

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

31. Dezember 2022

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	6
2	Einführung in die Blockchain	7
2.1	Blockchain Definition	7
2.2	Konstruktion des Blocks	8
2.3	Blockchaining-Mechanismus	9
3	Theoretische Seite der Proof-Of-Work-Methode	10
3.1	Was ist Proof-Of-Work ?	10
3.2	Wie funktioniert Proof of Work bei einer Blockchain ?	10
3.3	Wie genau funktionieren die Proof-of-Work-Berechnungen?	13
3.4	Was hat es mit der Schwierigkeit auf sich ?	13
3.5	Sicherheit des Proof-Of-Work	14
3.6	Vor- und Nachteile von Proof-Of-Work	14
4	Praktische Anwendung der Proof-Of-Work-Methode	18
5	Der Bitcoin-Markt und die Verwendung von Proof of Work	21
5.1	Kryptowährungen, auf die Proof-Of-Work basieren	21
5.2	Wie kann ich mit Kryptowährung Geld verdienen ?	23
5.2.1	Kryptowährungen und ihre produktive Seite: Eine Untersuchung des Krypto-Minings	23
5.2.2	Wo sollte ich mein Geld in Kryptowährungen investieren?	28
6	Schluss	29

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

2.2 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

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

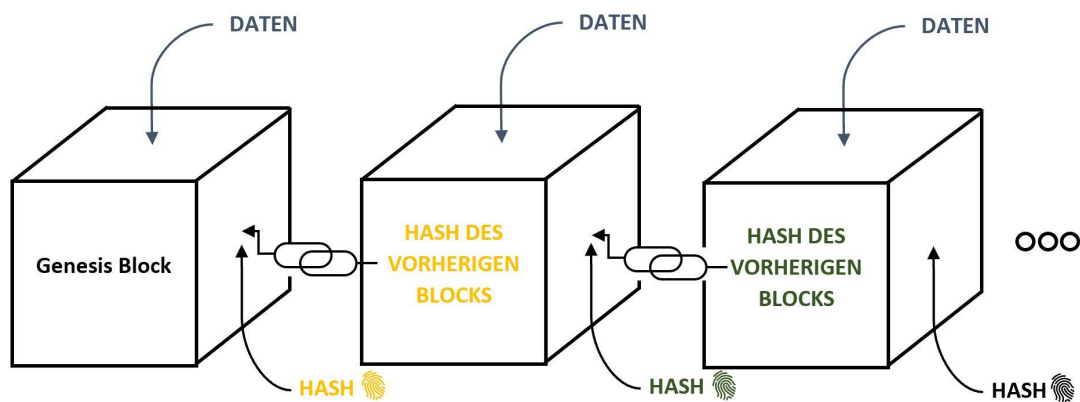


Abbildung 2.2: Der erste Block der Kette wird als Genesis-Block bezeichnet.

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

In solchen Fällen sollte man immer bedenken, welche Handlungen von verdächtigen Personen ausgehen könnten, beispielsweise das Modifizieren oder Manipulieren der Daten im Block (i). Dies führt zu einer Änderung des tatsächlichen Blocks i und macht den vorherigen Hash im Block (i+1) ungültig. Dies bedeutet, dass das Ändern eines Blocks alle darauf folgenden Blöcke in der Blockchain ungültig macht, was die Integrität der Kette beweist.

Achtung : Ist dieser Mechanismus gesichert?

Der Einsatz von Hashes allein reicht nicht aus, um Manipulationen zu verhindern. Da Computer heutzutage sehr schnell sind und Tausende von Hashes berechnen können, besteht technisch gesehen die Möglichkeit, einen Block zu manipulieren und alle nachfolgenden Hashes der nachfolgenden Blöcke erneut zu berechnen, um das Blockchain-Netzwerk wieder gültig zu machen. Aus diesem Grund verwendet die Blockchain den sogenannten "Proof of Work (POW)", um dieses Problem zu vermeiden.

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

3.1 Was ist Proof-Of-Work ?

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 Angriffen 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 Coins in einem Proof-of-Work-System einen tatsächlichen Einsatz von Ressourcen. Dadurch wird ein fairer Mechanismus für die Verteilung von Coins gewährleistet. Academy, 2021

3.2 Wie funktioniert Proof of Work bei einer Blockchain ?

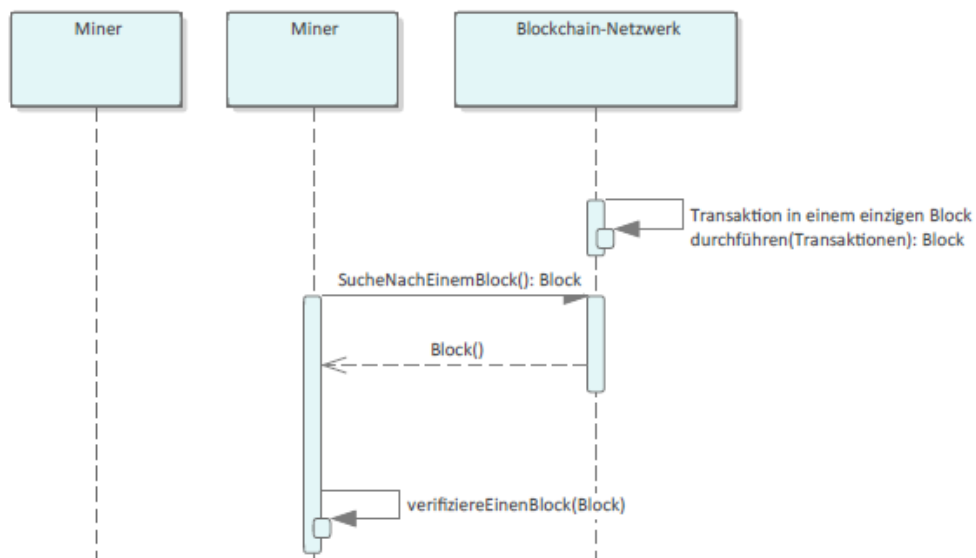
Der Proof-of-Work-Mechanismus erfordert, dass Miner mithilfe von Brute-force-Methoden versuchen, eine Nonce zu finden, die bestimmte Eigenschaften aufweist, wodurch Milliarden von Berechnungen durchgeführt werden. Sobald ein solches Ergebnis erzielt wurde,

wird den Minern eine Belohnung in Form einer Blocksubvention gewährt. Dieser Prozess wird als Mining bezeichnet.

Diese beschreiben den Prozess einer Transaktion im Blockchain-Netzwerk.

- Die Blockchain generiert einen Block, der alle Transaktionen enthält, die in einem bestimmten Zeitraum stattgefunden haben.
- Der Verifizierer wird die Integrität der Transaktionen überprüfen, um sicherzustellen, dass sie legitim sind. Academy, 2021
- Die Miner im Netzwerk überprüfen dann die Legitimität dieser Transaktionen und führen anschließend eine Suche durch, indem sie die Nonce erraten. Der erfolgreiche Miner, der als erstes die Lösung findet, wird mit einer Belohnung und den Transaktionsgebühren belohnt. Dieser Prozess wird als "Mining" bezeichnet. Das Blockchain-Netzwerk wird dann um den Block mit den bestätigten Transaktionen erweitert und wird als Teil der Kette von Blöcken gespeichert. Academy, 2021
- Die Transaktionsbestätigung im Blockchain-Netzwerk wird wiederholt

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





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

- Die Miner im Blockchain-Netzwerk nutzen Hash-Funktionen, die in ihrer Funktionsweise unumkehrbar sind. Sie können eine beliebig lange Zeichenfolge in eine eindeutige Zeichenfolge festgelegter Länge umwandeln. Die Schwierigkeit besteht darin, ein Ergebnis zu erzielen, das bestimmte Eigenschaften aufweist, die sich aus der Verwendung der Hash-Funktion ergeben. Ein bekanntes Beispiel hierfür ist der Einsatz der SHA-256-Hash-Funktion im Bereich des Minings bei Bitcoin. Academy, 2021
- Die Hash-Funktion ist eine eindeutige, nicht invertierbare mathematische Funktion, die aus einer beliebigen Eingabestring eine feste Länge erzeugt. Sie wird häufig in der Kryptographie und im Blockchain-Bereich verwendet. Im Fall von Kryptowährungen wie Bitcoin wird sie beim Mining verwendet, wobei Miner versuchen, einen Wert mit bestimmten Eigenschaften zu finden, indem sie der Hash-Funktion Zeichenfolgen übergeben. Da die Rückgängigmachung der Hash-Funktion nicht möglich ist, kann der Miner den erhaltenen Wert nicht einfach umkehren und die Eingabe der Hash-Funktion erhalten. Fool, 2022, Academy, 2021
- Aus diesem Grund gibt es das Konzept **"Mining"**, Mining ist ein Prozess, bei dem Miner versuchen, die Nonce und die Reihenfolge der 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 von Operationen durchführen, um den Wert der Eingabe für die Hash-Funktion zu ermitteln. Dies geschieht durch das Konzept des Minings, bei dem Miner versuchen, die Nonce und die Reihenfolge jedes Parameters, die von der Hash-Funktion als Eingabe akzeptiert werden, zu erraten.
- Wenn der Block abgebaut wird, überprüfen alle Teilnehmer des Blockchain-Netzwerks die präsentierte Lösung, um zu bestätigen, dass die Gültigkeit der Blockchain aufrechterhalten wird. Academy, 2021

3.4 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

3.5 Sicherheit des Proof-Of-Work

- Der Proof-of-Work ist eine Technik, die in vielen Kryptowährungen eingesetzt wird, um Transaktionen zu verifizieren und neue Blöcke in die Blockchain einzufügen. Miner müssen dabei bestimmte Berechnungen durchführen, um einen neuen Block zu abbauen und somit eine Belohnung zu erhalten.
- Der Proof-of-Work bietet eine gewisse Sicherheit, da es für Angreifer schwierig ist, die Blockchain zu verändern, ohne die erforderliche Rechenleistung zu erbringen. Allerdings gibt es auch Nachteile, wie hohe Energiekosten und langsamere Transaktionsgeschwindigkeiten im Vergleich zu anderen Konsensmechanismen.

3.6 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 Sicherheitsniveau in einem auf Proof-of-Work basierenden Blockchain-Netzwerk zu gewährleisten, müsste eine spekulative Person die Kontrolle über die Mehrheit der Mining-Kapazität erlangen. Dies würde bedeuten, dass sie mindestens 50% des Netzwerks besitzen müsste, was aufgrund der verteilten Natur von Proof-of-Work-Systemen als unmöglich gilt. Eine solche Person benötigte auch eine beträchtliche Menge an Hardware und Energie, um in der Lage zu sein, die benötigte Rechenleistung zu erbringen.
 - Ein "51%-Angriff" stellt eine Sicherheitsmaßnahme dar, die verhindern soll, dass eine spekulative Person die Kontrolle über ein auf Proof-of-Work basierendes Blockchain-Netzwerk übernimmt. Um ein solcher Angriff zu verhindern, müsste die Person mindestens 50% der Mining-Kapazität besitzen, was aufgrund der dezentralisierten Natur von Proof-of-Work-Systemen als unmöglich gilt.

- Es gibt jedoch auch andere Faktoren, die die Sicherheit von Proof-of-Work-Systemen beeinflussen. Dazu gehören die Größe und Zentralisierung von Mining-Pools, die Sicherheit von Hardware und die Implementierung des Konsensmechanismus. Um das Sicherheitsniveau eines Proof-of-Work-Systems vollständig zu verstehen, ist es wichtig, diese Faktoren zu berücksichtigen.

- **Gute Anreizstruktur :**

- Eine gut ausgelegte Anreizstruktur ist ein wesentlicher Faktor für den Erfolg eines Proof-of-Work-Systems. Miner erhalten eine finanzielle Belohnung für das Lösen von Rechenaufgaben und die damit verbundenen Bemühungen, die als Anreiz dienen, ihre Rechenleistung bereitzustellen und somit die Integrität und Sicherheit der Blockchain zu gewährleisten.
- Eine gute Anreizstruktur kann auch dazu beitragen, das Gleichgewicht des Systems aufrechtzuerhalten und die Beteiligung von Miner zu fördern. Wenn die Belohnungen für das Mining zu gering sind, könnten Miner weniger motiviert sein, ihre Rechenleistung zur Verfügung zu stellen, was zu einer Beeinträchtigung der Sicherheit führen könnte. Auf der anderen Seite könnten zu hohe Belohnungen dazu führen, dass das System unausgeglichene wird und es zu einer Zentralisierung von Mining-Pools kommt.
- Es ist wichtig, dass die Anreizstruktur von Proof-of-Work-Systemen sorgfältig abgestimmt ist, um eine ausgeglichene Beteiligung von Miner und ein hohes Sicherheitsniveau zu gewährleisten.

- **Verteilte Konsensfindung :** Die dezentralisierte Konsensbildung ist ein wichtiger Aspekt von Blockchain-Systemen, die nicht von einer zentralen Stelle kontrolliert werden, wie dem Proof-of-Work. Bei diesem Verfahren werden Transaktionen von allen Teilnehmern des Netzwerks überprüft, anstatt von einer zentralen Institution wie einer Bank oder Regierung.

- **Belohnung** Viele Menschen schätzen Bitcoin aufgrund der Möglichkeit, an der Mining-Operation teilzunehmen. Dazu können sie spezielle Hardware, sogenannte "Rig MiningGeräte, einrichten und damit mit dem Abbau von Bitcoin beginnen. Für jeden erfolgreichen Abbauvorgang erhalten sie eine Belohnung in Form von Bitcoin. Die Möglichkeit, an der Mining-Operation teilzunehmen, macht Bitcoin für viele Menschen attraktiv und gibt ihnen die Möglichkeit, daran zu verdienen. Es ist jedoch wichtig zu beachten, dass das Mining von Bitcoin auch mit hohen Energiekosten und möglichen technischen Herausforderungen verbunden ist.

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

- Transaktionen sind so langsam, weil sie eine Menge von Mining-Operationen benötigen, um einen Block zu überprüfen, der Bitcoin-Transaktionen enthält, auch Blockchain Durchschnitt der Suche nach einem Block nonce ist 1 Nonce pro 10 Minuten, die es so langsam für einen großen Market ist.
- **Hohe Energiekosten :**
 - Der Betrieb eines auf Proof-of-Work basierenden Blockchain-Netzwerks kann mit hohem Energiebedarf verbunden sein, da Miner Rechenleistung bereitstellen müssen, um neue Blöcke zu erstellen und Transaktionen zu validieren. Dies erfordert häufig die Verwendung von spezialisierten Mining-Geräten, die viel Strom verbrauchen und möglicherweise auch Kühlsysteme benötigen, um hohe Temperaturen zu vermeiden.
 - Eine Möglichkeit, den Energiebedarf von Mining-Operationen zu reduzieren, besteht darin, erneuerbare Energien zu nutzen, um den benötigten Strom zu erzeugen. Dies kann zwar höhere Anfangsinvestitionen erfordern, aber es bietet auch langfristige Vorteile, da Mining-Unternehmen keinen externen Strom verbrauchen und somit keine Energiekosten haben. Erneuerbare Energien wie Solar- und Windenergie können eine umweltfreundliche Alternative zu fossilen Brennstoffen darstellen und können dazu beitragen, den CO₂-Ausstoß von Mining-Operationen zu reduzieren.
 - Es ist wichtig, den Energiebedarf von Mining-Operationen sorgfältig zu berücksichtigen, um sicherzustellen, dass sie nachhaltig und umweltfreundlich sind. Wenn zu viele Miner ohne Rücksicht auf den Energieverbrauch minen, könnten die Energiepreise steigen und die Umwelt belasten. Daher ist es wichtig, dass Miner ihren Energieverbrauch sorgfältig planen und, falls möglich, erneuerbare Energien nutzen.
- **Langsame Transaktionsgeschwindigkeiten :**
 - Eines der Haupthindernisse für die Schnelligkeit von Bitcoin-Transaktionen ist die Tatsache, dass sie von Minern validiert werden müssen, um in die Blockchain aufgenommen zu werden. Dies erfordert, dass Miner bestimmte Rechenaufgaben lösen, um einen neuen Block zu erstellen, der die Transaktionen enthält. Da die Schwierigkeit, einen neuen Block zu finden, von Zeit zu Zeit angepasst wird, kann es durchaus eine Weile dauern, bis ein Block gefunden wird.
 - Die durchschnittliche Zeit, die benötigt wird, um einen neuen Block zu finden, beträgt derzeit etwa 10 Minuten. Dies bedeutet, dass es in der Regel etwa 10 Minuten dauern wird, bis eine Transaktion bestätigt wird und in die Blockchain aufgenommen wird. Für einige Benutzer könnte dies als langsam empfunden werden, insbesondere im Vergleich zu traditionellen Zahlungsmethoden.
 - Es gibt jedoch auch Maßnahmen, die getroffen werden können, um die Schnelligkeit von Bitcoin-Transaktionen zu verbessern, wie zum Beispiel die Verwen-

dung von Segregated Witness (SegWit) oder Lightning-Netzwerken. Diese Technologien können die Größe von Transaktionen reduzieren und somit die 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 3.1: Die heutige Schwierigkeit ist
URL : https://www.blockchain.com/explorer/api/blockchain_api

- **Hardware-Anforderungen :**

- Das Abbauen von Bitcoin kann hohe Investitionskosten erfordern, da es oft notwendig ist, spezielle Mining-Hardware wie leistungsstarke Grafikkarten und entsprechende Motherboards zu beschaffen, um erfolgreich neue Blöcke zu erstellen. Die hohen Preise für diese Ausrüstung können es schwierig machen, in das Bitcoin-Mining einzusteigen, insbesondere für Einzelpersonen oder kleine Unternehmen.
- Trotzdem kann das Bitcoin-Mining dennoch lukrativ sein, insbesondere für größere Mining-Unternehmen mit mehreren Mining-Geräten und Zugang zu günstigem Strom. In diesen Fällen können die Einnahmen aus dem Mining die Investitionskosten schnell übersteigen und eine rentable Einkommensquelle darstellen.
- Es ist wichtig zu beachten, dass das Bitcoin-Mining auch ein hochvolatiles Unterfangen sein kann, da der Wert von Bitcoin und damit auch die Belohnungen für das Mining stark schwanken können. Daher ist es wichtig, sorgfältig zu planen und das Risiko sorgfältig abzuwägen, bevor man in das Bitcoin-Mining investiert.

4 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": "000000000000bae09a7a393a8acded75aa67e46cb81f7acaa5ad94f9eacd103",
  "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--"
  ]
}
```

Abbildung 4.1: 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": "b6f6991d03df0e2e04daffcd6bc418aac66049e2cd74b80f14ac86db1e3f0da",
  "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": "29d6a3540acfa0a950bef2bdc75cd51c24390fd",
      "script": "76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
    },
    {
      "value": "2000000",
      "hash": "17b5038a413f5c5ee288caa64cfab35a0c01914e",
      "script": "76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
    }
  ]
}
```

Abbildung 4.2: Die echten Blockchain-Block-Transaktionen.

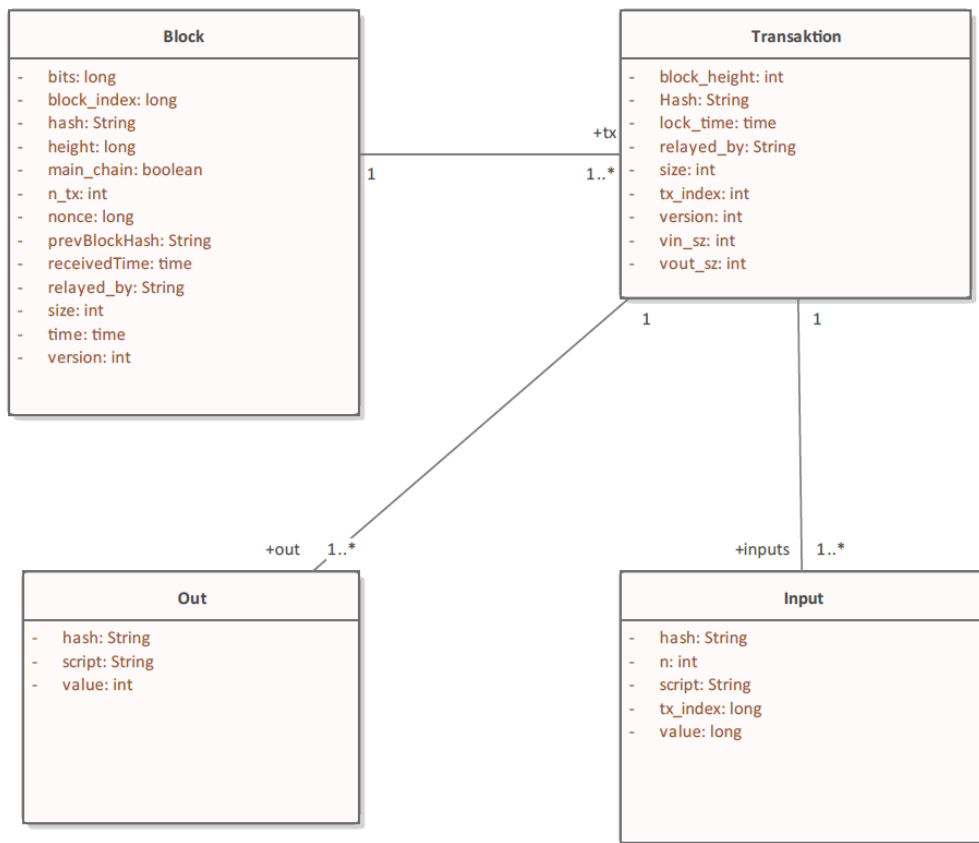


Abbildung 4.3: Das nächste Diagramm, das als Klassendiagramm bezeichnet wird, gibt eine visuelle Darstellung aller Daten, die im realen Blockchain-Netzwerk enthalten sind. Dieses Diagramm ist hilfreich, um die Implementierung des Blockchain-Netzwerks besser zu verstehen und zu analysieren. Es zeigt die 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.

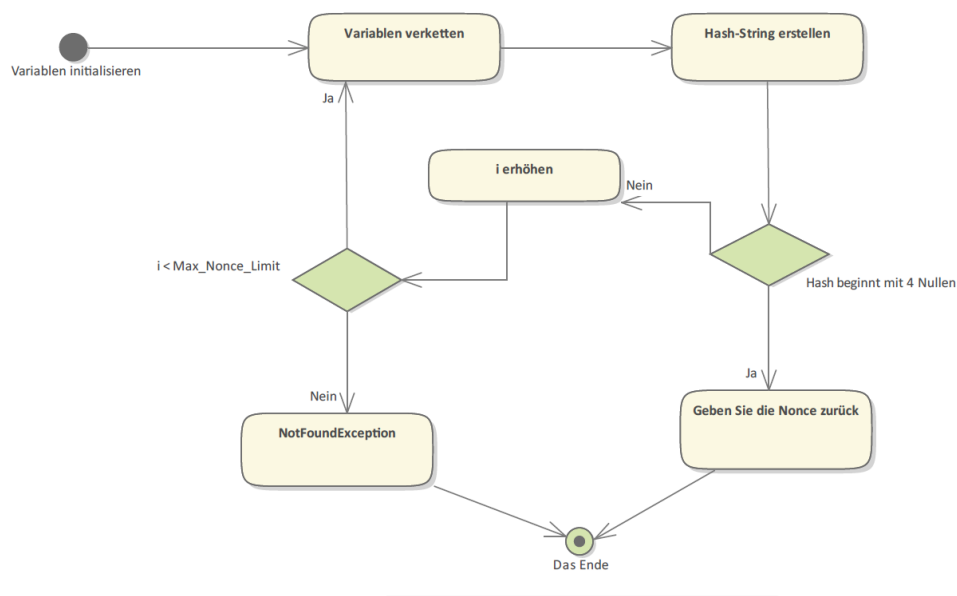


Abbildung 4.4: Der Algorithmus zur Bestimmung der Nonce wird mit dem Aktivitätsdiagramm erklärt. Zunächst müssen wir die initialen Daten initialisieren, einschließlich des `MaxNonceLimit`, der Anzahl der Nullen, die der Hash haben sollte. In diesem Beispiel betrachten wir die Anforderung, dass der Hash 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
  
```

5 Der Bitcoin-Markt und die Verwendung von Proof of Work

5.1 Kryptowährungen, auf die Proof-Of-Work basieren

Einige der bekanntesten Kryptowährungen, die den Konsensmechanismus Proof-Of-Work verwenden, sind Bitcoin, Bitcoin Cash, Bitcoin Sv, Litecoin und Dogecoin.



Abbildung 5.1: Bitcoin Cash

URL : https://upload.wikimedia.org/wikipedia/commons/5/58/Bitcoin_Cash.png



Abbildung 5.2: Bitcoin SV

URL : <https://upload.wikimedia.org/wikipedia/commons/c/c1/Bsv-icon-small.png>



Abbildung 5.3: Litecoin

URL : <https://www.creativefabrica.com/wp-content/uploads/2021/06/16/Cryptocurrency-Litecoin-Logo-Graphics-13458855-1.jpg>



Abbildung 5.4: Dogecoin

URL : <https://block-builders.de/wp-content/uploads/2021/01/ony3qesa3ebx-1024x1024.png>



Abbildung 5.5: Bitcoin Gold

URL : <https://s2.coinmarketcap.com/static/img/coins/200x200/2083.png>

Es gibt auch viele andere Kryptowährungen, die nicht auf Bitcoin basieren, aber die Proof-of-Work-Methode verwenden :



Abbildung 5.6: Ethereum Classic

URL : <https://s2.coinmarketcap.com/static/img/coins/200x200/1321.png>



Abbildung 5.7: Monero

URL : <https://s2.coinmarketcap.com/static/img/coins/200x200/328.png>



Abbildung 5.8: Zcash

URL : <https://z.cash/wp-content/uploads/2018/10/zcash-logo-fullcolor-512sq.png>



Abbildung 5.9: Kadena

URL : <https://s2.coinmarketcap.com/static/img/coins/200x200/5647.png>

5.2 Wie kann ich mit Kryptowährung Geld verdienen ?

5.2.1 Kryptowährungen und ihre produktive Seite: Eine Untersuchung des Krypto-Minings

Konzept

Der aktuelle Marktwert von Bitcoin im Jahr 2022 liegt bei 15.891 Euro pro Einheit. Dies stellt einen hohen Preis für diese Kryptowährung dar und könnte für manche Personen oder Unternehmen von Interesse sein, die in das Mining von Bitcoin einsteigen möchten. Es ist jedoch wichtig zu beachten, dass das Bitcoin-Mining eine volatilen und riskanten Aktivität sein kann und gründliche Recherche und Planung erfordert, um erfolgreich zu sein.

Ein Krypto-Mining-Rig ist ein spezielles Computersystem, das für das Mining von Kryptowährungen wie Bitcoin entwickelt wurde. Ein solches Rig besteht in der Regel aus einer Vielzahl von Computerkomponenten wie CPUs, GPUs, Motherboards, RAM und Speicher, die zusammengefügt werden, um eine möglichst hohe Rechenleistung zu erreichen.

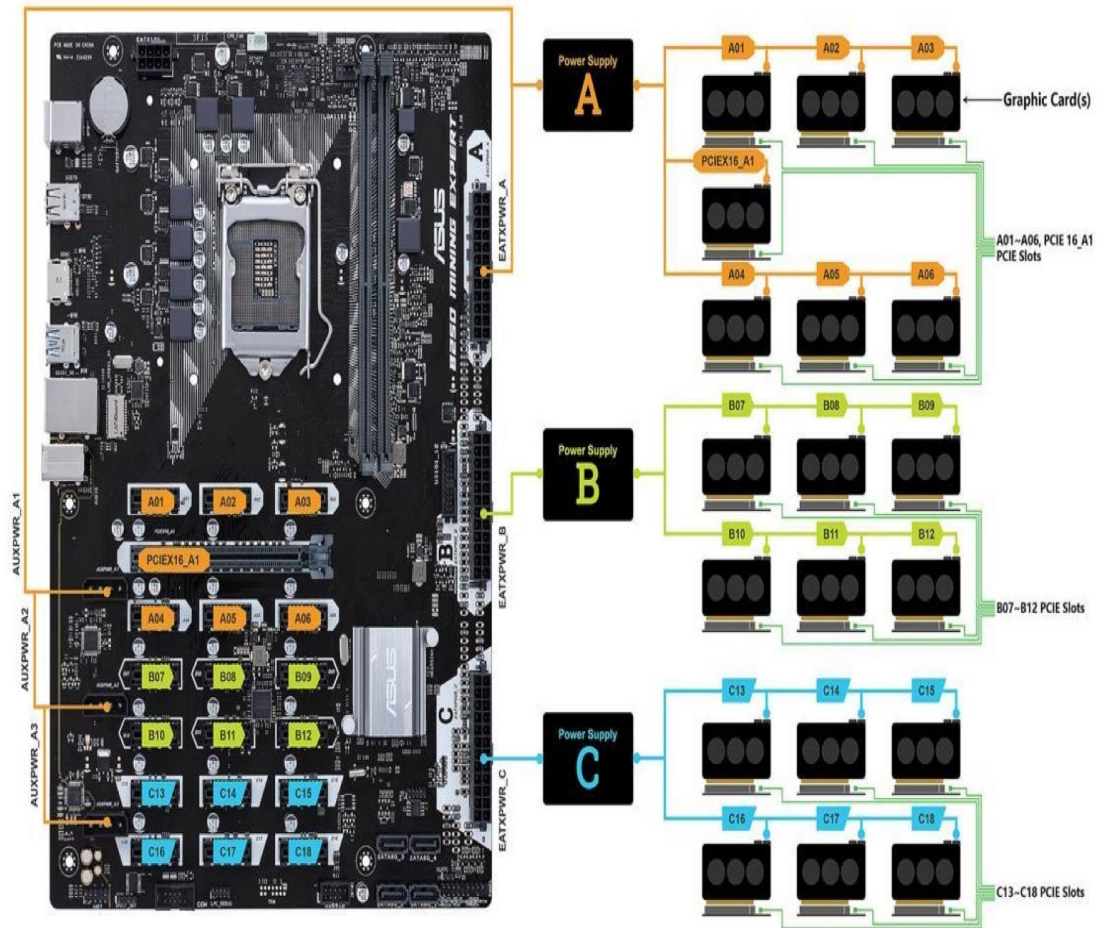
Um ein erfolgreiches Krypto-Mining-Rig aufzubauen, ist es wichtig, eine geeignete Hardware auszuwählen, die leistungsfähig genug ist, um die erforderlichen Rechenaufgaben zu lösen, aber auch effizient genug, um die Energiekosten zu minimieren. Dazu gehört auch die Auswahl von Kühlsystemen, um die Hitzeentwicklung zu minimieren und die Lebensdauer der Hardware zu verlängern.

Ein Krypto-Mining-Rig ist ein spezieller Computer, der für das Mining von Kryptowährungen entwickelt wurde. Die Hardware, die für ein solches Rig benötigt wird, umfasst in der Regel eine leistungsstarke Hauptplatine, die mehrere Grafikkarten unterstützt, sowie eine robuste Stromversorgung, um die benötigte Rechenleistung zu gewährleisten. Es ist wichtig, dass das Rig über ausreichende Kapazitäten verfügt, um die hohen Anforderungen des Krypto-Minings erfüllen zu können, insbesondere bei hoher Konkurrenz und entsprechender Schwierigkeit.

Es ist von größter Bedeutung, dass man sich über die aktuellen Marktbedingungen und den Wert der Kryptowährungen informiert, in die investiert wird, um sicherzustellen, dass man das bestmögliche Preis-Leistungs-Verhältnis bei der Hardware-Auswahl erhält und das Rig weiterhin wirtschaftlich rentabel bleibt. ZDNet, 2022

Hardware

Motherboard : Asus B250 Mining Expert



Das Motherboard, das in der Lage ist, 19 angeschlossene Grafikkarten zu verarbeiten, stellt eine leistungsstarke Hardware dar, die für das Krypto-Mining von Nutzen sein kann. Das Unternehmen Asus hat empfohlene GPU-Layouts für dieses Motherboard veröffentlicht, die für 19, 13 und 11 Grafikkarten vorsehen. Es kann jedoch auch mit anderen Layouts umgehen, obwohl es empfehlenswert ist, sich an den von Asus vorgeschlagenen Layouts zu orientieren, um optimale Leistung zu erzielen. ZDNet, 2022

CPU : Intel Core i5-6500



Die Hauptprozessoreinheit, auch als CPU bezeichnet, wird auch für diese Einrichtung in Betracht gezogen, obwohl sie für das Mining an sich weniger von Bedeutung ist. Es ist jedoch wichtig, dass sie kompatibel mit dem Motherboard ist, um einen problemlosen Betrieb des Systems zu gewährleisten.

RAM : G.SKILL Aegis 16GB (2 x 8GB)



Für unsere Mining-Operationen ist es nicht notwendig, in einen enormen Vorrat an Arbeitsspeicher (RAM) zu investieren. Stattdessen reichen 16 GB DDR4-RAM aus, um unsere Ziele zu erreichen und den Betrieb unseres Unternehmens reibungslos zu gestalten. Es ist wichtig, sorgfältig abzuwägen, wie viel RAM benötigt wird, um unnötige Kosten zu vermeiden, ohne dabei die Leistungsfähigkeit des Systems

zu beeinträchtigen.

Storage : SanDisk SSD Plus 1TB



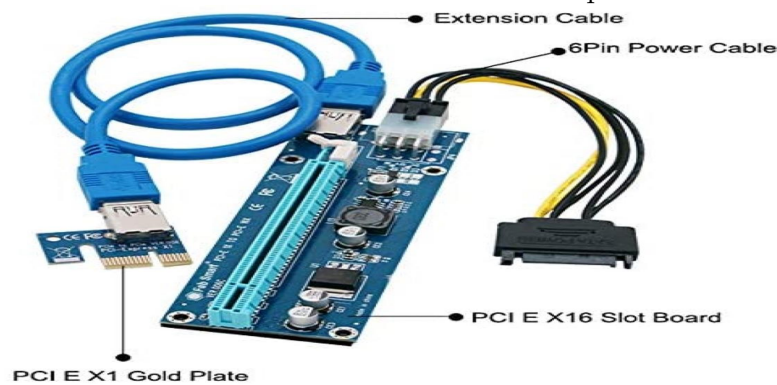
Die Verwendung von SSDs kann dazu beitragen, die Leistung des Mining-Rigs zu verbessern und den Betrieb zu beschleunigen. Es ist wichtig, sicherzustellen, dass die gewählten SSDs mit dem Motherboard kompatibel sind und genügend Speicherplatz für die Betriebsbedürfnisse des Unternehmens bereitstellen.

PSU : Segotep 850W Full-Modular PSU



Es kann von Vorteil sein, mehrere Segotep PSUs zu verwenden, um sicherzustellen, dass ausreichend Leistung für das Krypto-Mining-Rig bereitgestellt wird, insbesondere wenn es mehrere Grafikkarten enthält. Allerdings ist es wichtig zu beachten, dass der Einsatz von mehreren PSUs auch mit höheren Kosten verbunden sein kann. Eine gründliche Überlegung der Leistungsanforderungen des Mining-Rigs und der dafür benötigten Stromversorgung kann helfen, die richtige Anzahl an PSUs und die damit verbundenen Kosten zu bestimmen.

PCI-e Riser : FebSmart 16x to 1x Powered Riser 6-pack



Das Verwenden von powered risers ist eine wichtige Überlegung bei der Einrichtung eines Krypto-Mining-Rigs, da sie es ermöglichen, die Grafikkarten indirekt an das Motherboard anzuschließen. Sie bieten auch eine stabile Stromversorgung für die Grafikkarten, um eine zuverlässige Leistung zu gewährleisten. Es ist wichtig zu beachten, dass der Bedarf an powered risers abhängig ist von der Anzahl der installierten Grafikkarten und dass es möglicherweise notwendig sein kann, mehrere von ihnen zu verwenden, um eine optimale Leistung zu erzielen.

Nvidia graphics card : MSI Ventus 3X GeForce RTX 3090



Die Verwendung einer leistungsstarken Grafikkarte wie der beschriebenen ist für das Krypto-Mining von großer Bedeutung, da sie für die Verarbeitung von Rechenaufgaben und das Mining von Kryptowährungen verantwortlich ist. Diese spezifische Grafikkarte zeichnet sich durch ihre Fähigkeit zur Übertaktung, Stabilität und gute Kühlung aus. Sie ist auch bekannt für ihre Effizienz, was zu niedrigeren Stromkosten und reduzierten Bergbaukosten beitragen kann. Es ist wichtig, sich über die aktuellen Marktbedingungen und die Leistungsfähigkeit verschiedener Grafikkarten zu informieren, um die bestmögliche Wahl für das Krypto-Mining-Rig zu treffen.

5.2.2 Wo sollte ich mein Geld in Kryptowährungen investieren?

Es gibt einige Faktoren, die bei der Auswahl der nächsten erfolgreichen Kryptowährung berücksichtigt werden sollten. Dazu gehören die Skalierbarkeit der Blockchain, die Sicherheit der Technologie und die zugrunde liegende Idee, die von der Kryptowährung angegangen wird. Es ist auch wichtig, das Team hinter der Währung und ihre Erfolgsbilanz in der Vergangenheit zu betrachten. Es ist von großer Bedeutung, gründliche Recherchen durchzuführen und die damit verbundenen Risiken sorgfältig abzuwägen, bevor man in eine Kryptowährung investiert. Investopedia, 2022 SmartAsset, 2022

- **Der Preis spielt eine wichtige Rolle bei der Entscheidung.**

Erklärung : Eine wichtige Überlegung bei der Suche nach einer Kryptowährung ist der Preis des Tokens. Investoren, die nicht über ein großes Budget verfügen, können in Betracht ziehen, Kryptowährungen mit einem niedrigeren Preis zu erwerben. Es ist jedoch wichtig, dass Investoren gründliche Recherchen durchführen und Risiken sorgfältig abwägen, bevor sie in eine Kryptowährung investieren.

- **Es gibt gute Aussichten auf Annahme für die Kryptowährung, wenn sie von vielen Nutzern und Unternehmen akzeptiert wird.**

Erklärung : Eine Kryptowährung, die einen wettbewerbsfähigen Vorteil gegenüber anderen bietet und von vielen Nutzern und Unternehmen akzeptiert wird, bietet gute Aussichten für eine erfolgreiche Investition. Es ist wichtig, sorgfältig die Eigenschaften und die Akzeptanz der Kryptowährung zu überprüfen, bevor man das eigene Geld investiert.

- **Die Versorgung ist ein Faktor, den man bei der Auswahl einer Kryptowährung berücksichtigen sollte.**

Erklärung : Die Menge an Einheiten einer Kryptowährung, die momentan im Umlauf sind, wird als Versorgung bezeichnet. Eine geringere Versorgung könnte den Preis der Kryptowährung erhöhen, während eine höhere Versorgung möglicherweise dazu führt, dass der Preis sinkt. Bevor man in eine Kryptowährung investiert, ist es wichtig, sich über die Versorgung des Tokens zu informieren.

- **Preis und Volumen sind wichtig**

Erklärung : In 2022 gibt es viele Plattformen, die das Investieren in Kryptowährungen vereinfachen, indem sie die wechselhafte Geschichte der Kryptowährungen und die Preise über den Blockchain-Markt verfolgen. Es ist daher ratsam, den Markt sorgfältig zu scannen und eine informierte Entscheidung über die Investition in Kryptowährungen zu treffen. Es gibt auch künstliche intelligente Modelle, die auf alten Kryptowährungsdaten basieren und es erleichtern, vorherzusagen, ob der Preis einer Kryptowährung in Zukunft steigen oder fallen wird. Allerdings sollte beachtet werden, dass der Preis von Kryptowährungen volatil ist und es immer das Risiko von Verlusten gibt.

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

- 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>
- 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>
- Investopedia. (2022). How to Identify the Next Big Cryptocurrency. <https://www.investopedia.com/news/how-identify-next-big-cryptocurrency/>
- Proof of work [Accessed on 2022-12-30]. (2022). https://en.wikipedia.org/wiki/Proof_of_work
- SmartAsset. (2022). How to Invest in Cryptocurrency: A Beginner's Guide. <https://smartasset.com/investing/how-to-invest-in-cryptocurrency>
- ZDNet. (2022). How to build a crypto-mining rig. <https://www.zdnet.com/article/how-to-build-a-cryptomining-rig/>