Blockchain-Technologie in Bezug auf Bitcoin

Elias Kounakas
8B

BG|BRG Mössinger
9020 Klagenfurt am Wörthersee

Betreuer: Franz Furtschegger
Abgabedatum: TT.MM.JJ

Inhaltsverzeichnis

Kapitel 1

Einleitung

1.1 Was ist Bitcoin?

Häufig wird Bitcoin einzig und allein mit der Kryptowährung selbst assoziiert. Der Begriff Bitcoin umfasst jedoch alle Konzepte und Technologien, die das digitale Zahlungssystem ermöglichen. (Vgl. Antonopoulos, 1) Eines dieser Konzepte ist das Bitcoin-Netzwerk, wodurch Nutzer Zahlungen propagieren und verifizieren können. Mit der Kryptowährung Bitcoin selbst kann man Käufe tätigen, Geld an Verwandte oder Organisationen versenden und Waren verkaufen, genauso wie es bei einer herkömmlichen Währung der Fall ist. Der große Unterschied zwischen Bitcoin und herkömmlicher Währung ist, dass es kein handgreifliches Bitcoin gibt. Die Menge an Bitcoin, die man besitzt, wird durch die Zusammenfassung aller erhaltenen Transaktionen auf die eigene Bitcoin-Addresse erlangt.

Als Grundlage für Transaktionen in Bitcoin dient die assymetrische Kryptographie, ein kryptographisches System, welches auf einem Schlüsselpaar basiert. Das Schlüsselpaar setzt sich aus dem privaten Schlüssel und öffentlichen Schlüssel zusammen. Mit dem öffentlichen Schlüssel wird die Bitcoin-Addresse des Nutzers abgeleitet, welche benötigt wird, um Zahlungen zu empfangen. Ähnlich wie der PIN oder das Passwort bei einem herkömmlichen Bankkonto lassen sich Zahlungen mit dem privaten Schlüssel im Bitcoin-Netzwerk tätigen.

In Bitcoin gibt es keine zentrale Macht oder Bank, die neues Geld produziert. Stattdessen werden neue Bitcoins mit einem Prozess names Mining gewonnen, welcher die

Lösung zu einem mathematischen Problem sucht und gleichzeitig neue Transaktionen verifiziert. Alle 10 Minuten wird eine neue Lösung gefunden und alle Miner starten wieder von vorne. Das bedeutet, dass jeder Nutzer auch ein Miner sein kann und Transaktionen maximal 10 Minuten brauchen, um verifiziert zu werden.

Die kleinste Einheit von Bitcoin ist der Satoshi, welcher nach dem Erfinder von Bitcoin, Satoshi Nakamoto benannt wurde. Ein Bitcoin entspricht dem Wert von 100 Millionen Satoshis. Da der Wert von Bitcoin in den letzten Jahren exponentiell gestiegen ist, gewann der Satoshi immer mehr an Bedeutung. Transaktionen haben meist einen 8-stelligen Dezimalwert unter 1 (Bsp.: 0,00140209 BTC), was konventionell schlecht darstellbar ist. Hier wäre es sinnvoll, den Wert in Satoshis anzugeben, also 140 209 Satoshis.

1.2 Geschichte von Bitcoin

2008 veröffentlichte jemand unter dem Alias Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System". (Vgl. Nakamoto 2008) Mit dieser Arbeit erfand Nakamoto die erste Kryptowährung, Bitcoin. Er kombinierte frühere Erfindungen mit seinen Ideen und erfand somit das erste komplett dezentralisierte, elektronische Zahlungssystem. Die Schlüsselrolle spielte die Implementierung von einem verteilten Aufwand der Prozessorkraft, wodurch alle 10 Minuten demokratisch für die korrekte Folge von Aktionen abgestimmt werden kann.

In dem Jahr 2011, als Nakamoto sich von seinem Projekt abwandte und es nicht länger optimisierte, stieg Bitcoin mit einem Aufschwung von 3000% in nur drei Monaten von 1USD auf 32USD. Explodiert ist der Wert jedoch erst 2018, als Bitcoin einen Höchstwert von 19,000USD erreichte. Im vierten Quartal des Jahres 2021 hat Bitcoin seinen bislang höchsten Wert (Stand: 24/08/2022) von 67,000USD erreicht. (Vgl. Coinbase 2022)

Kapitel 2

Struktur des Bitcoin-Netzwerkes

2.1 Peer-to-Peer-Netzwerk

Im Bitcoin-Netzwerk gibt es keine zentrale Macht. Alle verbundenen Computer arbeiten miteinander als Peers. Peer-to-Peer bzw. P2P heißt, dass alle teilnehmenden Computer die gleichen Rechte und Hindernisse haben. Die einzelnen verbundenen Computer nennt man Nodes. Jede Node kommuniziert rund um die Uhr mit ihren benachbarten Nodes. Nodes können Informationen abfragen, weiterleiten und verifizieren. Das Bitcoin-Netzwerk ist demnach die Gesamtheit aller Nodes.

Was passiert aber, wenn eine Node für bösartige Zwecke falsche Informationen an andere Nodes verschickt? Dafür hat man ein Vertrauens-System im Bitcoin-Netzwerk implementiert. Bevor eine Node empfangene Informationen abspeichert, prüft sie diese auf Korrektheit in Bezug auf den derzeitigen Standard. Dieser Standard wird im BIP (Bitcoin Improvement Proposal) festgelegt, welcher periodisch immer neue Richtlinien festlegt. (Dashjr, 2011) Natürlich hat das BIP keine Macht über die Nodes, diese können nämlich selber entscheiden, ob sie nun nach den neuen Richtlinien arbeiten wollen oder nicht. Jedoch übernehmen die meisten Nodes mit einem kurzen Update den neuen Standard, da dieser lediglich für das Interesse der Teilnehmer entwickelt wird.

Bitcoin Nodes sind nicht leistungshungrig und benötigen wenig Energie, solange sie nicht für Mining genutzt werden. Deswegen ist es für so gut wie jede Person möglich, selber zu Hause eine Bitcoin Node zum Laufen zu bringen. Die Zwecke für diese Node könnnen aber von Person zu Person variieren. Zum einen gibt es Leute, die mit ihrer

Node nur mithören wollen, zum anderen aber auch diejenigen, die durch Mining Geld verdienen wollen. Aus diesem Grunde gibt es verschiedene Implementierungen und Rollen von Nodes.

2.1.1 Full Node

Eine Full Node benötigt von allen Nodetypen am meisten Speicherplatz, ist dafür aber die mächtigste und fasst alle Funktionen in einer Node zusammen. Der distinkte Unterschied von der Full Node ist, dass diese die komplette Blockchain herunterlädt und verifiziert. Der benötigte Speicherplatz der Blockchain liegt bei 423GB (Stand: 25/8/2022).

Damit die Blockchain erweitert wird und alle Transaktionen verfiziert werden könnnen, müssen sogenannte Mining Nodes alle 10 Minuten eine Lösung zu einem mathematischen Problem finden, indem sie mit der Hashfunktion SHA256 einen bestimmten Wert suchen. Das muss vor allem schnell und präzise geschehen, damit die Chance, die Lösung als Erstes zu finden, maximiert wird. Mining Nodes profitieren vor allem von modernen GPUs, welche hunderte Millionen Hashes pro Sekunde berechnen.

Die wahrscheinlich beste Node fÍür den Otto Normalverbraucher ist der SPV Client (Simplified Payment Verification Client). Dieser installiert lediglich eine Wallet, eine Kopie der Block Header und stellt eine Verbindung zum Bitcoin-Netzwerk her. Er ist einzig und allein dafür ausgestattet, Transaktionen auf das eigene Konto zu empfangen und Geld zu versenden. (Antonopoulos, 2017, S. 172f)

2.2 Die Blockchain

Die Blockchain ist eine Datenstruktur, welche Transaktionen in miteinander verbundenen Blöcken speichert. Visualisieren kann man diese wie einen Turm von Blöcken. Der unterste Block dient als Fundament und die Anzahl der Blöcke bestimmt die Höhe. Ein neuer Block wird hinzugefügt, wenn ein Miner eine neue Lösung mit der SHA256 Hashfunktion gefunden hat. Der Miner kann dann aussuchen, welche Transaktionen er in seinem Block inkludieren möchte. Bei einer Transaktion kann man eine beliebig hohe Spende an den Miner abgeben. Transaktionen mit einer hohen Spende haben eine größere Wahrscheinlichkeit, im nächsten Block inkludiert zu werden.

Nun kann es jedoch passieren, dass zwei Miner gleichzeitig eine Lösung finden und im Bitcoin-Netzwerk zwei verschiedene Versionen der Blockchain im Umlauf sind. Diese Diskrepanz wird aufgelöst, sobal einer der Ketten einen nächsten Block bekommt. Der Grund dafür ist, dass das Bitcoin-Netzwerk nach einem Konzept namens Proof of workärbeitet. Wenn ein neuer Block hinzugefügt wird, kann man sich sicher sein, dass ein Miner Prozesskraft und Energie dafür aufopfern musste. Die Kette, welche im Endeffekt mehr Blöcke besitzt, wird als gültig anerkannt.

Einer der bekanntesten Wege, um das Bitcoin-Netzwerk anzugreifen, ist der "51% Attack". Wenn man mit bösartigen Absichten in Besitz von mehr als 50% der Mining-Kraft kommt, kann man zwei schwerwiegende Dinge tun. Zum einen kann das Bitcoin-Netzwerk komplett lahmgelegt werden, indem keine neuen Transaktionen in den Blöcken inkludiert werden. Zum anderen können Zahlungen rückgängig gemacht werden, indem man in der einen Kette die Zahlung akzeptiert hat, dann jedoch eine andere Kette ohne diese Zahlung weiterführt und verlängert. Ein Angriff dieser Art wird jedoch immer unwahrsheinlicher, da die Warscheinlichkeit für einen solchen Angriff exponentiell abfällt. (Nakamoto, 2008, 8)

2.2.1 Struktur eines Blocks

Ein Block ist ein Behälter für eine Datenstruktur, welche für die Einschließung von Transaktionen in der Blockchain sorgt. Der Block besteht aus einem Header, welcher für die Identifizierung des Blocks notwendig ist, gefolgt von einer Liste aller Transaktionen. Im Block Header befinden sich Informationen wie die derzeitige Schwierigkeit zur Lösung des Problems der Miner, einen Zeitstempel, welcher die Entstehung des Blocks angibt und einer Zusatzzahl, welche nützlich für Miner ist.

Zur Identifizierung von Blöcken gibt es zwei Wege: Die Berechnung des Block Header Hashes und die Höhe des Blocks. Einen Block durch seine Höhe zu identifizieren scheint simpler, jedoch gibt es hierbei ein Problem. Bei dem vorher angesprochenen Fall, dass zwei Miner gleichzeitig einen Block finden, scheitert die Identifizierung eines Blocks durch dessen Höhe. Um den Block Header Hash zu berechnen, wird der Block Header (Schwierigkeit, Zeitstempel, Zusatzzahl) zwei mal mit dem SHA256 Algorithmus gehashed. Hierbei kommt ein 32-byte Hash heraus, welcher mit vielen Nullstellen beginnt. Jeder Block hat einen distinkten Block Header Hash, wodurch es keine dop-

pelte Blöcke geben kann. Der erste Block (Genesis-Block) der Blockchain hat einen Hashwert von 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f. (Antonopoulos, 2017, S. 199)

2.2.2 Genesis-Block

Der Genesis-Block ist der erste Block der Blockchain mit einer Höhe von 0. Anders als die darauffolgenden Blöcke gilt dieser als unveränderbar. Kreiert wurde dieser 2009 und wenn man jeden einzelnen Block auf der Blockchain zurückverfolgt, gelangt man schlussendlich an den Genesis-Block. Standardmäßig fügt jede Implementierung von Bitcoin den Genesis-Block schon bei der Installation hinzu.

Kapitel 3

Adressen

3.1 Bitcoin-Adressen generieren

In Bitcoin werden Adressen verwendet, um Transaktionen zu empfangen und zu senden. Eine Bitcoin-Adresse ist eine Zeichenfolge, die aus einer Reihe von Zahlen und Buchstaben besteht und einem öffentlichen Schlüssel entspricht.

Um eine Bitcoin-Adresse zu generieren, wird der öffentliche Schlüssel mithilfe einer kryptographischen Hashfunktion verarbeitet. Die Hashfunktion nimmt den öffentlichen Schlüssel als Eingabe und gibt einen Hash als Ausgabe. Der öffentliche Schlüssel selbst wird nicht als Adresse genutzt, weil der Hash weniger Speicherplatz benötigt. Der Hash wird dann mithilfe einer weiteren Mathematikfunktion, der Base58Check-Codierung, in eine lesbare Adresse umgewandelt.

3.2 Base58Check-Codierung

Um große Zahlen mit wenigen Zeichen darzustellen, nutzen Computersysteme häufig alphanumerische Zahlensysteme mit einer Basis, die größer als 10 ist. Das Dezimalsystem nutzt die 10 Ziffern 0-9, während das Hexadezimalsystem zusätzlich die Buchstaben A-F nutzt, wodurch es 16 Ziffern hat. Deshalb sind Zahlen, welche hexadezimal dargestellt werden, kürzer. Base64 ist ein weiteres Zahlensystem, das noch viel kompakter ist. Es nutzt die 26 Buchstaben des Alphabets doppelt, nämlich in Klein- und Großschreibung. Zusätzlich nutzt Base64 die 10 Ziffern 0-9 und die Symbole + sowie /.

Base58 hingegen ist eine Ableitung von Base64, welche ähnlich aussehende Symbole vermeidet, da sie in manchen Schriftarten identisch aussehen können. Diese Symbole sind die Zahl null, der Buchstabe O (großes o), l (kleines L), I (großes i), das Zeichen + und /. Das vollständige Alphabet von Base58 ist:

$$123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz$$

Base58Check wiederum ist ein Codierungsformat von Base58, welches oft in Bitcoin genutzt wird und einen eingebauten Fehlerüberprüfungs-Code besitzt. Die Prüfsumme wird vom Hash der codierten Daten abgeleitet und kann deswegen genutzt werden, um Tippfehler und andere Fehler zu erkennen. Wenn die Prüfsumme also nicht mit den codierten Daten übereinstimmt, gilt die eingegebene Bitcoin-Adresse als ungültig. Dies verhindert den Versand an falsche Bitcoin-Adressen und dadurch den Verlust von Geld. (Vgl. Antonopoulos, 2017, 67)

Die meisten Daten in Bitcoin werden Base58Check-codiert, was es einfacher macht, mit den Daten zu arbeiten. Zudem wird ein Präfix bei jeder Base58Check-Codierung genutzt, welche den Datentyp angibt, um welchen es sich handelt. Das ermöglicht dem Nutzer, schnell zu erkennen, welche Art von Daten dargestellt werden. Beispielsweise haben Bitcoin-Adressen in Base58Check den Präfix 0x00, welcher umgewandelt auf Base58 1 ergibt. Private Schlüssel wiederum haben den Präfix 0x80 in Base58Check bzw. 5 in Base58.

3.3 Private Schlüssel

Im Bitcoin-Netzwerk ist der private Schlüssel eine geheime Zahl, die genutzt wird, um Bitcoin-Ausgaben ausgehend von einer bestimmten Bitcoin-Adresse zu authorisieren. Der private Schlüssel ist eine kritische Komponente der kryptographischen Sicherheit, auf welche das Bitcoin-Netzwertk aufbaut. Genutzt wird der private Schlüssel, um Authentizität bei Transaktionen zu beweisen und versichert dabei, dass die Transaktionen nicht verändert oder gefälscht sind.

Meist sind private Schlüssel in einer sogenannten Wallet, eine Applikation, welche dem Nutzer ermöglicht, Transaktionen zu tätigen, gespeichert. Jede Wallet hat einen einzigartigen privaten Schlüssel, welche für Unterschriften bei Transaktionen genutzt

wird und den Besitz der jeweiligen Bitcoins beweist. Es ist essentiell, dass der private Schlüssel geschützt ist und mit niemanden geteilt wird, da jeder mit Zugriff auf den privaten Schlüssel Bitcoins ausgeben kann.

Private Schlüssel werden als Abfolge von Zahlen und Buchstaben dargestellt. Genauer gesagt werden private Schlüssel durch ein bestimmtes Format wie das Base64 Zahlensystem codiert. Folgende Hexadezimalzahl zeigt, wie ein privater Schlüssel im Normalfall aussieht: 8a708d03d461a5c5839b53da4c40912ca094cc0edee8574a62d6895d033db7ea. Diese Zahl entspricht einem Dezimalwert von ungefähr $6.2 * 10^{70}$. Generiert werden private Schlüssel mit verschiedenen Methoden wie beispielsweise ein Zufallszahlengenerator. Gespeichert werden private Schlüssel im Normalfall auf einem Computer oder Smartphone in einer sicheren Datei.

3.3.1 Private Schlüssel generieren

Prinzipiell sind private Schlüssel eine zufällige Zahl zwischen 1 und 2^{256} bzw. $1,15*10^{77}$. Um diese enorme Zahl zu relativisieren: die geschätzte Anzahl der Atome im sichtbaren Universum beträgt 10^{80}. (Vgl. Antonopoulos, 2017, 59) Die Chance, zwei mal denselben privaten Schlüssel zu generieren ist also extrem gering. Die einfachste Methode, um einen privaten Schlüssel zu generieren, ist der Munzwurf: Kopf und Zahl wird jeweils 0 und 1 zugewiesen. Danach muss die Münze 256 mal geworfen werden und man erhält eine 256-Bit lange Zahl. Prinzipiell kann man mit allem, was zufällig geschieht, einen privaten Schlüssel generieren. Natürlich möchte man nicht für jeden privaten Schlüssel 256 Münzwürfe machen, deswegen werden hierfür Rechner genutzt. Ein großes Problem in der Computerwelt ist es jedoch, zufällige Zahlen erzeugen zu können. Computer sind schlicht und ergreifend nicht dazu geeignet, Zufälle generieren zu können.

3.3.2 Natürliche Zufallsquellen

Aufgrund des Kerchoff'schen Prinzips muss die Definition eines Zufallszahlengenerators, der für Kryptografie geeignet ist, beinhalten, dass selbst wenn jedes Detail über den Generator bekannt ist (Schaltplan, Algorithmen usw.), er immer noch vollständig unvorhersehbare Bits erzeugen muss. Im Gegensatz zu PRNGs(Pseudorandom number generator) extrahieren physische (echte, Hardware) Zufallszahlengeneratoren Zufällig-

keit aus physischen Prozessen, die auf fundamental undeterministischer Weise verhalten, was sie zu besseren Kandidaten für die Erzeugung von wahren Zufallszahlen macht. Physische Prozesse sind (Vgl. Stipčević, 2014, S. 5f):

- Geräusche (Radiowellen, Atmosphärische)
- harmonische Oszillatoren
- Quantenfluktuation

Diese VWA beschäftigt sich mit den geräusch-basierten Zufallsgeneratoren.

Wärmerauschen ist eine Art von Rauschen, das in elektrischen Schaltungen auftritt und durch die thermische Bewegung von Ladungsträgern (normalerweise Elektronen) in elektrischen Leitern verursacht wird. Die thermische Bewegung der Ladungsträger in einem elektrischen Leiter führt zu Schwankungen im Stromfluss, die als Rauschen interpretiert werden können. Dieses Rauschen ist proportional zur Temperatur des Leiters und der elektrischen Leitfähigkeit des Materials. Es ist auch unabhängig von der Art des Leiters und tritt in allen elektrischen Leitern auf, einschließlich Metallen, Halbleitern und sogar Isolatoren.Das Johnson-Nyquist-Rauschen ist ein weißes Rauschen, das bedeutet, dass die Frequenzverteilung des Rauschens gleichmäßig über einen breiten Frequenzbereich verteilt ist. Es hat auch eine bestimmte Spectral Density (Leistung pro Frequenzband) die proportional zur Temperatur und der elektrischen Leitfähigkeit des Leiters ist.

Eine weitere Art des Rauschens ist das chaotische Rauschen das durch chaotische Systeme erzeugt wird. Chaotische Systeme sind Systeme, die sehr empfindlich auf kleine Änderungen in den Anfangsbedingungen reagieren und dazu neigen, unvorhersehbare und zufällige Muster zu erzeugen. Ein Beispiel für ein chaotisches System, das zur Erzeugung von Chaos-Noise verwendet werden kann, ist die Lorenz-Attraktor, die auf drei gekoppelten Differentialgleichungen basiert und eine Art von chaotischem Verhalten erzeugt, das als "Butterfly-Effekt"bekannt ist. (Vgl. Uwe Jönck und Florian Prill, 2003, S. 3ff)

Manche Arten von Rauschen (insbesondere Johnson-Rauschen) erzeugen sehr kleine Spannungen, die vor der Umwandlung in digitale Form stark verstärkt werden müssen. Die starke Verstärkung führt zu weiteren Abweichungen von der Zufälligkeit aufgrund der begrenzten Bandbreite und nicht-linearen Verstärkung des Verstärkers. Außerdem

kann schnelles elektrisches Schalten von binärer Logik, die in der RNG-Schaltung verwendet wird, starke elektromagnetische Störungen verursachen, so dass mehrere RNGs in der Nähe (insbesondere auf einem Chip) tendenziell zur gegenseitigen Synchronisierung neigen, was zu einem starken Rückgang der Gesamtentropie führt. Darüber hinaus können empfindliche Verstärker durch externe elektromagnetische Felder leicht manipuliert werden, was für Kryptoangriffe ausgenutzt werden kann. (Vgl. Stipčević, 2014, S. 7)

Kapitel 4

Transaktionen

Kapitel 5

Kritik an Bitcoin