Bitcoin-Community akzeptierter Update des Bitcoin-Protokolls
  - Hardfork
    - Nur von einem Teil der Bitcoin-Community akzeptierter Update des Bitcoin-Protokolls → neue Bitcoin → BitcoinCash (8 MB Blockgröße), von Minern initiiert, hat sich nicht durchgesetzt, weil die Nodes die Änderung nicht aktzepiert haben (leistungsfähigere Hardware)
  - Bitcoin-Governance
    - Bitcoin-Core → Bitcoin.org
      - Hauptversion der Bitcoin-Software
      - Betreibt fast alle Nodes
      - Sicherheit, Skalierbarkeit, Verbesserung
      - Opensource
      -

Bitcoin Netz schrittweise verstehen S.362

- Bitcoin-Core → Bitcoin.org
  - Hauptversion der Bitcoin-Software
  - Läuft auf fast allen Nodes
  - Sicherheit, Skalierbarkeit, Verbesserung
  - Opensource
  - Bitcoin Improvement Proposal (BIP)
    - Vorschlag
    - Diskussion und Überprüfung
    - Akzeptance oder Ablehnung
    - Implementierung
    - Veröffentlichung und Adaption
    - Jeder Node eiintscheidet einzeln, ober upfdated oder nicht

Bitcoin Netz schrittweise verstehen S.362

- Entwickler
  - Freiwillige
  - Unternehmen und Institutionen
  - Aktuell auf GitHub 800 ??? Mitwirkende
- Gewaltenteilung
  - Entwickler („Legislative“)
    - Können Änderungen vorschlagen → BIP
    - Nodes entscheiden über Implementierung
  - Nodes („Judikative“)
    - Nodes entscheiden über Implementierung
    - Überwachen die Einhaltung des Protokolls

Bitcoin Netz schrittweise verstehen S.362

- Wallets
  - Bicoins Empfangen und erhalten
  - Bitcoins liegen immer in der Blockchain, die Wallet verwaltet nur die Bitcoin-Adressen (Schlüssel), die einem selbst gehören
  - Hot Wallets (ständig mit Internet verbunden über ggf. unsicheres Gerät, auf dem sie installiert sind)
    - Desktop, Online (Kauf bei Börse und läßt sie dort liegen), Mobile
    - Drittanbieterrisiko
  - Cold Wallets („unabhängig von PC,Phone etc.)
    - Paper, Hardware, Brain
    - Eigenständige Verwahrung
    - Harware-Wallet: Mit PC über Applikation verbunden, an die aber keine sicherheitsrelevanten Informationen weitergegeben werden (Schlüssel). Alle sicherheitsrelevanten Operationen (Signaturen) geschehen auf der Hardware-Wallet

Bitcoin Netz schrittweise verstehen S.362

- Wallets
  - Backup/Seed
    - 24 englische Worte
    - Mit Ihnen können die Bitcoins auf jeder anderen Wallet wiederhergestellt werden
    - Abschreiben und aufbewahren
    - Kein Photo, nicht auf PC oder Cloud speichern
    - Am besten Stahl
    - Seed weg, Bitcoin weg!
  -

Bitcoin Netz schrittweise verstehen S.406

- Wallets
  - Backup/Seed
    - Bitcoin stirbt nicht – Sie schon!
      - Zugriff auf Wallet vorhanden
        - Neue Wallet anschaffen und neuen Seed erstellen
        - Alle BTC von der alten auf die neue Wallet übertragen
        - Sicherstellen, dass die Transaktion(en) bestätigt wurden
      - Wallet weg – Seed vorhanden
        - Mit Hilfe der Seed BTC-Bestand auf neuer Wallet wiederherstellen
      - Seed verloren und kein Zugang zur Wallet
        - Endgültiger Verlust

Bitcoin Netz schrittweise verstehen S.406

- Wallets
  - Backup/Seed
    - Bitcoin stirbt nicht – Sie schon!
      - Zugriff auf Wallet vorhanden
        - Neue Wallet anschaffen und neuen Seed erstellen
        - Alle BTC von der alten auf die neue Wallet übertragen
        - Sicherstellen, dass die Transaktion(en) bestätigt wurden
      - Wallet weg – Seed vorhanden
        - Mit Hilfe der Seed BTC-Bestand auf neuer Wallet wiederherstellen
      - Seed verloren und kein Zugang zur Wallet
        - Endgültiger Verlust (Schätzung: 20% aller Bitcoins)

Bitcoin Netz schrittweise verstehen S.408

- Risiko
  - Bitcoin verschlüsselt mit SHA256
  - $(2^{32})^8$ =+/- 2^{256} = $(4{,}2\ \text{Mrd})^8$
- Hodl
  - Bitcoin halten (aus Tippfehler hold → hodl)
  - Auch wenn starke Korrekturen erfolgt sind
- Halving
  - Halbierung der Belohnung für Miner alle 210.000 Blöcke
  - 210.000 x 10 Minuten = $2{,}1^6$ Minuten
  - 365 * 24 *60 = 525600 Minuten pro Jahr
  - Also ungefähr alle 4 Jahre ein Halving
  - Bisher: Nach jedem Halving steigt der Preis Abb.74

Lightning-Netzwerk S.451

- Transaktionen
  - Werden off-chain (ausserhalb der Blockchain abgewickelt)
  -
- MultiSig
  - Transaktionen werden erst authorisiert, wenn mehrer Signateure ihre Signatur gleichzeitig leisten
- MultiSig-Wallet
  - Jeder Teilnehmer schließt beliebig viel BTC darin ein und erhält dafür Schluessel (Wird das geprüft ?)
  - Sind genügend Transaktionen vorhanden, wird der letzte Stand auf die Blockchain geschrieben
  - Mehr Transaktionen je Sekunde
  - Anschließend wird die Zahlung als Bitcoin-Transaktion abgewickelt.
  -

Lightning-Netzwerk S.451

- Vorteile
  - Anonym, fast wie Bargeld
  - Ausgenommen De-Anonymisierung des Bargelds
- Geringe Gebühren
- Schnelligkeit
- Kritik
  - Kapazität
  - Gefahr der Zentralisierung
- Produkt: WalletofSatoshi

Bitcoin life

- Ende