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 Private Key und Public Key zusammen. Mit dem Public Key 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 Private Key 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) 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)

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. () 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 kaum leistungshungrig und benötigen wenig Energie. 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) und steigt pro Monat um etwa 3GB an.

2.1.2 Mining Node

Damit die Blockchain erweitert wird und alle Transaktionen verfiziert werden könnnen, müssen sogenannte Miner 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.

2.1.3 SPV Client

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.

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. (vgl Nakamoto, 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 doppelte Blöcke geben kann. Der erste Block (Genesis-Block) der Blockchain hat einen Hashwert von 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.

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

Elliptische-Kurven-Kryptographie

3.1 Elliptische Kurve

Elliptische Kurven sind die Menge aller Punkte in den reellen Zahlen, die die Gleichung $4y^2 = x^3+ax+b$ erfüllen, wobei $4a^3+27b^2 \neq 0$, um Singularitäten auszuschließen. Diese Form der elliptischen Kurve nennt man die Weierstraß-Normalform. Außerdem wird ein Punkt im Unendlichen benötigt, welcher Teil der Kurve ist. Für den Zweck dieser Arbeit wird der Punkt im Unendlichen als ∞ bezeichnet. Um den Punkt der Unendlichkeit explizit zu definieren, lautet die vollständige Definition (vgl andrea corbellini):

$$\{(x, y) \in \mathbb{R}^2 | y^2 = x^3 + ax + b, 4a^3 + 27b^2 \neq 0\} \cup \{\infty\}$$

3.1.1 Gruppenoperationen

Kapitel 4

Addressen

4.1 Asymmetrische Kryptographie

Die Kryptographie ist ein Zweig der Mathematik, welcher vor allem in der Cyber-Security Branche verwendet wird. Mit Kryptographie kann man beispielsweise beweise, dass man ein Geheimniss kennt, ohne das Geheimniss zu verraten. Im Falle von Bitcoin wird es genutzt, um den Zugriff auf eine Bitcoin-Addresse zu beweisen. Erreicht wird dies mit dem Public-Key-Verfahren/Asymmetrische Verschlüsselung. Hierbei wird ein Schlüsselpaar generiert, welches aus dem Public Key und dem Private Key besteht. Der Public Key darf von anderen gesehen werden, der Private Key jedoch nicht. Generiert werden diese Schlüssel mit einem Algorithmus namens ECDSA (Elliptic Curve Digital Signature Algorithm).

Transaktionen werden mit einer digitalen Signatur abgeschlossen, für welche der Private Key benötigt wird. Das heißt, dass jeder mit Zugriff auf den Private Key Transaktionen abschließen kann. Den Private Key kann man sich also wie ein Passwort für ein Bankkonto vorstellen. Bitcoin Addressen werden meist aus dem Public Key generiert, indem dieser gehashed wird. Der Public Key kann zwar von anderen gesehen werden, da es keine Sicherheitsrisiken kreiert, wird jedoch trotzdem gehashed. Grund dafür ist, dass Speicherplatz in Bitcoin eine sehr große Rolle spielt. Public Keys haben nämlich mehr Bits als das Ergebnis einer Hashfunktion.

Kapitel 5

Transaktionen

Kapitel 6

Kritik an Bitcoin