Blockchain- Technologie : Analyse von Proof of Work (Bitcoin)

Ziad Bougrine

15. November 2022

Hier steht eine kurze Zusammenfassung des Inhaltes, es geht hier um den Aufbau eines Artikels, insbesondere um die geeignete Gliederung.

Inhaltsverzeichnis

1 Einleitung

Seit den späten 2000er Jahren hat sich Blockchain zu einer der disruptivsten Technologien auf dem globalen Markt für digitale Transaktionen entwickelt.

In der Jahre 2008 wurde ein Whitepaper mit dem Titel Bitcoin: „A Peer-to-Peer Electronic Cash System“ von einer Person (oder einer Gruppe von Personen) unter dem Namen Satoshi Nakamoto veröffentlicht. Vier Monate später, am 3. Januar 2009, erstellten sie den Genesis-Block, was der Beginn und der Tag 0 des Bitcoin- und Blockchain-Netzwerks ist. Blockchain betrachtet als öffentlich verteiltes Hauptbuch für Bitcoin-Kryptowährung Transaktionen zu dienen, basierend auf die Methode „Proof-Of-Work“, um die Schaffung und den Handel von Bitcoin und anderen Kryptowährungen während der Finanzkrise 2007/08 zu unterstützen. In heutigen Tagen gibt es jetzt viele Kryptowährungen. Zum Beispiel : Litecoin(2011), Ethereum(2015), Dogecoin(2013) usw...

Die Implementierung der Blockchain in Bitcoin machte es zur ersten digitalen Währung, die das Problem der doppelten Ausgaben ohne die Notwendigkeit einer vertrauenswürdigen Behörde löst. Einer der Hauptvorteile besteht darin, dass jeder erstellten Block, der Datensatz enthält unveränderlich ist und seine Authentizität von der gesamten Gemeinschaft autorisierter Benutzer und nicht von einer einzigen zentralen Behörde überprüft werden kann. Das System ist daher darauf ausgelegt, die Transparenz und Rechenschaftspflicht einer digitalisierten Transaktion zu verbessern. Nehmen wir ein Beispiel, um dieses Konzept gut zu verstehen. Wir haben ein Transaktionsbanksystem, von dem aus einem Server oder Systemadministrator alles verwalten kann. Dies kann die Wartung des Systems, das Verwalten, Löschen und Hinzufügen von Benutzer- oder Transaktionsinformationen zur Datenbank umfassen. Oder er sagt einfach, dass Sie ihm 10.000 € schulden, was gefährlich ist.

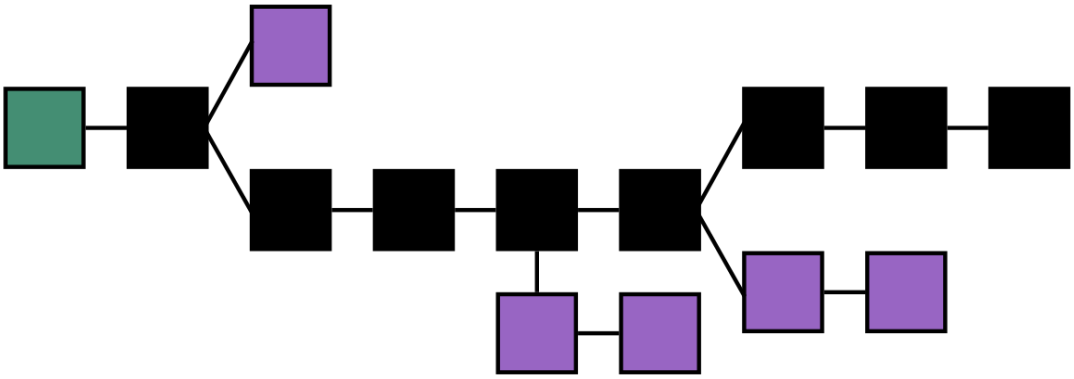
Das ist der Hauptgrund, warum Blockchain-Technologie erfunden worden. Indem es immer für alle sichtbar im Hauptbuch aufgezeichnet wird, wenn Geld von einem Konto auf ein anderes überwiesen wird.

2 Einführung in die Blockchain

2.1 Blockchain Definition

Blockchain ist eine kontinuierlich erweiterbare Liste von Datensätzen in einzelnen Blöcken, es ist ein offenes Hauptbuch für Personen, die Datensätze sehen und erstellen können. Jeder Block besteht aus Daten, Hash, vorherigem Hash und Zeitstempel. Entscheidend ist, dass wir spätere Transaktionen auf früheren Transaktionen aufbauen können und diese als richtig bestätigen können, indem wir die Kenntnis der früheren Transaktionen beweisen können. Damit wird es unmöglich gemacht, Existenz oder Inhalt der früheren und späteren Transaktionen zu manipulieren. Andere Teilnehmer der dezentralen Buchführung erkennen eine Manipulation der Blockchain dann an der Inkonsistenz der Blöcke.

Blockchain ist ein Distributed Ledger, diese Technologie nennt sich Self regieren (Self governing), was bedeutet, dass es nicht eine Person gibt, die kontrollieren und machen kann ändern, stattdessen kommen Beiträge von Tausenden von Benutzern die am Blockchain-Netzwerk teilnehmen, um es funktionsfähig zu machen. Wenn eine Person betrügt, wird sie schnell sein als Betrug angesehen, da der Rest des Netzwerks sie überprüft.



2.2 Konstruktion des Blocks

Ein Block speichert Informationen über Transaktionen, Zeitstempel, vorherigen Hash, Block-Hash.

- **Magische Zahl :** Nummer, die diesen Block als Teil des Netzwerks einer bestimmten Kryptowährung identifiziert.
- **Transaktionen :** die Hauptinformationen und auch den größten Teil des Blocks
- **Transaktionszähler :** die Anzahl der im Block gespeicherten Transaktionen
- **Block Größe :** die maximale Größe der Informationen, die der Block enthält

Ein Block enthält viele Informationen, belegt jedoch nicht viel Speicherplatz. Nehmen wir diese Elemente als Beispiel: Was ist die Hauptinformationen, die ein Block (Transaktionen) enthält?

- **Version:** Sie ist benutzbar, um einen neuen Block zu erstellen und um eine neue Version von Software zu identifizieren. Es ist auf 4 Bytes (4 x 8 „bits“) codiert.
- **Vorheriger Block-Hash:** Enthält einen Hash des Headers des vorherigen Blocks (md5, sha256 ...). Es ist auf 32 Bytes (32 x 8 = 256 „bits“) codiert.
- **Hash Merkle root:** Hash of transactions in the Merkle tree of the current block. Es ist auf 32 Bytes (32 x 8 = 256 „bits“) codiert.
- **Time:** Erstellungszeit des Blocks. Es ist auf 32 Bytes (32 x 8 „bits“) codiert.
- **Bits:** Es ist ein Wert, der die Schwierigkeitsbewertung des Ziel-Hashes und die Schwierigkeit beim Lösen der „Nonce“ angibt. Es ist auf 32 Bytes (32 x 8 „bits“) codiert.
- **Nonce:** Es ist die magische Zahl, die der Miner lösen muss, um einen Block im Blockchain-Netzwerk zu verifizieren und zu schließen.

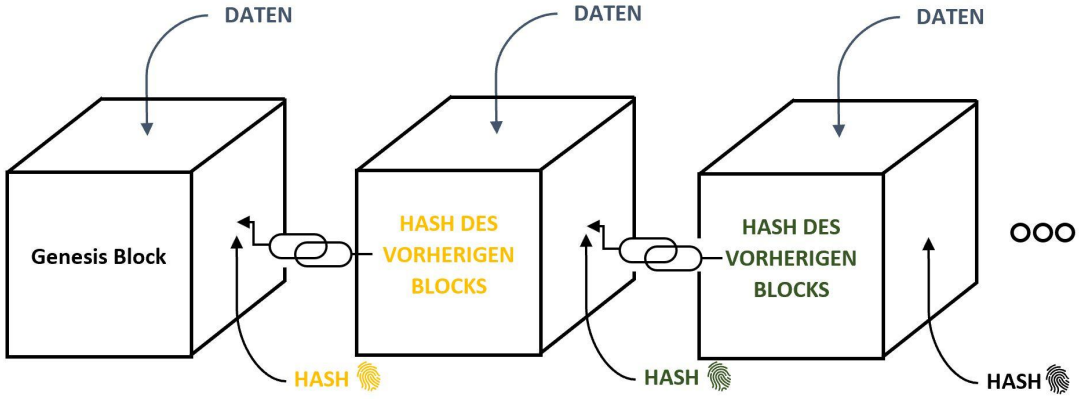
Information : Die Miner interessieren sich für die Nonce, weil das Mining-Programm Zufallszahlen (Bruteforce) verwendet, um die Nonce im Hash zu erraten. Der Hash wird verifiziert, wenn die Nonce gelöst ist. Wenn die Nonce oder eine Zahl darunter erraten wird. Dann schließt das Netzwerk diesen Block, generiert einen neuen mit einem Header und der Prozess wiederholt sich.

Was sind Merkle-Bäume?

Es handelt sich um eine Datenstruktur in Form eines Binärbaums, der in Bitcoin und Kryptowährung weit verbreitet ist und zur effizienteren und sichereren Codierung von Daten verwendet wird.

2.3 Blockchaining-Mechanismus

Der Blockchain-Mechanismus funktioniert wie eine Linkedlist, er enthält eine Kette von Blöcken dass jeder Block der Kette aus einem Hash dieses Blocks und einem Hash des vorherigen Blocks zusammengesetzt ist. Es ist derselbe Mechanismus wie bei der Linkedlist, da jeder Knoten der Liste einen Zeiger auf den letzten Knoten enthält. Was es ermöglicht, über die Kette zu iterieren.



Der erste Block der Kette wird als Genius-Block bezeichnet.

In diesen Situationen sollten wir immer darüber nachdenken, was verdächtige Personen tun könnten, sie könnten die Daten im Block (i) ändern oder manipulieren. dies führt zu einer Modifikation des tatsächlichen Blocks i und macht den vorherigen Hash im Block (i+1) ungültig. Das bedeutet, dass das Ändern eines Blocks alle nächsten folgenden Blöcke im Blockchain-Netzwerk ungültig macht, was die Qualität der Herstellung einer Kette beweist.

Achtung : ist dieser Mechanismus gesichert ?

Die Verwendung von Hashes reicht nicht aus, um Manipulationen zu verhindern. Computer sind heutzutage sehr schnell und können Tausende von Hashes berechnen. Technisch gesehen können wir einen Block manipulieren und alle nächsten Hashes der nächsten Blöcke neu berechnen, um das Blockchain-Netzwerk wieder gültig zu machen.

Aus diesem Grund verwendet Blockchain Proof of Work in diesen Fällen. Es gibt eine Möglichkeit, dieses Problem zu verhindern. Es ist der berühmte „Proof of Work (POW)“.