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. Nutzer können über das sogenannte Bitcoin-Netzwerk Zahlungen propagieren und verifizieren. Mit der Kryptowährung Bitcoin kann man Käufe tätigen, Geld an Verwandte oder Organisationen versenden und Waren verkaufen. 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 erlangt. Dieser Wert kann bis zu acht Dezimalstellen besitzen, da die kleinste Einheit von Bitcoin ein Satoshi ist. 100 Millionen Satoshis entsprechen einem bitcoin.

Transaktionen werden mithilfe von assymetrischer Verschlüsselung abgeschlossen. Diese setzt sich aus dem Private Key und Public Key zusammen. Mit dem Public Key wird die Bitcoin-Addresse des Nutzers hergestellt, 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.

1.2 Geschichte von Bitcoin

2008 veröffentlichte jemand unter dem Alias Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System". 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.

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 für den Otto Normalverbraucher ist der SPV Client. Dieser installiert lediglich eine Wallet und stellt eine Verbindung zum Bitcoin-Netzwerk her. Er ist einzig und allein dafür ausgestattet, Transaktionen auf das eigene Konto zu empfangen und Gled zu versenden.

2.2 Die Blockchain

2.2.1 Struktur eines Blocks

2.2.2 Genesis-Block

Kapitel 3

Adressen

Kapitel 4

Transaktionen

Kapitel 5

Kritik an Bitcoin