

UNIVERSITY OF APPLIED SCIENCES

SEMINARARBEIT

FACHBEREICH09

ANGEWANDTE MATHEMATIK UND INFORMATIK

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

Author:

Ziad BOUGRINE (3560356)

Lecturer:

prof. dr. Volker SANDER

prof. dr. Walk LUKAS

14. Februar 2023

Diese Arbeit ist von mir selbständig angefertigt und verfasst. Es sind keine anderen als die angegebenen Quellen und Hilfsmittel benutzt worden.

Ziad Bougrine

Diese Arbeit wurde betreut von:

1. Prüfer : **Volker, Sander**
2. Prüfer : **Walk, Lukas**

Zusammenfassung auf Deutsch

In diesem Bericht wurde eine umfassende Analyse der Technologie der Blockchain-Netzwerke und der Kryptowährungen auf der Basis von Proof-Of-Work durchgeführt. Die Funktionsweise von Kryptowährungen wurde detailliert untersucht und die Investitionsmöglichkeiten in diese Währungen wurden erläutert. Zudem wurden die Vor- und Nachteile von Proof-Of-Work und anderen Konsensmechanismen aufgezeigt und die Zukunftsaussichten für diese Technologien wurden diskutiert. Der Bericht bietet somit eine wertvolle Ressource für diejenigen, die sich für die Blockchain-Technologie und das Investieren in Kryptowährungen interessieren.

Abstract in English

This report presents a comprehensive analysis of the technology of blockchain networks and cryptocurrency based on Proof-Of-Work. The functioning of cryptocurrency was thoroughly studied, and the investment opportunities in these currencies were explained. The pros and cons of Proof-Of-Work and other consensus mechanisms were also highlighted, and the future prospects for these technologies were discussed. This report therefore provides a valuable resource for those interested in blockchain technology and investing in cryptocurrency.

Inhaltsverzeichnis

| | | |
|----------|---|-----------|
| 1 | Einleitung | 8 |
| 2 | Einführung in die Blockchain | 9 |
| 2.1 | Blockchain Definition | 9 |
| 2.2 | Konstruktion des Blocks | 10 |
| 2.3 | Blockchaining-Mechanismus | 11 |
| 2.4 | wie wird bei eine Blockchain die Unveränderlichkeit und Zensurresistenz der Daten gewährleistet ? | 12 |
| 2.4.1 | Was ist ein Konsensmechanismus ? | 12 |
| 2.4.2 | Warum benutzt die Blockchain die Kryptographie, um die Daten zu sichern ? | 12 |
| 2.4.3 | Was bedeutet die Dezentralisierung ? | 12 |
| 2.4.4 | Warum benutzt die Blockchain Mehrere Kopien, um die Daten zu sichern ? | 12 |
| 2.5 | Was ist Mining-Pool | 13 |
| 3 | Theoretische Seite der Proof-Of-Work-Methode | 14 |
| 3.1 | Einführung in die Proof-of-Work-Methode? | 14 |
| 3.1.1 | Was bedeutet Proof-Of-Work ? | 14 |
| 3.1.2 | Warum ist es empfehlenswert, die Proof-of-Work zu benutzen? . . | 14 |
| 3.1.3 | Ist die Dezentralisierung von Proof-Of-Work gesichert ? | 15 |
| 3.1.4 | Wie wird die Dezentralisierung von Proof-of-Work verbessert ? . . | 15 |
| 3.2 | Wie genau funktionieren die Proof-of-Work-Berechnungen? | 15 |
| 3.3 | Praktische Anwendung der Proof-Of-Work-Methode | 18 |
| 3.4 | Vor- und Nachteile von Proof-Of-Work | 22 |
| 4 | Schwierigkeit und Sicherheit des Proof-Of-Work | 25 |
| 4.1 | Was hat es mit der Schwierigkeit auf sich ? | 25 |
| 4.2 | Wie wird die Schwierigkeit genau angepasst bei Proof of Work ? | 25 |
| 4.3 | was passiert wenn die PoW-Schwierigkeit zu niedrig eingestellt sein? . . . | 26 |
| 4.4 | wie beeinflusst die Schwierigkeit des PoW und die Größe des netzwerkes die Sicherheit und Intigrität der Blockchain? | 26 |
| 5 | Sidechains | 27 |
| 5.1 | Was ist eine Sidechain? | 27 |
| 5.1.1 | Definition von Sidechain | 27 |
| 5.1.2 | Sidechain, auf die Proof-Of-Work basieren | 28 |
| 5.1.3 | Eigenschaften | 28 |

| | | |
|----------|---|-----------|
| 5.2 | Two-way peg | 29 |
| 5.3 | Intelligente Verträge | 30 |
| 5.4 | Sidechain bei Bitcoin | 31 |
| 5.5 | Woher weiß ein Client, dass er in der Mainchain ist und nicht in einer Sidechain ? | 32 |
| 5.6 | Was gibt es für Angriffszenarien und wie funktionieren diese ? | 33 |
| 5.7 | Sybil-Angriff | 33 |
| 5.7.1 | Was ist ein Sybil-Angriff ? | 33 |
| 5.7.2 | Die Funktionsweise dieses Angriffs | 33 |
| 5.7.3 | Wie kann man sich vor diesem Angriff schützen? | 34 |
| 5.8 | Doublespending | 35 |
| 5.8.1 | Was ist Doublespending ? | 35 |
| 5.8.2 | Die Funktionsweise dieses Angriffs | 35 |
| 5.8.3 | Ist die Blockchain, die auf PoW basiert, gegen diesen Angriff ge- sichert ? | 35 |
| 5.9 | 51% Angriff | 36 |
| 5.9.1 | Was ist ein 51%-Angriff ? | 36 |
| 5.9.2 | Die Funktionsweise dieses Angriffs | 36 |
| 5.9.3 | Welche Folgen kann eine 51%-Angriff haben? | 36 |
| 5.9.4 | Wie macht sich eine 51%-Angriff bemerkbar? | 36 |
| 5.9.5 | Die Grenzen des 51%-Angriffs | 37 |
| 5.9.6 | Wie kann man sich vor einem 51%-Angriff schützen? | 37 |
| 5.10 | Routing Angriff | 38 |
| 6 | Schluss | 39 |

Abbildungsverzeichnis

| | | |
|-----|--|----|
| 2.1 | Ein Beispiel für eine Blockchain-Kette | 9 |
| 2.2 | Der erste Block der Kette wird als Genius-Block bezeichnet. | 11 |
| 3.1 | Die echten Blockchain-Block-Transaktionen. | 19 |
| 3.2 | Das nächste Diagramm, das als Klassendiagramm bezeichnet wird, gibt eine visuelle Darstellung aller Daten, die im realen Blockchain-Netzwerk enthalten sind. Dieses Diagramm ist hilfreich, um die Implementierung des Blockchain-Netzwerks besser zu verstehen und zu analysieren. Es zeigt die Beziehungen und Abhängigkeiten zwischen den verschiedenen Elementen des Netzwerks und hilft, die Struktur und Funktionsweise des Systems zu verdeutlichen. Die Verwendung eines Klassendiagramms ermöglicht es, die komplexen Zusammenhänge einfacher darzustellen und die Implementierung des Blockchain-Netzwerks besser zu verstehen. | 20 |
| 3.3 | Der Algorithmus zur Bestimmung der Nonce wird mit dem Aktivitätsdiagramm erklärt. Zunächst müssen wir die initialen Daten initialisieren, einschließlich des MaxNonceLimit, der Anzahl der Nullen, die der Hash haben sollte. In diesem Beispiel betrachten wir die Anforderung, dass der Hash mit 4 Nullen beginnen sollte. Es ist wichtig zu beachten, dass die Anzahl der Nullen eine wichtige Rolle bei der Bestimmung der Komplexität des Algorithmus spielt. Je höher die Anzahl der Nullen, desto länger wird es dauern, die Nonce mit begrenzter Hardware zu finden. Wir sollten auch unsere Inkrementierungsvariable für die for-Schleife initialisieren. . . | 21 |
| 3.4 | Die heutige Schwierigkeit ist | 24 |
| 5.1 | Mechanismus der Sidechain | 29 |
| 5.2 | Two way peg | 30 |
| 5.3 | Intelligente Verträge | 31 |

1 Einleitung

Blockchain ist seit den späten 2000er Jahren eine der wichtigsten Technologien im Bereich digitaler Transaktionen. Im Jahr 2008 veröffentlichte eine Person oder Gruppe von Personen unter dem Namen Satoshi Nakamoto ein Whitepaper mit dem Titel "Bitcoin: A Peer-to-Peer Electronic Cash System". Vier Monate später, am 3. Januar 2009, wurde der Genesis-Block erstellt, der den Beginn und Tag 0 des Bitcoin- und Blockchain-Netzwerks markierte. Die Blockchain wurde entwickelt, um als öffentliches Hauptbuch für Bitcoin-Transaktionen zu dienen und basiert auf der "Proof-of-Work-Methode, um die Schaffung und den Handel von Bitcoin und anderen Kryptowährungen während der Finanzkrise 2007/08 zu unterstützen. Heutzutage gibt es viele Kryptowährungen wie Litecoin (2011), Ethereum (2015) und Dogecoin (2013).

Die Implementierung der Blockchain in Bitcoin machte es zur ersten digitalen Währung, die das Problem der doppelten Ausgaben ohne die Notwendigkeit einer vertrauenswürdigen zentralen Behörde löst. Einer der Hauptvorteile von Blockchain ist, dass jeder erstellte Block, der einen 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 von digitalisierten Transaktionen zu verbessern.

Ein Beispiel: Stellen Sie sich ein Transaktionsbanksystem vor, das von einem Server oder Systemadministrator verwaltet wird. Dies könnte die Wartung des Systems, das Verwalten, Löschen und Hinzufügen von Benutzer- oder Transaktionsinformationen zur Datenbank umfassen. Es könnte auch bedeuten, dass der Administrator behauptet, dass Sie ihm 10.000 € schulden, was gefährlich ist. Das ist der Grund, warum die Blockchain-Technologie erfunden wurde. Indem es immer für alle sichtbar im Hauptbuch aufgezeichnet wird, wenn Geld von einem Konto auf ein anderes überwiesen wird, kann jeder Benutzer die Transaktion überprüfen und sicherstellen, dass sie korrekt ist. "Blockchain - Wikipedia", 2022 "Blockchain", 2022

2 Einführung in die Blockchain

2.1 Blockchain Definition

Die **Blockchain** ist eine ständig wachsende Liste von Datensätzen, die in einzelnen Blöcken organisiert sind. Sie dient als öffentliches Hauptbuch, in dem Personen Datensätze einsehen und erstellen können. Jeder Block besteht aus Daten, einem Hash, dem Hash des vorherigen Blocks und einem Zeitstempel. Das Wesentliche an der Blockchain ist, dass wir spätere Transaktionen auf früheren Transaktionen aufbauen und deren Richtigkeit bestätigen können, indem wir die Kenntnis der früheren Transaktionen nachweisen. Auf diese Weise wird es unmöglich gemacht, die Existenz oder den Inhalt früherer und späterer Transaktionen zu manipulieren. Andere Teilnehmer der dezentralen Buchhaltung erkennen eine Manipulation der Blockchain an der Inkonsistenz der Blöcke. Insider, 2022

Die **Blockchain** ist ein verteiltes Hauptbuch, das sich selbst reguliert, das heißt, dass es keine Person gibt, die Kontrolle oder Veränderungen vornehmen kann. Stattdessen tragen Tausende von Benutzern, die am Blockchain-Netzwerk teilnehmen, dazu bei, es funktionsfähig zu halten. Wenn eine Person versucht, das System zu betrügen, wird sie schnell als Betrugserkennung markiert, da das gesamte Netzwerk sie überprüft. Chapter247Infotech, n. d.

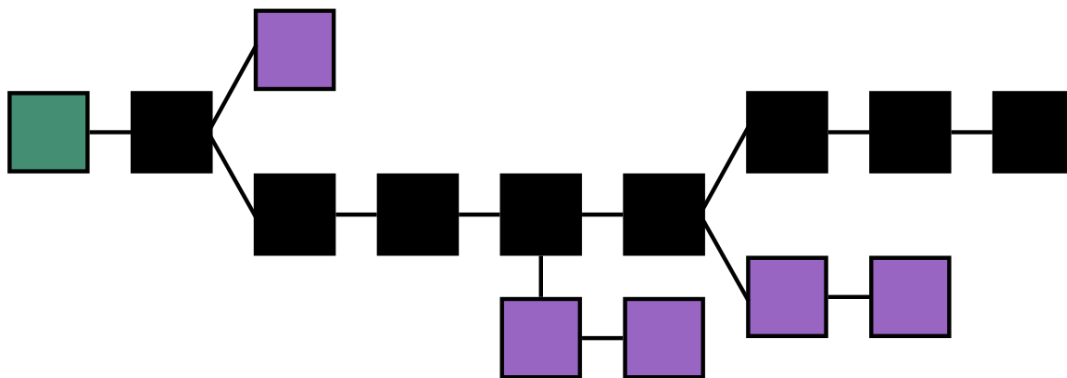


Abbildung 2.1: Ein Beispiel für eine Blockchain-Kette

URL : <https://de.wikipedia.org/wiki/Blockchain>

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 (4×8 „bits“) codiert.
- **Vorheriger Block-Hash**: Enthält einen Hash des Headers des vorherigen Blocks (md5, sha256 ...). Es ist auf 32 Bytes ($32 \times 8 = 256$ „bits“) codiert.
- **Hash Merkle root**: Hash of transactions in the Merkle tree of the current block. Es ist auf 32 Bytes ($32 \times 8 = 256$ „bits“) codiert.
- **Time**: Erstellungszeit des Blocks. Es ist auf 32 Bytes (32×8 „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 (32×8 „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 setzen ihre Rechenleistung ein, um mithilfe von Zufallszahlen (Bruteforce) die Nonce im Hash zu erraten. Sobald die Nonce erfolgreich bestimmt wurde, wird der Hash verifiziert und der Block geschlossen. Anschließend wird ein neuer Block mit einem Header erstellt und der Prozess wiederholt sich. Die Nonce ist von Interesse für Miner, da sie einen wichtigen Bestandteil des Mining-Prozesses darstellt, bei dem versucht wird, den Hash zu lösen.

Was sind Merkle-Bäume?

Es handelt sich um eine Datenstruktur in Form eines Binärbaums, die in Bitcoin und Kryptowährung weit verbreitet ist und zur effizienten und sicheren Kodierung von Daten verwendet wird.

2.3 Blockchaining-Mechanismus

Eine Blockchain funktioniert ähnlich wie eine verkettete Liste, da sie aus einer Reihe von Blöcken besteht, die jeweils durch einen Hash des aktuellen Blocks und einen Hash des vorherigen Blocks miteinander verbunden sind. Dieser Mechanismus ermöglicht es, über die Kette zu iterieren, ähnlich wie bei einer verketteten Liste, bei der jeder Knoten einen Zeiger auf den vorherigen Knoten enthält. [Fool, 2022]

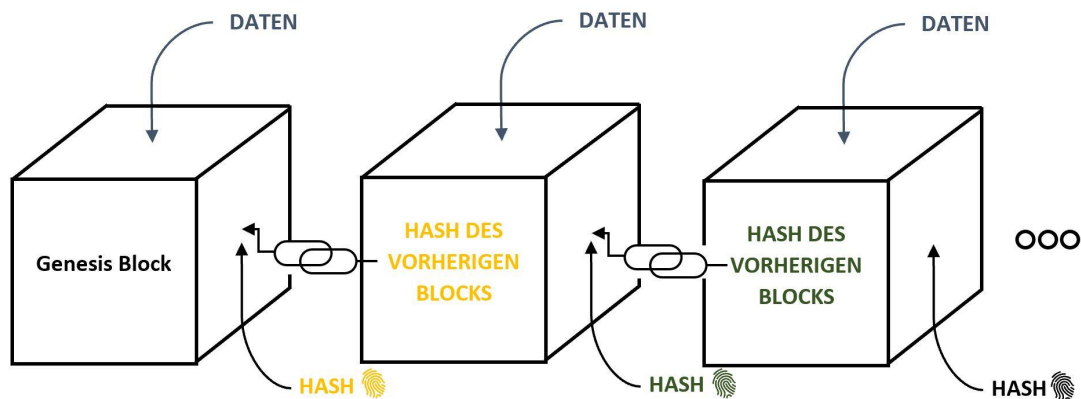


Abbildung 2.2: Der erste Block der Kette wird als Genius-Block bezeichnet.

URL : <https://muenchen.digital/wp-content/uploads/Blockchain-1.jpg>

In solchen Fällen sollte man immer im Hinterkopf behalten, dass Hacker versuchen werden, viele Angriffe auf das Blockchain-Netzwerk zu entwerfen, z. B. die Änderung oder Manipulation der Daten in Block (i). Dies führt zu einer Änderung des tatsächlichen Blocks i und macht das Feld "vorheriger Hash in Block (i+1) ungültig. Das bedeutet, dass die Änderung eines Blocks alle nachfolgenden Blöcke in der Blockkette ungültig macht, was die Integrität der Kette beweist.

Achtung : Ist dieser Mechanismus gesichert?

Die Verwendung von Hash reicht jedoch nicht aus, um verdächtige Manipulationen zu verhindern. Da Computer heute sehr schnell sind und Tausende von Hash-Operationen berechnen können, besteht technisch die Möglichkeit, einen Block zu manipulieren und alle Hashes der folgenden Blöcke neu zu berechnen, um das Netzwerk der Blockkette mit falschen Informationen wieder gültig zu machen. Aus diesem Grund verwendet die Bitcoin-Blockchain einen Konsensmechanismus, der als Proof-Of-Work (PoW) bezeichnet wird, um das Problem der Neuberechnung von Blöcken zu lösen.

2.4 wie wird bei eine Blockchain die Unveränderlichkeit und Zensurresistenz der Daten gewährleistet ?

Die Unveränderlichkeit und Zensurresistenz der Daten in einer Blockchain wird durch verschiedene Technologien und Mechanismen gewährleistet, darunter :

- Konsensmechanismus
- Kryptografie
- Dezentralisierung
- Mehrere Kopien

2.4.1 Was ist ein Konsensmechanismus ?

Konsensmechanismus: ist ein Mechanismus, der es allen Teilnehmern einer Blockchain ermöglicht, Mining-Operationen durchzuführen, was bedeutet, komplexe mathematische Operationen zu lösen, um einen Block zu validieren und ihn der Hauptkette hinzuzufügen. In unserem Bericht haben wir ausschließlich über PoW berichtet. Es gibt verschiedene Beispiele dafür, z. B. "Proof-of-Work", "Proof-of-Stake" oder "Proof-of-Space".

2.4.2 Warum benutzt die Blockchain die Kryptographie, um die Daten zu sichern ?

Kryptografie: Die Blockchain-Technologie nutzt Kryptografie, um Daten zu verschlüsseln und mit Hash-Funktionen wie SHA256, die von PoW verwendet werden, zu signieren. Dadurch wird die Sicherheit der Daten in der Blockchain gewährleistet, da jede Änderung an einer Transaktion oder einem Block sofort erkannt wird.

2.4.3 Was bedeutet die Dezentralisierung ?

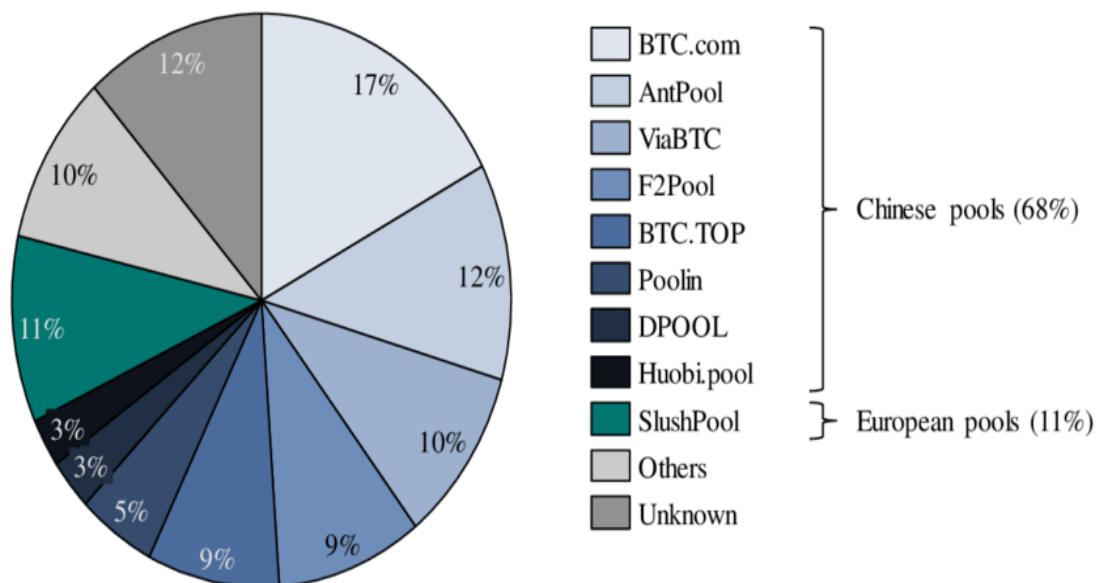
Dezentralisierung: Eine Blockchain ist ein dezentralisiertes Netzwerk, das viele verschiedene Teilnehmer enthält. Das bedeutet, dass keine zentrale Behörde die Kontrolle über das Netzwerk hat, was es einer einzelnen böswilligen Person erschwert, die Daten zu verändern.

2.4.4 Warum benutzt die Blockchain Mehrere Kopien, um die Daten zu sichern ?

Mehrere Kopien: Die Blockchain speichert mehrere Kopien ihrer Daten bei vielen verschiedenen Teilnehmern, was bedeutet, dass es schwieriger ist, alle Kopien einer Blockkette zu zensieren.

2.5 Was ist Mining-Pool

Ein Mining-Pool ist eine Gruppe von Minern, die ihre Hardware kombinieren, um ihre Chancen auf Belohnungen durch den Prozess des Minings von Kryptowährungen zu erhöhen, die auf dem Proof-of-Work (PoW)-Konsensmechanismus basieren. Die kryptografischen Rätsel, die gelöst werden müssen, um Belohnungen zu erhalten, sind für einzelne Miner oft zu komplex zu lösen, und das Poolen von Ressourcen ermöglicht eine dynamischere Nutzung der Rechenleistung. Der Mining-Pool ist dafür verantwortlich, die Verteilung der Belohnungen unter seinen Teilnehmern zu verwalten, was in der Regel automatisch geschieht, je nachdem, wie viel jeder Miner zur Lösung beigetragen hat, um den Hash zu finden. Einige bekannte Mining-Pools im Jahr 2023 sind Antpool, BTCC Mining Pool und Slush Pool.



<https://www.researchgate.net/profile/Christian-Stoll-3/publication/331407183/figure/fig2/AS:772160457031680@1561108807083/Hash-rate-distribution-among-mining-pools-as-of-November-2018-Data-pulled-from-png>

3 Einführung in die „Proof-Of-Work“-Methode

3.1 Einführung in die Proof-of-Work-Methode?

3.1.1 Was bedeutet Proof-Of-Work ?

Proof-Of-Work ist eine dezentrale Konsensmethode (Es ist in Abschnitt 2.4.1 behandelt), bei der die Netzwerkteilnehmer Rechenleistung geben müssen, um ein Hash zu finden. Dieser Prozess dient als Abschreckung gegen Manipulation oder Ausbeutung des Systems, weil die Teilnehmer (Nodes) Arbeit leisten müssen. Was es ein sicheres Mittel zur Überprüfung der Integrität von Transaktionen und zur Aufrechterhaltung des Konsenses zwischen allen Mitgliedern des Netzwerks bietet.

3.1.2 Warum ist es empfehlenswert, die Proof-of-Work zu benutzen?

Proof-Of-Work (POW) wurde entwickelt, um zu verhindern, dass Nutzer Blocks in der Blockchain leicht manipulieren. Es verlangt von Minern, eine signifikante Menge an Mühe aufzuwenden, um einen Block zu erstellen. Diese Methode basiert auf verschiedenen Grundprinzipien in der Kryptowährung [“Proof of work”, 2022], wie folgt:

- **Der Proof-Of-Work-Mechanismus sorgt dafür**, dass das Hinzufügen von Blöcken zur Blockchain-Kette mit einer gewissen Schwierigkeit verbunden ist, indem es Miner dazu zwingt, einen gültigen Hash zu finden. Diese Methode wurde so konzipiert, dass etwa alle zehn Minuten ein neuer Block mit einer festgelegten Menge an BTC in die Kette aufgenommen wird. Dies gewährleistet das algorithmische Wachstum der Geldmenge. [Academy, 2021]
- **Die Verwendung von Proof-Of-Work** ermöglicht es den Nodes, die Integrität der Blockchain zu überprüfen, indem sie diejenige wählen, die den größten Aufwand in Form von Rechenleistung darstellt. Auf diese Weise ist es einfach zu erkennen, welche Blockchain die authentische ist.
- **Die Verwendung von Proof-Of-Work** dient dazu, das Blockchain-Netzwerk vor Angreifern zu schützen, da diese eine größere Energiemenge in das Netzwerk einspeisen müssten als alle anderen verfügbaren Miner insgesamt über einen längeren Zeitraum. Dies ist beim Bitcoin aufgrund der enormen Rechenleistung, die benötigt wird, um einen gültigen Block zu erstellen, praktisch unmöglich.

- **Proof-Of-Work ist eine bewährte Methode** zur Sicherung von Blockchains und zur Neuverteilung von digitalen Währungen. Im Gegensatz zu Fiatgeld, das von Zentralbanken gedruckt werden kann, erfordert die Erschaffung von Währungen in einem Proof-Of-Work-System einen tatsächlichen Einsatz von Ressourcen. Dadurch wird ein fairer Mechanismus für die Verteilung von Währungen gewährleistet. [Academy, 2021]

3.1.3 Ist die Dezentralisierung von Proof-Of-Work gesichert ?

Die Dezentralität (Es ist in Abschnitt 2.4.3 behandelt) in dieser Methode ist abhängig von verschiedenen Faktoren, der Verteilung der Mining-Ressourcen und der Zentralisierung der Mining-Pools. Wenn eine hohe Konzentration unter den Mining-Pools besteht, kann das zu einer kleineren Dezentralisierung führen, denn ein einzelner Mining-Pool könnte in der Lage sein, die Mehrheit der Rechenleistung des Netzwerks zu kontrollieren.

3.1.4 Wie wird die Dezentralisierung von Proof-of-Work verbessert ?

Es gibt oft Maßnahmen wie die Förderung einer gleichmäßigen Verteilung der Mining-Ressourcen und die Einführung von Mechanismen, die eine Zentralisierung der Mining-Pools einschränken, ergriffen. Dies trägt zu einer fairen Verteilung der Rechenleistung bei und unterstützt außerdem den Aufbau eines robuster und sichereren Netzwerks.

3.2 Wie genau funktionieren die Proof-of-Work-Berechnungen?

Hash-Funktion Zuerst muss man wissen, wie die Hash-Funktion funktioniert, indem sie eine eindeutige, nicht invertierbare mathematische Funktion, die aus einer beliebigen Eingabestring eine feste Länge erzeugt. Sie könnte eine beliebig lange Zeichenfolge in eine eindeutige Zeichenfolge festgelegter Länge umwandeln. Beispiel hierfür ist der Einsatz der SHA-256-Hash-Funktion im Bereich des Minings. [Academy, 2021]

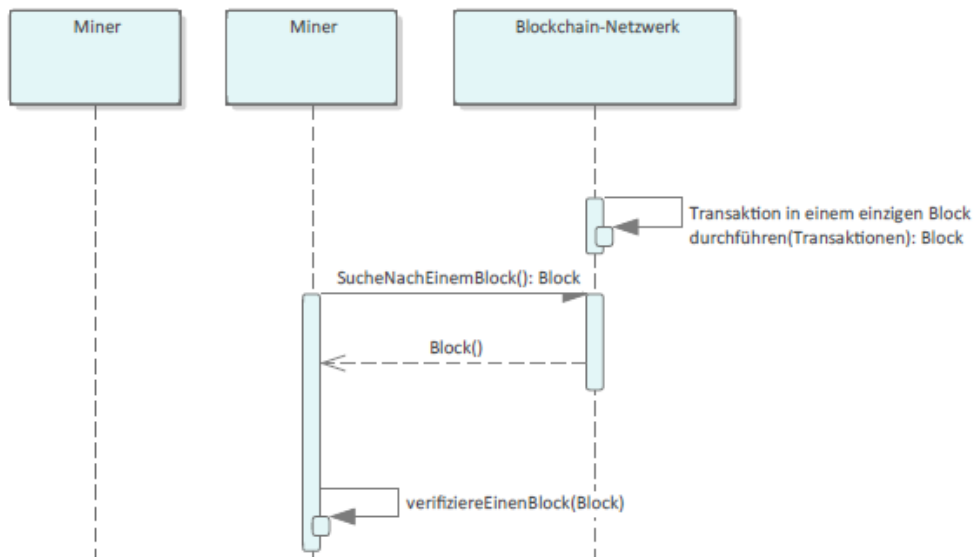
Mining ist ein Prozess, bei dem Miner versuchen, die Nonce und die Reihenfolge von jeden Parameter zu erraten, die von einer Hash-Funktion als Eingabe akzeptiert werden, um ein Ergebnis zu liefern. Da es unmöglich ist, die Hash-Funktion umzukehren, um die ursprüngliche Eingabe zu erhalten, müssen Miner eine Vielzahl (Milliarden von Berechnungen) von Operationen durchführen, um den Wert der Eingabe für die Hash-Funktion zu ermitteln. Sobald ein solches Ergebnis erzielt wurde, wird den Minern eine Belohnung gewährt. [Academy, 2021]

Diese beschreiben den Prozess einer Transaktion im Blockchain-Netzwerk.

1. Die Blockchain generiert einen Block, der alle Transaktionen enthält, die in einem bestimmten Zeitraum stattgefunden haben.

2. Der Verifizierer wird die Integrität der Transaktionen überprüfen, um sicherzustellen, dass sie legitim sind. [Academy, 2021]
3. Die Miner im Netzwerk überprüfen dann die Legitimität dieser Transaktionen und führen anschließend eine Suche durch, indem sie die Nonce und die Reihenfolge von jeden Parameter erraten. Der erfolgreiche Miner, der als erstes die Lösung findet, wird mit einer Belohnung (Anzahl von Bitcoins) bekommen.
4. Das Blockchain-Netzwerk wird dann um den Block mit den bestätigten Transaktionen erweitert und wird als Teil der Blockchain gespeichert. [Academy, 2021]
5. Eine Transaktion wird als durchgeführt angesehen.
6. Der Prozess wird wiederholt

Dies ist ein sequentielles Diagramm, das erklärt, wie es funktioniert





3.3 Algorithmus zur Bestimmung der Nonce in Kryptowährungen

Single Block

- [https://blockchain.info/rawblock/\\$block_hash](https://blockchain.info/rawblock/$block_hash)
- You can also request the block to return in binary form (Hex encoded) using ?format=hex

```
{
  "hash": "0000000000000bae09a7a393a8acded75aa67e46cb81f7acaa5ad94f9eacd103",
  "ver": 1,
  "prev_block": "0000000000007d0f98d9edca880a6c124e25095712df8952e0439ac7409738a",
  "mrkl_root": "935aa0ed2e29a4b81e0c995c39e06995ecce7ddbebb26ed32d550a72e8200bf5",
  "time": 1322131230,
  "bits": 437129626,
  "nonce": 2964215930,
  "n_tx": 22,
  "size": 9195,
  "block_index": 818044,
  "main_chain": true,
  "height": 154595,
  "received_time": 1322131301,
  "relayed_by": "108.60.208.156",
  "tx": [
    "--Array of Transactions--"
  ]
}
```

Es ist von Interesse, die technische Funktionsweise von Proof-of-Work zu untersuchen. Als Erstes betrachten wir eine tatsächliche Blockstruktur von der offiziellen Website.

Single Transaction

- [https://blockchain.info/rawtx/\\$tx_hash](https://blockchain.info/rawtx/$tx_hash)
- You can also request the transaction to return in binary form (Hex encoded) using ?format=hex

```
{
  "hash": "b6f6991d03df0e2e04da99cd6bc418aac66049e2cd74b80f14ac86db1e3f0da",
  "ver": 1,
  "vin_sz": 1,
  "vout_sz": 2,
  "lock_time": "Unavailable",
  "size": 258,
  "relayed_by": "64.179.201.80",
  "block_height": 12200,
  "tx_index": "12563028",
  "inputs": [
    {
      "prev_out": {
        "hash": "a3e2bcc9a5f776112497a32b05f4b9e5b2405ed9",
        "value": "100000000",
        "tx_index": "12554260",
        "n": "2"
      },
      "script": "76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
    }
  ],
  "out": [
    {
      "value": "98000000",
      "hash": "29d6a3540acfa0a950bef2bfdc75cd51c24390fd",
      "script": "76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
    },
    {
      "value": "2000000",
      "hash": "17b5038a413f5c5ee288caa64cfab35a0c01914e",
      "script": "76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
    }
  ]
}
```

Abbildung 3.1: Die echten Blockchain-Block-Transaktionen.

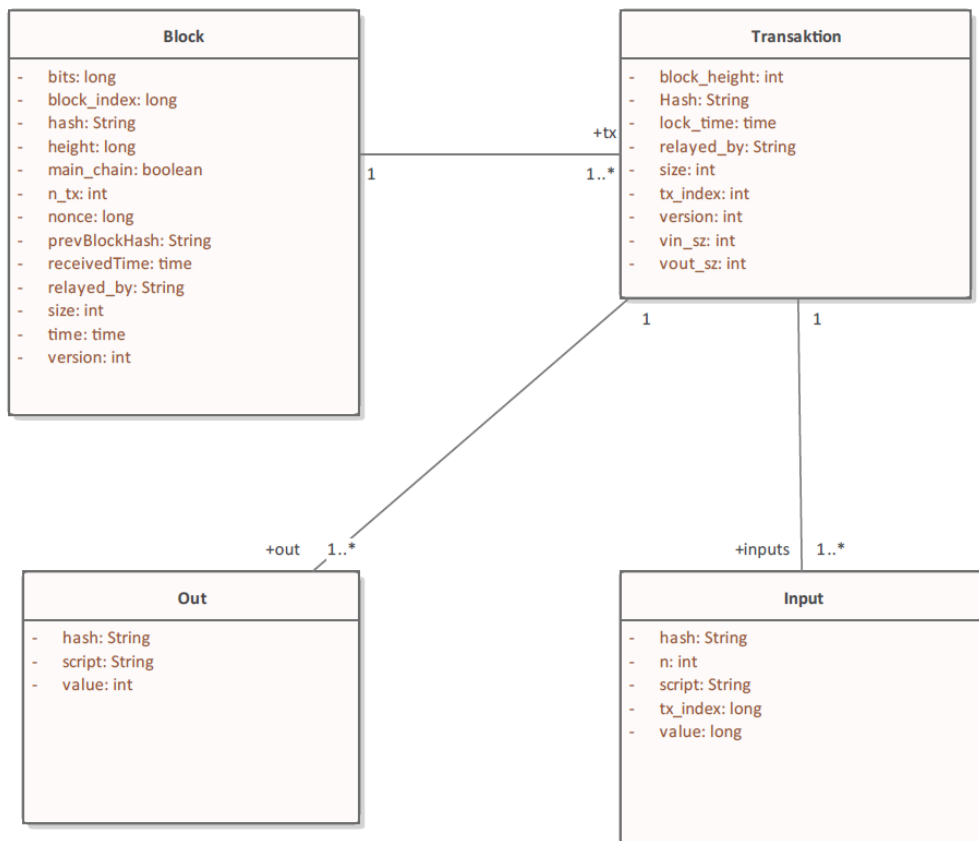


Abbildung 3.2: Das nächste Diagramm, das als Klassendiagramm bezeichnet wird, gibt eine visuelle Darstellung aller Daten, die im realen Blockchain-Netzwerk enthalten sind. Dieses Diagramm ist hilfreich, um die Implementierung des Blockchain-Netzwerks besser zu verstehen und zu analysieren. Es zeigt die Beziehungen und Abhängigkeiten zwischen den verschiedenen Elementen des Netzwerks und hilft, die Struktur und Funktionsweise des Systems zu verdeutlichen. Die Verwendung eines Klassendiagramms ermöglicht es, die komplexen Zusammenhänge einfacher darzustellen und die Implementierung des Blockchain-Netzwerks besser zu verstehen.

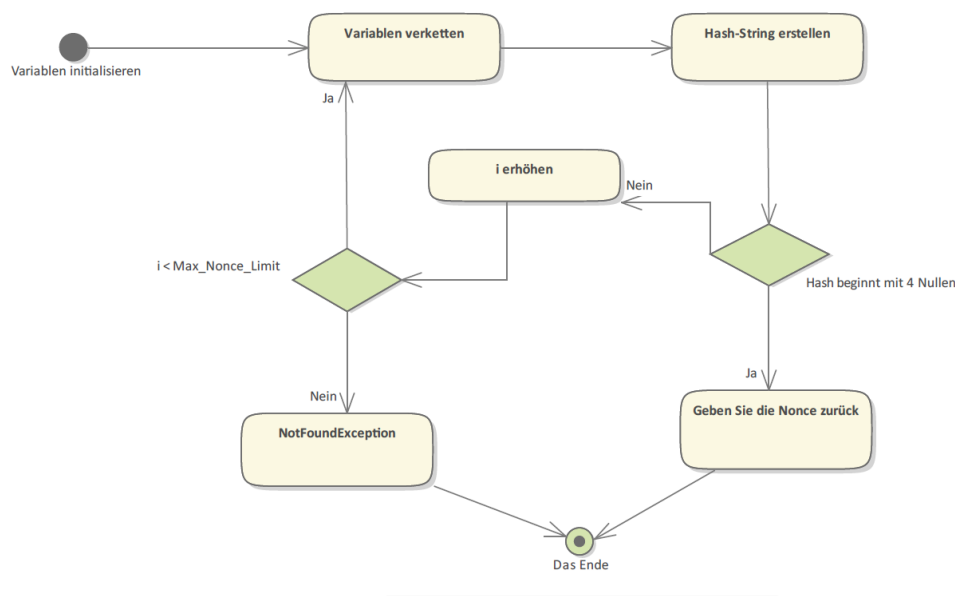


Abbildung 3.3: Der Algorithmus zur Bestimmung der Nonce wird mit dem Aktivitätsdiagramm erklärt. Zunächst müssen wir die initialen Daten initialisieren, einschließlich des `MaxNonceLimit`, der Anzahl der Nullen, die der Hash haben sollte. In diesem Beispiel betrachten wir die Anforderung, dass der Hash mit 4 Nullen beginnen sollte. Es ist wichtig zu beachten, dass die Anzahl der Nullen eine wichtige Rolle bei der Bestimmung der Komplexität des Algorithmus spielt. Je höher die Anzahl der Nullen, desto länger wird es dauern, die Nonce mit begrenzter Hardware zu finden. Wir sollten auch unsere Inkrementierungsvariable für die for-Schleife initialisieren.

Dies ist der Algorithmus der für dieses Beispiel zum Schürfen von Bitcoin geschrieben wurde

Algorithm 1 Nonce für gültigen Hash finden

```

1: nonce ← 0
2: repeat
3:   hash ← Hash(block_data, nonce)
4:   if hash meets difficulty level then
5:     return nonce
6:   end if
7:   nonce ← nonce + 1
8: until hash meets difficulty level
  
```

3.4 Vor- und Nachteile von Proof-Of-Work

Um die Vor- und Nachteile dieser Methode genau zu erklären, wurde diese Tabelle erstellt: Fool, 2022

| Vorteile | Nachteile |
|--------------------------|---|
| Sicherheit | Hohe Energiekosten |
| Gute Anreizstruktur | Langsame Transaktionsgeschwindigkeiten |
| Breite Akzeptanz | Mögliche Zentralisierung von Mining-Pools |
| Verteilte Konsensfindung | Hardware-Anforderungen |

Eklärung :

- **Sicherheit :** Um ein hohes Maß an Sicherheit in einem auf Proof-Of-Work basierenden Blockchain-Netzwerk zu gewährleisten, müsste eine spekulative Person nicht die Kontrolle über den größten Teil der Mining-Kapazität übernehmen. Dies würde bedeuten, mindestens 50% des Netzwerks zu besitzen, was aufgrund der verteilten Natur von Proof-of-Work-Systemen als unmöglich angesehen wird. Eine solche Person würde auch eine große Menge an Hardware und Energie benötigen, um die notwendige Rechenleistung erbringen zu können.
- **Gute Anreizstruktur :** Eine gute durchdachte Anreizstruktur ist ein wesentlicher Faktor für den Erfolg eines Proof-of-Work-Systems. Die Miner erhalten eine finanzielle Belohnung für das Lösen von Rechenproblemen und die damit verbundenen Anstrengungen, was sie dazu veranlasst, ihre Rechenleistung (z.B. : mit Rig MiningGeräte) zur Verfügung zu stellen, um auf diese Weise die Integrität und Sicherheit der Blockchain zu gewährleisten. Dies bedeutet, dass eine gute Anreizstruktur auch dazu beitragen kann, das System im Gleichgewicht zu halten und die Teilnahme der Miner zu fördern. Wenn die Belohnungen für das Mining zu niedrig sind, könnten die Miner weniger motiviert sein, ihre Rechenleistung zur Verfügung zu stellen, denn manchmal, wenn die Belohnung zu niedrig ist, wird dies nicht die Stromkosten für die Mining-Operationen bezahlen, folglich könnte die Sicherheit darunter leiden. Andererseits könnten zu hohe Belohnungen dazu führen, dass das System aus dem Gleichgewicht gerät und die Mining-Pools zentralisiert werden. Es ist wichtig, dass die Anreizstruktur von Proof-of-Work-Systemen sorgfältig angepasst wird, um eine ausgewogene Beteiligung der Miner und ein hohes Sicherheitsniveau zu gewährleisten.
- **Breite Akzeptanz :** PoW wird in der Kryptowährungsgemeinschaft weitgehend akzeptiert, da diese Methode ein hohes Maß an Sicherheit sowie Integration und Dezentralisierung bietet.
- **Verteilte Konsensfindung :** Die dezentralisierte Konsensbildung, die hier in Abschnitt 2.4.3 erklärt ist ein wichtiger Aspekt von Blockchain-Systemen.

Obwohl der Proof-of-Work ein wichtiger Konsensmechanismus in vielen Kryptowährungen ist, gibt es auch einige Nachteile, die berücksichtigt werden sollten.

- **Hohe Energiekosten :** Der Betrieb eines Proof-of-Work-Blockchain-Netzwerks kann energieintensiv sein, da die Miner Rechenleistung aufbringen müssen, um neue Blöcke zu erzeugen und Transaktionen zu validieren. Dies erfordert ständig den Einsatz von speziellen Mining-Geräten, die viel Energie verbrauchen und möglicherweise auch Kühlsysteme benötigen, um hohe Temperaturen zu vermeiden. Eine Möglichkeit, den Energiebedarf des Mining-Betriebs zu senken, besteht darin, erneuerbare Energien zur Erzeugung des wichtigen Stroms zu nutzen. Dies kann zwar eine größere Anfangsinvestition erfordern, bietet aber auch langfristige Vorteile, da die Mining-Unternehmen keinen externen Strom verbrauchen und somit keine Energiekosten anfallen. Erneuerbare Energien wie Solar- und Windenergie können eine umweltfreundliche Alternative zu fossilen Brennstoffen bieten und können helfen, die CO₂-Emissionen aus dem Bergbau zu reduzieren. Es ist wichtig, den Energiebedarf des Bergbaubetriebs sorgfältig zu prüfen, um sicherzustellen, dass er nachhaltig und umweltfreundlich ist. Wenn zu viele Bergleute ohne Rücksicht auf den Energieverbrauch abbauen, könnten die Energiepreise ansteigen und die Umwelt schädigen. Daher ist es notwendig, dass die Bergleute ihren Energieverbrauch ernsthaft planen und es ist besser, erneuerbare Energien zu nutzen.
- **Langsame Transaktionsgeschwindigkeiten :** Eines der Haupthindernisse für die Geschwindigkeit von Bitcoin-Transaktionen ist die Tatsache, dass sie von Minern validiert werden müssen, um in die Blockchain aufgenommen zu werden. Da die Schwierigkeit, einen neuen Block zu finden, von Zeit zu Zeit angepasst wird, kann es durchaus einige Zeit dauern, bis ein Block gefunden wird. Die durchschnittliche Zeit, die benötigt wird, um einen neuen Block zu finden, beträgt derzeit etwa 10 Minuten. Das bedeutet, dass es normalerweise etwa 10 Minuten dauert, bis eine Transaktion bestätigt und in die Blockchain eingetragen wird. Für einige Nutzer mag dies als langsam empfunden werden, insbesondere im Vergleich zu herkömmlichen Zahlungsmethoden. Es gibt jedoch Maßnahmen, die die Geschwindigkeit von Bitcoin-Transaktionen verbessern können, wie z. B. die Verwendung von SegWit (Segregated Witness) oder Lightning-Netzwerken. Diese Technologien können die Größe der Transaktionen verringern und somit ihre Geschwindigkeit erhöhen.


| | |
|---------------|---|
| Depth | 1 |
| Size | 1 695 479 |
| Version | 0×2a152000 |
| Merkle Root | d7-3b  |
| Difficulty | 36 950 494 067 222,41 |
| Nonce | 1 117 283 344 |
| Bits | 386 375 189 |
| Weight | 3 993 569 WU |
| Minted | 6,25 BTC |
| Reward | 6.35686843 BTC |
| Mined on | Nov 28, 2022, 6:06:41 PM |
| Height | 765 066 |
| Confirmations | 1 |
| Fee Range | 0-1274 sat/vByte |
| Average Fee | 0.00006392 |
| Median Fee | 0.00002340 |
| Miner | Unknown |

Abbildung 3.4: Die heutige Schwierigkeit ist
URL : https://www.blockchain.com/explorer/api/blockchain_api

- **Mögliche Zentralisierung von Mining-Pools** : Proof-of-Work-Mining-Pools können zentralisiert werden, wenn einige wenige große Mining-Pools einen Hauptteil der Blockgenerierungsrate kontrollieren und damit Kontrolle über das Netzwerk ausüben können. Dies kann zu einer Verletzung der Dezentralisierung und der Netzwerksicherheit führen, wenn diese Pools die Macht haben, das Netzwerk zu beeinflussen oder anzugreifen.
- **Hardware-Anforderungen** : Das Bitcoin-Mining kann hohe Investitionskosten erfordern, da oftmals spezielle Mining-Hardware wie leistungsstarke Grafikkarten, entsprechende Motherboards oder sogar die Erstellung von Rig-Computern notwendig sind, um erfolgreich neue Blöcke zu erzeugen. Der hohe Preis dieser Hardware kann den Einstieg in das Bitcoin-Mining hingegen für Gruppen oder kleine Unternehmen schwierig machen. Dennoch kann das Bitcoin-Mining lukrativ sein, vor allem für große Mining-Unternehmen, die über mehrere Mining-Anlagen verfügen und Zugang zu billigem Strom haben. In diesen Fällen können die Einnahmen aus dem Mining die Investitionskosten schnell übersteigen und eine profitable Einnahmequelle darstellen.

4 Schwierigkeit und Sicherheit des Proof-Of-Work

4.1 Was hat es mit der Schwierigkeit auf sich ?

- Die Schwierigkeit besteht darin, die gewünschte Hash-Ausgabe zu finden. Zum Beispiel Bitcoin, es wird eine Frage gestellt: Wie viele Nullen soll die Ausgabe am Anfang des Strings haben. Je mehr Nullen gefordert sind, desto schwieriger wird es schließlich, den Output zu finden. Academy, 2021
- Die Schwierigkeit ist bei Bitcoin immer so gewählt, dass im Schnitt alle zehn Minuten ein neuer Block gefunden werden soll. Dieser Benchmark wird alle zwei Wochen überprüft. Stellt sich heraus, dass in zwei Wochen der Richtwert von 2.016 Blöcken überschritten wurde, also mehr Blöcke als gewünscht gefunden wurden, ist die Schwierigkeit zu gering und wird nach oben korrigiert – und umgekehrt. Academy, 2021

4.2 Wie wird die Schwierigkeit genau angepasst bei Proof of Work ?

- Die Schwierigkeit eines PoW kann angepasst werden, um sicherzustellen, dass die Blockerzeugungsrate stabil bleibt. In einem PoW-System werden Miner ausgewählt, um einen neuen Block mit PoW zu erstellen. Wenn viele Miner am Netzwerk beteiligt sind, werden die Blöcke schneller erstellt, was zu einer Erhöhung der Blockerzeugungsrate führt. Wenn hingegen nur wenige Miner am Netzwerk teilnehmen, werden die Blöcke sehr langsam erstellt, was zu einer Abnahme der Blockerzeugungsrate führt. Um die Stabilität der Blockerzeugungsrate zu behalten, wird eine Technologie zur Anpassung der Schwierigkeit verwendet, die in Englisch "Difficulty Adjustment Algorithm (DAA)" heißt. Diese Implementierung ist spezifisch für jede verwendete Kryptowährung, aber ihr Konzept besteht darin, die Schwierigkeit auf dynamische Weise anzupassen.
- Das Konzept dieses Algorithmus besteht darin, die Schwierigkeit so anzupassen, dass die für die Erstellung eines neuen Blocks erforderliche Zeit konstant bleibt. Diese Änderung der Schwierigkeit wird für jeden Block dynamisch angepasst, abhängig von der Zeit, die für die Erstellung des vorherigen Blocks benötigt wurde. Wenn ein Block schneller als erwartet erstellt wurde, wird die Schwierigkeit erhöht, um die Blockerstellung zu verlangsamen. Falls ein Block langsamer

erstellt wurde, wird die Schwierigkeit verringert, um die Blockerstellung zu beschleunigen. Beachten Sie, dass die aktuelle Schwierigkeit der Blockerstellung in der Blockchain 10 Minuten ist. Dabei hilft die Verwendung von DAA diese Schwierigkeit konstant zu behalten.

4.3 was passiert wenn die PoW-Schwierigkeit zu niedrig eingestellt sein?

Wenn die PoW Difficulty zu niedrig eingestellt ist, kann dies zu Instabilitäts- und Integritätsproblemen, Sicherheitsproblemen und auch wirtschaftlichen Problemen führen: Sehr hohe Blockgenerierungsrate: Miner können schnell Blöcke erstellen, was zu einer höheren Blockgenerierungsrate führt, da die Schwierigkeit niedrig ist, was manchmal zu einer Überlastung des Netzwerks und einer langsameren Verarbeitung von Transaktionen führt. Sicherheitsprobleme: Ein niedriger Schwierigkeitsgrad macht das Netzwerk anfällig für 51%-Angriffe, bei denen ein Angreifer die Mehrheit der Mining-Kapazität nutzen und das Netzwerk mit leistungsstarker Hardware manipulieren kann. Wirtschaftliche Probleme: Wenn Blöcke schneller erzeugt werden, kann dies zu einem schnellen Drucken führen, da Kryptowährungen gedruckt werden. Dies kann den Wert der Kryptowährung verringern.

4.4 wie beeinflusst die Schwierigkeit des PoW und die Größe des netzwerkes die Sicherheit und Intigrität der Blockchain?

Der Schwierigkeitsgrad des Proof of Work (PoW) und die Größe des Netzwerks haben einen erheblichen Einfluss auf die Sicherheit und Integrität der Blockchain.

PoW-Schwierigkeit : Die PoW-Schwierigkeit bestimmt das Verhältnis zwischen der Zeit und der Anzahl der Berechnungen, die zur Lösung eines neuen Blocks erforderlich sind. Je höher der Schwierigkeitsgrad, desto mehr Rechenleistung ist für die Lösung des Blocks erforderlich. Diese zusätzliche Rechenleistung macht das Netzwerk sicherer, da es für einen Angreifer schwieriger ist, genügend Mining-Power zu haben, um seinen 51%-Angriff auszuführen.

Größe des Netzwerks : Ein großes Netzwerk bedeutet mehr Mining-Kapazität und eine bessere Verteilung der Verarbeitungsleistung, wodurch das Netzwerk sicherer wird. Größere Netzwerke sind auch weniger anfällig für 51%-Angriffe, da Angreifer mehr Mining-Kapazität benötigen, um ihre Angriffe zu starten.

Die Beziehung zwischen diesen beiden Begriffen besteht darin, dass sie beide zur Verbesserung der Sicherheit und Integrität von Blockchains beitragen. Eine angemessene PoW-Schwierigkeit hält das Netzwerk zu 51% sicher vor Angriffen, während ein größeres Netzwerk eine bessere Verteilung der Mining-Kapazität gewährleistet und das Netzwerk insgesamt stabiler macht.

5 Sidechains

Am 22. Oktober 2014 wurde die Idee einer Sidechain in einem bahnbrechenden wissenschaftlichen Dokument vorgestellt. Das Dokument wurde von Adam Back, dem Schöpfer von HashCash und CEO von Blockstream, und einer Gruppe führender Bitcoin-Ingenieure verfasst, darunter Matt Corallo, Luke Dashjr und Mark Friedenbach, Mitbegründer von Blockstream.

Diese Autoren spielten eine wichtige Rolle bei der Entwicklung von Satoshi Nakamotos Vision eines elektronischen Währungssystems, indem sie den Proof-of-Work-Konsensmechanismus von HashCash in die Bitcoin-Blockchain integrierten. Sie räumten jedoch ein, dass es noch Raum für Verbesserungen gab, wenn Bitcoin ein weltweites Publikum bedienen sollte.

Zu dieser Zeit stand die Bitcoin-Infrastruktur vor Herausforderungen wie Kompromissen zwischen Skalierbarkeit und Dezentralisierung sowie Bedenken hinsichtlich Datenschutz und Zensur. Um diesen Herausforderungen zu begegnen, schlugen die Autoren eine neue Technologie namens "pegged sidechains" vor, die es ermöglichen würde, Bitcoins und andere Ledger-Assets zwischen mehreren Blockchains zu transferieren. Dies würde den Nutzern den Zugang zu neuen und innovativen Kryptowährungssystemen ermöglichen, indem sie die Vermögenswerte nutzen, die sie bereits besitzen.

Das Weißbuch zu Seitenketten hat eine revolutionäre Lösung für die Beschränkungen der Bitcoin-Infrastruktur vorgestellt und die Grundlage für neue Entwicklungen in der Welt der Blockchain-Technologie geschaffen. ["Sidechain", 2022]

5.1 Was ist eine Sidechain?

5.1.1 Definition von Sidechain

Die Sidechains der Blockchain werden als separate Blockchains behandelt, die mit der Hauptblockchain verbunden sind. Diese Beziehung zwischen ihnen ermöglicht den Austausch und die Überprüfung von Daten auf die gleiche Weise wie bei der Hauptblockkette. Sidechains bieten in der Regel nicht die gleiche Sicherheit und Skalierbarkeit wie ihre Hauptblockchain. Das liegt daran, dass es weniger Knoten gibt und somit weniger Ressourcen benötigt werden. Daher sollte die Verwendung von Sidechains gut abgewogen werden.

5.1.2 Sidechain, auf die Proof-Of-Work basieren

Die Sidechains der Blockchain werden durch PoW verifiziert. Das bedeutet, dass die Sidechain-Knoten eine bestimmte Anzahl von Ressourcen benötigen, um die Integrität des Netzwerks zu gewährleisten und Transaktionen zu bestätigen. Allerdings kann die Schwierigkeit der PoW für Sidechains und Mainchains unterschiedlich oder gleich sein, je nach den spezifischen Anforderungen und Einschränkungen der Sidechains.

5.1.3 Eigenschaften

Eine Sidechain ist ein einzelnes Blockchain-Netzwerk, das über eine bidirektionale Verbindung mit einer anderen Blockchain, dem sogenannten Mainnet oder der übergeordneten Blockchain (hier wird alles in Abschnitt 2.1 beschrieben), verbunden ist. Diese sekundäre Blockchain hat ihren eigenen Satz von Konsensprotokollen, was den Datenschutz und die Sicherheit verbessert und den Bedarf an Vertrauen verringert.

Einer der Hauptvorteile von Sidechains ist die Möglichkeit des einfachen Austauschs von Vermögenswerten zwischen dem Mainnet und der sekundären Blockchain. Dadurch können digitale Vermögenswerte wie Token sicher von einer Blockchain auf eine andere übertragen werden, was Projekten neue Möglichkeiten eröffnet, ihr Ökosystem auf dezentrale Weise zu erweitern.

Nehmen wir an, Sie haben einige Bitcoin im Haupt-Bitcoin-Netzwerk. Um Ihre Bitcoin auf eine Sidechain zu verschieben, senden Sie sie an eine bestimmte Ausgabeadresse. Diese Adresse könnte eine Hardware-Wallet, eine Hot-Wallet oder eine Sidechain sein. Sobald die Transaktion bestätigt ist, wird sie über das Bitcoin-Netzwerk verbreitet.

Nach einer kurzen Sicherheitsprüfung wird der Bitcoin auf die Sidechain übertragen, so dass Sie Ihr Vermögen in das neue Netzwerk verschieben können. Dieser Prozess ermöglicht einen nahtlosen Übergang von Vermögenswerten zwischen verschiedenen Blockchain-Netzwerken und bietet den Nutzern mehr Optionen und Flexibilität. [“Sidechain”, 2022]

Obwohl das Konzept der Seitenketten einfach zu sein scheint, gibt es eine Reihe entscheidender Elemente, die notwendig sind, damit sie optimal funktionieren. Zu diesen wesentlichen Komponenten gehören:

- Two-way peg
- Intelligente Verträge

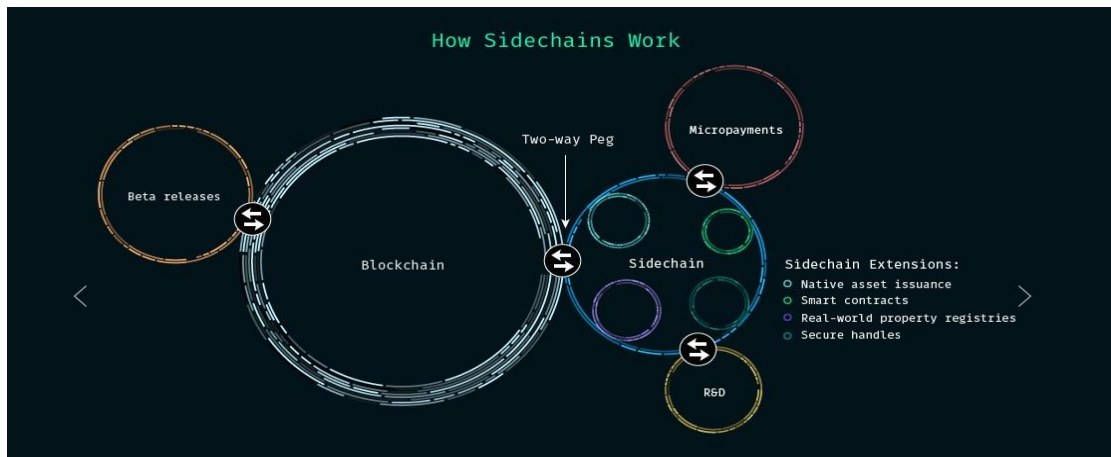


Abbildung 5.1: Mechanismus der Sidechain

<https://cloudfront-us-east-1.images.arcpublishing.com/coindesk/V2EL75HGEVFITCE5U752QJ4HCY.jpg>

5.2 Two-way peg

Sidechains wurden geschaffen, um eine nahtlose Übertragung von digitalen Vermögenswerten zwischen verschiedenen Blockchains zu ermöglichen, unabhängig davon, wer sie besitzt. Diese Übertragung sollte ohne die Möglichkeit der Beeinflussung durch eine dritte Partei erfolgen. Um dies zu erreichen, wird ein Zwei-Wege-Peg benötigt, den man sich wie einen Zwei-Wege-Tunnel vorstellen kann, der die beiden Blockchains miteinander verbindet.



Abbildung 5.2: Two way peg

<https://cloudfront-us-east-1.images.arcpublishing.com/coindesk/RIPFDA7FMJFEBBMCAQKGPV55HI.jpg>

Laut dem Sidechain-Whitepaper (“The mechanism by which coins are transferred between sidechains [...] a pegged sidechain is a sidechain whose assets can be imported from and returned to other chains.”) bezieht sich ein Zwei-Wege-Peg auf die Methode, mit der digitale Vermögenswerte wie Bitcoin zwischen der Hauptblockchain und der neuen Sidechain hin und her übertragen werden können. Wichtig ist, dass die Übertragung von Vermögenswerten nicht tatsächlich stattfindet. Stattdessen werden die Vermögenswerte auf der Hauptblockchain gesperrt, während der entsprechende Wert auf der Sidechain freigegeben wird. [“Sidechain”, 2022]

Dies setzt das Vertrauen voraus, dass die Teilnehmer oder ”Validierer”, die an dem wechselseitigen Pflöck beteiligt sind, ehrlich handeln. Andernfalls könnte es zu betrügerischen Überweisungen kommen oder legitime Überweisungen könnten blockiert werden.

5.3 Intelligente Verträge

Um digitale Vermögenswerte von einem Mainnet auf eine Sidechain oder umgekehrt zu übertragen, ist ein Prozess erforderlich, der außerhalb des Haupt-Blockchain-Netzwerks stattfindet und Informationen zwischen den beiden Blockchains überträgt. Dieser Prozess, der als Off-Chain bezeichnet wird, beinhaltet einen intelligenten Vertrag, der sicherstellt, dass die Übertragung von digitalen Vermögenswerten fair und sicher ist. [“Sidechain”, 2022] Wenn eine Transaktion stattfindet, bestätigt der intelligente Vertrag diese und benachrichtigt das Hauptnetz. Anschließend sendet der Off-Chain-Prozess die Transaktionsdetails an einen intelligenten Vertrag auf der Sidechain, wo sie überprüft werden. Nach der Verifizierung werden die digitalen Vermögenswerte auf der Sidechain freigeschaltet, so dass sie frei zwischen den beiden Blockchains bewegt werden können. [“Sidechain”, 2022] Intelligente Verträge spielen eine wichtige Rolle bei der Gewährleistung der Sicherheit dieser Transaktionen, da sie die Teilnehmer sowohl im Mainnet als auch auf

der Sidechain zu ehrlichem Handeln verpflichtet. Durch ein sicheres Verfahren können digitale Vermögenswerte zwischen den Blockchains übertragen werden, ohne dass das Risiko eines Fehlverhaltens besteht.[“Sidechain”, 2022]

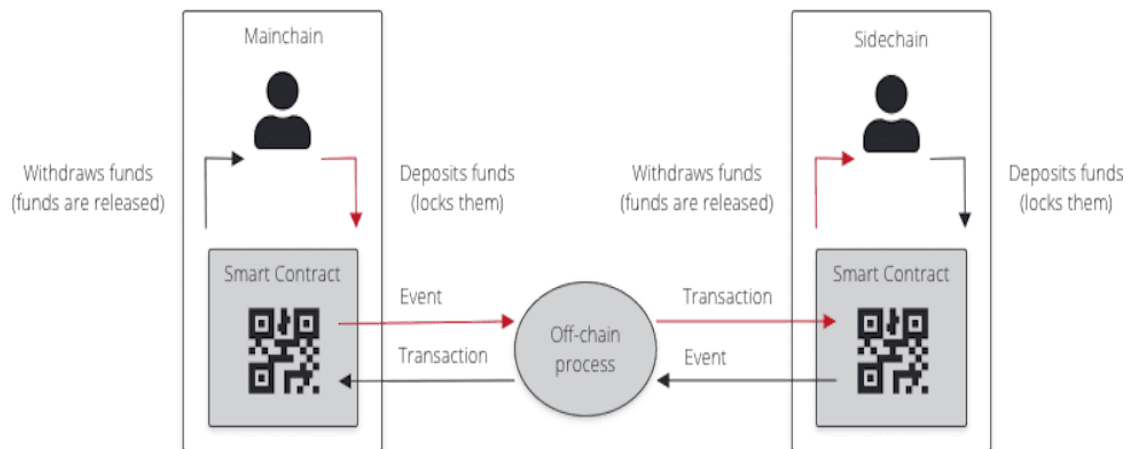


Abbildung 5.3: Intelligente Verträge

<https://cloudfront-us-east-1.images.arcpublishing.com/coindesk/5XF3FUGIXZBTFTHPYD47KK5FA.png>

5.4 Sidechain bei Bitcoin

Beispiele für praktische Sidechain-Anwendungen sind das Liquid Network und Root-Stock (RSK). Beide Sidechains sind mit dem Bitcoin-Mainnet verbunden und können nur für Aktivitäten im Zusammenhang mit Bitcoin genutzt werden. [“Sidechain”, 2022]

Das Liquid Network, eine von Blockstream entwickelte Open-Source-Sidechain, baut auf dem Bitcoin-Mainnet auf. Die schnelle Blockentdeckungszeit von einer Minute im Vergleich zu 10 Minuten bei Bitcoin ermöglicht es, 10 Mal mehr Blöcke zu seiner Sidechain hinzuzufügen. Darüber hinaus bietet das Netzwerk einen verbesserten Datenschutz, indem es die Menge und die Art der übertragenen digitalen Vermögenswerte verbirgt. [“Sidechain”, 2022]

RSK hingegen ist eine Sidechain, die speziell für die Unterstützung intelligenter Verträge entwickelt wurde. Bei der Verwendung von RSK wird Bitcoin vorübergehend im Mainnet gesperrt und als RSK-eigene Währung, Smart Bitcoin (SBTC), freigegeben. Aufgrund seiner Smart-Contract-Fähigkeiten müssen Nutzer ihre Bitcoin nicht in andere Vermögenswerte umwandeln, um Smart Contracts zu nutzen, was es mit anderen Blockchain-Netzwerken wie Ethereum interoperabel macht.

Prozess der Sidechain bei Proof of work

1. Die Übertragung von digitalen Assets von der Hauptkette zur Sidechain wird gestartet.
2. Das digitale Asset wird an eine spezielle Ausgabeadresse auf der Hauptkette gesendet.
3. Die Übertragung wird bestätigt und auf beiden Blockchains dokumentiert.
4. Die Bestätigung wird über das Netzwerk der Hauptkette verbreitet.
5. Nach einer Sicherheitsprüfung wird das digitale Asset auf die Sidechain transferiert.
6. In der Sidechain wird das digitale Asset in einem Block gespeichert und über das Netzwerk verbreitet.
7. Das digitale Asset ist jetzt auf der Sidechain verfügbar und kann für Transaktionen verwendet werden.
8. Die Validierung jeder Transaktion in der Sidechain erfolgt durch den PoW-Konsensmechanismus. Minenarbeiter lösen ein komplexes mathematisches Problem, um einen neuen Block zu validieren und zu hinzufügen.
9. Sobald eine Transaktion bestätigt wurde, wird sie in einem Block gespeichert und über das Netzwerk verbreitet.

5.5 Woher weiß ein Client, dass er in der Mainchain ist und nicht in einer Sidechain ?

- Es ist wichtig, dass jeder Kunde weiß, zu welcher Kette er gehört, um sicherzustellen, dass er die richtigen Informationen erhält und seine Transaktionen korrekt verarbeitet werden. Dies bedeutet, dass die Kunden über die richtigen Mechanismen verfügen müssen, um zu wissen, in welcher Kette sie sich befinden. Es gibt also zwei Merkmale, die für jede Kette spezifisch sind.
- Eine Haupt-Blockchain kann manchmal ein anderes Konsensprotokoll verwenden als eine Neben-Blockchain, wodurch es für einen Kunden einfacher wird, zwischen den beiden Arten von Ketten zu unterscheiden. Auch kann die Haupt-Blockchain bestimmte Regeln haben, die für sie einzigartig sind und sich von denen der Neben-Blockchain stark unterscheiden.
- Ein weiteres Unterscheidungsmerkmal ist, dass ein Kunde auch die Länge der Kette überprüfen kann, um festzustellen, ob es sich um die Mainchain oder eine Sidechain handelt. Wenn ein Kunde also eine Kette sieht, die länger ist als er erwartet, kann er erkennen, dass er sich in einer Sidechain befindet. Da die Mainchain oft am längsten ist.

5.6 Was gibt es für Angriffsszenarien und wie funktionieren diese ?

In der Blockchain-Welt gibt es eine Reihe von Angriffsszenarien, die die Integrität und Sicherheit einer Blockchain gefährden können.

- 51% Angriff
- Sybil-Angriff
- Doppelspendeangriff
- Routing-Angriff

5.7 Sybil-Angriff

5.7.1 Was ist ein Sybil-Angriff ?

Ein **Sybil-Angriff** ist ein Angriff, bei dem viele Knoten in einem Netzwerk im Besitz derselben Partei sind und versuchen, die Netzwerkaktivität zu stören, indem sie das Netzwerk mit fehlerhaften Transaktionen überfluten oder die Weiterleitung gültiger Transaktionen manipulieren. Diese Angriffe sind theoretisch und größtenteils eine grundlegende Designentscheidung bei der Entwicklung eines Kryptowährungssystems. [“Cybersecurity Makes me Wanna Cry”, 2022]

5.7.2 Die Funktionsweise dieses Angriffs

In einem Blockchain-System wie Bitcoin werden Entscheidungen von allen Mining-Punkten und -Zentren durch Abstimmung getroffen. In diesem Fall kann ein Vorschlag von den Minern entweder angenommen oder abgelehnt werden. Wenn mehrere Identitäten im Netzwerk erstellt werden, können Angreifer für so viele Identitäten stimmen, wie sie kontrollieren. Mit Sybil-Angriffen kann der Informationsfluss in einem Netz manipuliert werden. Dieser Angriff kann beispielsweise dazu verwendet werden, die IP-Adresse eines an das Netz angeschlossenen Punktes zu ermitteln. Dies gefährdet die Sicherheit, Privatsphäre und Anonymität der Online-Nutzer. Ein Angreifer braucht nur die Kontrolle über Punkte im Netz zu übernehmen, Informationen von diesen Punkten zu sammeln und gefälschte Punkte zu erstellen, die seine Identität angeben. Sobald das Netz unter der Kontrolle des Angreifers ist, kann er Zensur ausüben und andere Nutzer an der legalen Nutzung des Netzes hindern. [“Sybil Attack”, 2022]

Ablauf eines Sybil-Angriffs

1. Der Angreifer erstellt mehrere falsche Knoten oder Identitäten im Netzwerk. Dies kann durch das Ausführen mehrerer Instanzen der Bitcoin-Software oder durch andere Mittel geschehen, um legitime Knoten zu imitieren.

2. Der Angreifer verbindet diese falschen Knoten dann mit dem Netzwerk, um den Informationsfluss zu kontrollieren.
3. Wenn der Angreifer die Kontrolle über eine große Anzahl von Knoten übernimmt, kann er tatsächlich mehrfach über einen bestimmten Vorschlag oder eine Entscheidung im Netzwerk abstimmen, was ihm einen unfairen Vorteil gegenüber den legitimen Nutzern verschafft. Auch kann der Angreifer seine Kontrolle über die Knoten nutzen, um Informationen über andere Netzwerkbenutzer zu sammeln und so deren Privatsphäre und Anonymität zu gefährden.
4. Sobald ein Angreifer genügend Kontrolle über das Blockchain-Netzwerk hat, wird er beginnen, Zensur auszuüben, indem er legitime Nutzer daran hindert, das Netzwerk zu nutzen.

5.7.3 Wie kann man sich vor diesem Angriff schützen?

Diese Methode wurden aus diesem Artikel [“Sybil Attack”, 2022] entnommen und zusammengefasst.

Identitätsüberprüfung

Die Identitätsüberprüfung ist eine Technik, die dazu beitragen kann, Sybil-Angriffe zu verhindern, indem die Identität von Einheiten in einem Netz überprüft wird. Dies kann direkt geschehen, indem eine zentrale Behörde befragt wird, oder indirekt, indem man sich auf zuvor akzeptierte Identitäten stützt. Es können verschiedene Methoden wie die Überprüfung von Telefonnummern, Kreditkarten und IP-Adressen verwendet werden, die jedoch nicht perfekt sind und missbraucht werden können. Die identitätsbasierte Validierung bietet zwar die Möglichkeit, Rechenschaft abzulegen, aber sie opfert die Anonymität, die für die meisten Arten von Peer-to-Peer-Netzen wichtig ist.

Soziale Vertrauensdiagramme

Eine Möglichkeit, Sybil-Angriffe zu verhindern, besteht in der Analyse von Konnektivitätsdaten in sozialen Graphen, um den Schaden durch einen bestimmten Angreifer zu begrenzen und gleichzeitig die Anonymität zu wahren. Techniken wie SybilGuard, SybilLimit, Advogato Trust Metric und sparsity-based metric können zu diesem Zweck verwendet werden. Diese Techniken sind jedoch nicht perfekt und beruhen möglicherweise auf bestimmten Annahmen, die nicht für alle realen sozialen Netzwerke gelten. Daher können P2P-Netzwerke, die sich auf Social-Trust-Graph-Techniken stützen, immer noch anfällig für Sybil-Angriffe in kleinem Maßstab sein.

Wirtschaftliche Kosten

Wirtschaftliche Kosten, die Investitionen in Ressourcen wie Anteile oder Speicherplatz in bestehenden Kryptowährungen und die Implementierung von Proof of Work (PoW)

erfordern, können einen Sybil-Angriff verteuern. Bei PoW muss jeder Nutzer nachweisen, dass er Rechenaufwand betrieben hat, um ein kryptografisches Rätsel zu lösen. Bei erlaubnisfreien Kryptowährungen wie Bitcoin konkurrieren die Miner darum, Blöcke an die Blockchain anzuhängen, und erhalten Belohnungen, die in etwa dem Rechenaufwand entsprechen, den sie in einer bestimmten Zeit investiert haben.

Validierung der Personalität

Eine Möglichkeit, Sybil-Angriffe zu verhindern, besteht darin, dass P2P-Netze eine Identitätsüberprüfung verlangen und die Regel eine Einheit pro Person einführen. Eine Validierungsinstanz kann einen Mechanismus verwenden, bei dem die tatsächliche Identität der Teilnehmer nicht bekannt sein muss, z. B. indem die Nutzer ihre Identität durch ihre Anwesenheit zu einer bestimmten Zeit und an einem bestimmten Ort nachweisen, auch bekannt als Pseudonym-Party. Diese Methode des Nachweises der Personenidentität ist ein vielversprechender Weg, um Identitäten in erlaubnisfreien Blockchain- und Kryptowährungsnetzwerken zu validieren und gleichzeitig die Anonymität zu wahren und sicherzustellen, dass jeder menschliche Teilnehmer nur eine Stimme hat.

5.8 Doublespending

5.8.1 Was ist Doublespending ?

Double Spending ist das Risiko, dass eine Kryptowährung mehrfach ausgegeben werden kann. Unter bestimmten Bedingungen in der Blockchain erlauben es, Blöcke zu ändern. So kann die Person, die die Änderung vornimmt, die ausgegebenen Münzen zurückfordern. [“Double Spending”, n. d.]

5.8.2 Die Funktionsweise dieses Angriffs

Für Double Spending muss ein geheimer Block erstellt werden, bevor der tatsächliche Block geschürft wird. Anschließend muss die Person diese Kette in das Netzwerk einbringen, bevor das Netzwerk sie einholt. Wenn dies geschieht, wird diese Kette als der neueste Satz von Blöcken anerkannt und zur Kette hinzugefügt. Die Person, die den Double Spend durchgeführt hat, kann dann jede ausgegebene Kryptowährung zurückholen und erneut verwenden. [“Double Spending”, n. d.]

5.8.3 Ist die Blockchain, die auf PoW basiert, gegen diesen Angriff gesichert ?

Double Spending ist ein Risiko, wird aber durch die Blockchain und die Konsensmethode proof of work minimiert. Die Wahrscheinlichkeit, dass ein geheimer Block in die Blockchain eingefügt wird, ist sehr gering, weil das Netzwerk der Miner den Block tatsächlich überprüfen und akzeptieren müsste. Die einzige Chance für einen Miner mit illegalen Absichten, einen veränderten Block einzufügen, besteht darin, dass er dazu führt, dass er über die leistungsstarke Hardware verfügt, die 51% des Netzwerks einer Blockchain

überschreiten kann, um eine Transaktion mit seinem geheimen Block zu akzeptieren. [“Double Spending”, n. d.]

5.9 51% Angriff

5.9.1 Was ist ein 51%-Angriff ?

Ein 51%-Angriff stellt eine Methode des Angriffs auf Netzwerke dar, die auf Proof-of-Work basieren. Die Angreifer versuchen, mindestens 51% der Hashraten des Netzwerks zu erlangen. Durch die Mehrheit der Netzwerk-Hashraten wäre der Angreifer in der Lage, potenziell doppelte Ausgaben zu tätigen oder Transaktionen rückgängig zu machen. [“51 Angriff”, n. d.]

5.9.2 Die Funktionsweise dieses Angriffs

Wie bereits erwähnt, ist es sehr unwahrscheinlich, dass ein solcher Angriff stattfindet. Dennoch kann es hilfreich sein, sich bewusst zu machen, wie man einem Angreifer die Aufgabe so schwer wie möglich machen kann, damit ein Angriff zu 51% erfolgreich ist. [“51 Angriff”, n. d.]

Nachdem man eine Transaktion erhalten hat, kann man einfach einige Blöcke abwarten. Auf diese Weise erschwert man den Angriff. Ab etwa sechs Bestätigungen ist eine Transaktion mit Bitcoins sehr sicher. Bei Altcoins hängt die Anzahl der zu erwartenden Bestätigungen von der Hashrate des Netzwerks ab.

Ein weiterer Ansatz besteht darin, einen eigenen Full Node zu betreiben. Wer nur einen sogenannten Thin Client nutzt, also eine Software, die nicht selbst die komplette Blockchain speichert, ist besonders anfällig für den 51-Prozent-Angriff. Bei kleinen Guthaben lohnt sich der Aufwand, einen eigenen Full Node zu betreiben, nicht. Bei höheren Beträgen bietet ein Full Node jedoch zusätzliche Sicherheit. [“51 Angriff”, n. d.]

5.9.3 Welche Folgen kann eine 51%-Angriff haben?

- **Double Spending** : Abschnitt 5.9
- **Blockchain-Zensur** : Hacker mit einer ausreichenden Hashrate könnten das Netzwerk auch zensieren, indem sie einen erheblichen Vorsprung bei der Hashrate haben und diesen über einen langen Zeitraum aufrechterhalten. So könnten die Angreifer entscheiden, welche Transaktionen in die Blockchain aufgenommen und welche ausgeschlossen werden. Außerdem könnten sie andere Miner daran hindern, sich am Block-Mining zu beteiligen. [“51 Angriff”, n. d.]

5.9.4 Wie macht sich eine 51%-Angriff bemerkbar?

Ein Angriff um 51% ist ein großes und störendes Ereignis, das nie unbemerkt bleibt. Im Falle eines solchen Angriffs würde die Blockchain neu organisiert werden. [“51 Angriff”, n. d.]

Von Zeit zu Zeit kann es in auf Proof-of-Work basierenden Systemen wie Bitcoin vorkommen, dass zwei Miner gleichzeitig einen neuen Block finden. Diese Blöcke werden als Block A und Block B bezeichnet. Das Netzwerk wird für eine kurze Zeit geteilt. Wenn die Hälfte mit Block B zuerst einen neuen Block findet (Block B+1), teilt sie dies dem gesamten Netzwerk mit. Die Hälfte mit Block A erkennt, dass es eine neue, gültige Version der Blockchain gibt, und organisiert sich neu. Dabei lehnt sie Block A ab und passt die neue Kette mit Block B und Block B+1 an. Dieses Ereignis wird auch als Reorganisation der Blockkette oder "chain-reorg" bezeichnet.

Wenn jedoch ein Miner auch Block A+1 findet und ein anderer Miner gleichzeitig Block B+1 findet, werden die Blockketten durch zwei Blöcke getrennt. Wenn nun eine Neuordnung der Kette stattfindet, ist sie also zwei Blöcke lang. Die Wahrscheinlichkeit, dass dieses Ereignis eintritt, ist deutlich geringer.

Je größer der "chain-reorg" ist, desto unwahrscheinlicher ist das Ereignis und desto sichtbarer ist es. Selbst bei einem Angriff von 51% würde ein "chain-reorg" auftreten. Dieser würde von allen Betreibern vollständiger Knoten und ehrlichen Minern bemerkt werden. Auf diese Weise würde der 51%-Angriff entdeckt und die Bitcoin-Gemeinschaft könnte beschließen, Maßnahmen zu ergreifen.

5.9.5 Die Grenzen des 51%-Angriffs

Die 51%-Angreifer sind zwar mächtig, was das Double-Spending und die Blockchain-Zensur betrifft, aber sie sind nicht allmächtig. Die Regeln des Netzwerks können nicht geändert werden und es gibt immer Risiken, die mit einem solchen Angriff verbunden sind. Selbst mit 51% der Hash-Power kann der Angreifer weder neue Bitcoins aus dem Nichts erschaffen, noch die Blockbelohnungen oder Transaktionen anderer Teilnehmer ändern. Obwohl der Angreifer entscheiden kann, welche Transaktionen in die Blöcke aufgenommen werden, können die anderen Teilnehmer nicht gezwungen werden, seiner Kette zu folgen. Wenn sich die anderen Teilnehmer dem Angriff aktiv widersetzen, können sie ihn neutralisieren, indem sie den ersten Block der böartigen Kette für falsch erklären und damit alle nachfolgenden Blöcke ungültig machen. Letztendlich ermöglicht ein 51%-Angriff dem Angreifer doppelte Ausgaben und die Zensur von Transaktionen, aber nicht die willkürliche Manipulation des gesamten Regelwerks des Netzwerks. Angreifer könnten einmalig einen Double Spend versuchen, würden aber dank der Transparenz der Blockchain letztlich doch entdeckt werden. ["51 Angriff", n. d.]

5.9.6 Wie kann man sich vor einem 51%-Angriff schützen?

Wie bereits erwähnt, ist ein erfolgreicher 51%-Angriff ein seltenes Ereignis. Nichtsdestotrotz kann es hilfreich sein, zu wissen, wie man es einem Angreifer so schwer wie möglich macht, um die Wahrscheinlichkeit eines erfolgreichen Angriffs weiter zu reduzieren. ["51 Angriff", n. d.]

Nach Erhalt einer Transaktion kann es hilfreich sein, einige Blöcke abzuwarten, um die Sicherheit zu erhöhen. In der Regel wird eine Transaktion mit etwa sechs Bestätigungen als sehr sicher angesehen, wenn es um Bitcoin geht. Die Anzahl der Bestätigungen, die

für Altcoins benötigt werden, hängt von der Hashrate des Netzwerks ab. [“51 Angriff”, n. d.]

Ein weiterer Ansatz besteht darin, einen eigenen Full Node zu betreiben, anstatt nur einen Thin Client zu verwenden. Thin Clients, die nicht die gesamte Blockchain speichern, sind anfälliger für den 51%-Angriff. Bei kleinen Beträgen ist der Betrieb eines eigenen Full Nodes jedoch möglicherweise nicht notwendig. Für höhere Beträge bietet der Einsatz eines eigenen Full Nodes jedoch zusätzliche Sicherheit.

5.10 Routing Angriff

Ein Routing-Angriff kann durch die Kompromittierung oder Kooperation eines Internet Service Providers (ISP) ermöglicht werden. Obwohl es technisch möglich ist, einen Bitcoin-Knoten (oder einen Knoten für andere Münzen) überall auf der Welt zu betreiben, ist es in der Realität so, dass die Knoten relativ zentralisiert sind, was die ISPs betrifft, die den Internetverkehr von und zu ihnen leiten. Laut einer Untersuchung der ETH Zürich werden 30 Prozent des Bitcoin-Netzwerks von 13 ISPs gehostet, während 60 Prozent des gesamten Transaktionsverkehrs des Netzwerks von drei ISPs geleitet werden. Wenn ein ISP kompromittiert ist, wird er zu einem wichtigen Ausfallpunkt. Ein Routing-Angriff wird ausgeführt, indem der Internetverkehr zwischen autonomen Systemen abgefangen wird, bei denen es sich um Knoten der obersten Ebene in der Architektur des Internets handelt, die relativ leicht abgefangen werden können. Dies ist im Internet weit verbreitet und kann gegen Bitcoin oder anderen Kryptowährungsverkehr eingesetzt werden. Diese Methode kann ein Kryptowährungsnetzwerk in zwei oder mehr getrennte Netzwerke aufteilen, wodurch beide Seiten der Partition Angriffen mit doppelten Ausgaben ausgesetzt sind, da sie nicht mit dem gesamten Netzwerk kommunizieren können, um Transaktionen zu validieren. Sobald Münzen auf einer Seite des Netzwerks ausgegeben und Waren oder Dienstleistungen empfangen werden, kann die Partition entfernt werden, und die Seite des Netzwerks mit der kürzeren Kette würde vom gesamten Netzwerk zurückgewiesen werden, und diese Transaktionen würden ausgelöscht. Soweit wir wissen, ist diese Art von Angriff noch nicht vorgekommen, und es gibt Maßnahmen, die Münzen gegen dieses Verhalten immun machen können.[“Cybersecurity Makes me Wanna Cry”, 2022]

6 Schluss

Zusammenfassend lässt sich sagen, dass Bitcoin und andere Kryptowährungen durch den Einsatz des Konsensmechanismus "Proof-of-Work" validierte Transaktionen ermöglichen. Dieser Prozess erfordert starke Hardware-Ressourcen und kann durch das Mining von Belohnungen begleitet sein. Das Blockchain-Netzwerk spielt eine wichtige Rolle bei der Überprüfung der Gültigkeit von Transaktionen und der Aufrechterhaltung der Integrität des Systems. Vor dem Investieren in Bitcoin oder eine andere Kryptowährung ist es wichtig, sich über den Markt und die verschiedenen Optionen gründlich zu informieren und das Risiko sorgfältig abzuwägen.

Die Perspektiven für Proof-Of-Work und andere Konsensmechanismen in der Kryptowährungswelt sind derzeit ungewiss. Proof-Of-Work ist derzeit der am weitesten verbreitete Konsensmechanismus und wird von vielen Kryptowährungen wie Bitcoin und Ethereum verwendet, aber es hat auch einige Nachteile, wie hohe Energiekosten und langsame Transaktionsgeschwindigkeiten, die zu einer eingeschränkten Skalierbarkeit führen.

Es gibt auch andere Konsensmechanismen, wie Proof-Of-Stake, die derzeit entwickelt werden und möglicherweise eine Alternative zu Proof-Of-Work darstellen könnten. Proof-Of-Stake erfordert von Teilnehmern, eine bestimmte Menge an Kryptowährung zu "staken", um als Miner zu fungieren, was zu reduzierten Energiekosten führen könnte. Es gibt jedoch noch Fragen hinsichtlich der Sicherheit von Proof-Of-Stake und ob es die gleiche Sicherheit wie Proof-Of-Work gewährleisten kann.

Es ist unmöglich vorherzusagen, welcher Konsensmechanismus in Zukunft dominieren wird. Es ist jedoch wichtig, dass Kryptowährungen kontinuierlich verbessert werden, um Skalierbarkeit und Sicherheit zu verbessern. Es ist auch wahrscheinlich, dass es in der Zukunft weitere neue Konsensmechanismen geben wird, die die Landschaft der Kryptowährung verändern könnten. Eines dieser Konsensmechanismen, das zunehmend in den Fokus gerät, ist Proof-Of-Authority. Dieser Mechanismus basiert auf einem Netzwerk von autorisierten Validatoren, die Transaktionen bestätigen und das Netzwerk sicher halten. Proof-Of-Authority könnte eine günstigere und schnellere Alternative zu Proof-Of-Work darstellen, aber es gibt auch Bedenken bezüglich der Zentralisierung und der möglichen Einflussnahme von Validatoren. Es ist wichtig, dass die Entwickler weiter an neuen und verbesserten Mechanismen arbeiten, um die Effizienz und Sicherheit von Kryptowährungen zu gewährleisten. Investoren sollten sich über die verschiedenen Konsensmechanismen informieren und Risiken sorgfältig abwägen, bevor sie in Kryptowährungen investieren.

Literatur

- 51 Angriff. (n. d.). <https://www.btc-echo.de/academy/bibliothek/51-attacke/>
- Academy, B.-E. (2021). Proof-of-Work: Definition, Funktion, Sicherheit. <https://www.btc-echo.de/academy/bibliothek/proof-of-work/>
- Blockchain [Accessed on 2022-12-30]. (2022). <https://en.wikipedia.org/wiki/Blockchain>
- Blockchain - Wikipedia. (2022). Verfügbar 30. Dezember 2022 unter <https://de.wikipedia.org/wiki/Blockchain>
- Chapter247Infotech. (n. d.). Blockchain Technology Use Cases in 2022. Verfügbar 30. Dezember 2022 unter <https://www.iotforall.com/blockchain-use-cases-in-2022>
- Cybersecurity Makes me Wanna Cry. (2022). <https://coincentral.com/blockchain-hacks/>
- Double Spending. (n. d.). <https://www.btc-echo.de/academy/bibliothek/double-spending/>
- Fool, T. M. (2022). Proof of Work: What It Is and How It's Used in Cryptocurrency. <https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/proof-of-work/>
- Insider, B. (2022). What is proof of work? <https://www.businessinsider.com/personal-finance/proof-of-work>
- Proof of work [Accessed on 2022-12-30]. (2022). https://en.wikipedia.org/wiki/Proof_of_work
- Sidechain. (2022). <https://www.coindesk.com/learn/an-introduction-to-sidechains/>
- Sybil Attack. (2022). <https://www.imperva.com/learn/application-security/sybil-attack/>