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

Aufbau des Bitcoin-Netzwerkes

2.1 Peer-to-Peer-Netzwerk

2.1.1 Full Node

2.1.2 Mining Node

2.1.3 SPV Client

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