

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

30. 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**

Dieser Bericht ist eine Seminararbeit für mein 5. Semester, ich möchte mich wirklich bei den Professoren bedanken, dass sie mir diese Arbeit gegeben haben. Es war wirklich mein erster Schritt, um mit der Blockchain-Entwicklung zu beginnen, in dem ich viele Informationen über Kryptowährungen und Blockchain-Netzwerke recherchiert habe, außerdem habe ich die Funktionsweise von Kryptowährungen basierend auf Proof-Of-Work verstanden. Dieser Bericht enthält eine Zusammenfassung aller Informationen über Blockchain, in technischer und theoretischer Hinsicht. Er beinhaltet auch die Investitionsmethode und das Gewinnen von Geld aus Bitcoin und anderen Kryptowährungen auf Basis von Proof-Of-Work.

## **Abstract in Englisch**

This report is a seminar work for my 5th semester, I really want to thank the professors for giving me this work. It was really my first step to start with blockchain development, in which I researched a lot of information about cryptocurrencies and blockchain networks, also I understood the working of cryptocurrencies based on Proof-Of-Work. This report contains a summary of all the information about Blockchain, in technical and theoretical aspects. It also includes the investment method and making money from Bitcoin and other cryptocurrencies based on Proof-Of-Work.

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>6</b>
<b>2</b>	<b>Einführung in die Blockchain</b>	<b>7</b>
2.1	Blockchain Definition . . . . .	7
2.2	Konstruktion des Blocks . . . . .	7
2.3	Blockchaining-Mechanismus . . . . .	9
<b>3</b>	<b>Theoretische Seite der Proof-Of-Work-Methode</b>	<b>10</b>
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 ? . . . . .	14
3.5	Algorithmus zum Finden einer Nonce . . . . .	14
3.6	Sicherheit des Proof-Of-Work . . . . .	18
3.7	Vor- und Nachteile von Proof-Of-Work . . . . .	19
<b>4</b>	<b>Der Bitcoin-Markt und die Verwendung von Proof of Work</b>	<b>23</b>
4.1	Münzen . . . . .	23
4.2	Wie kann ich mit Kryptowährung Geld verdienen ? . . . . .	25
4.2.1	Krypto-Mining . . . . .	25
4.3	Wo sollte ich mein Geld in Kryptowährungen investieren? . . . . .	30
<b>5</b>	<b>Schluss</b>	<b>31</b>

# 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.

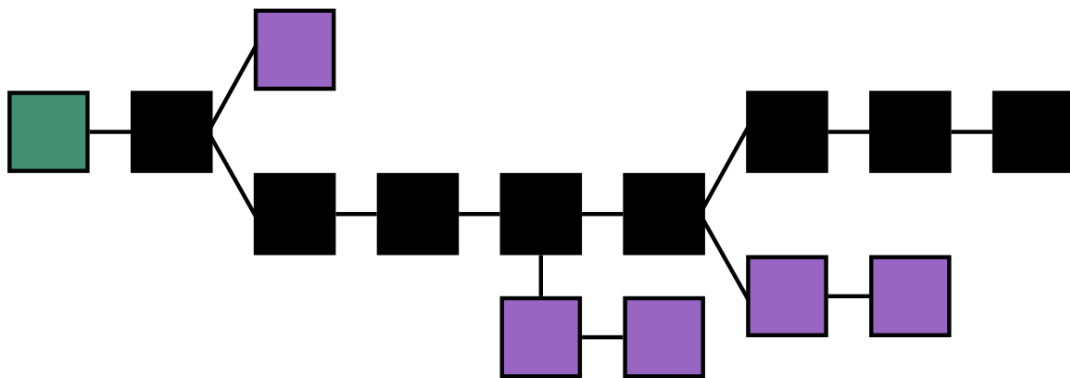
Ein Beispiel: Stellen Sie sich ein Transaktionsbanksystem vor, das von einem Server oder Systemadministrator verwaltet wird. Dies könnte die Wartung des Systems, das Verwalten, Löschen und Hinzufügen von Benutzer- oder Transaktionsinformationen zur Datenbank umfassen. Es könnte auch bedeuten, dass der 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.

## 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..

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.



### 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 ( $4 \times 8$  „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 ( $32 \times 8$  „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 ( $32 \times 8$  „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.

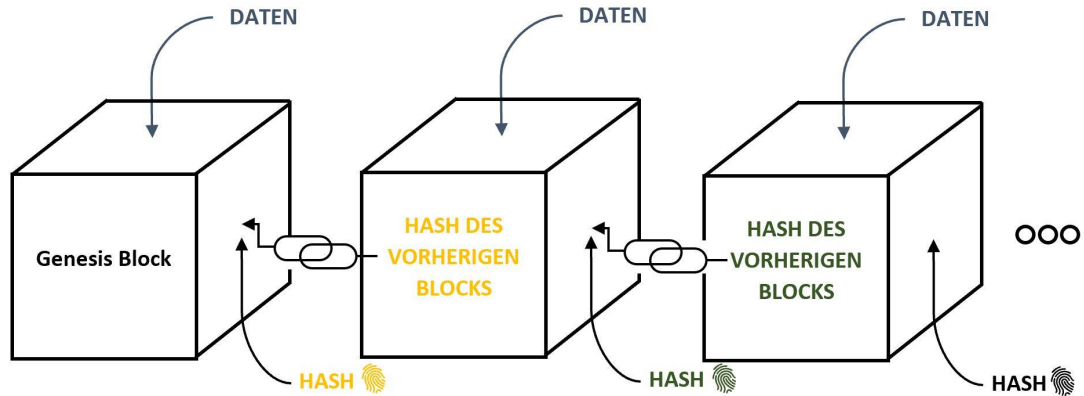
### Was sind Merkle-Bäume?

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.



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

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, 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.
- 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.

### 3.2 Wie funktioniert Proof of Work bei einer Blockchain ?

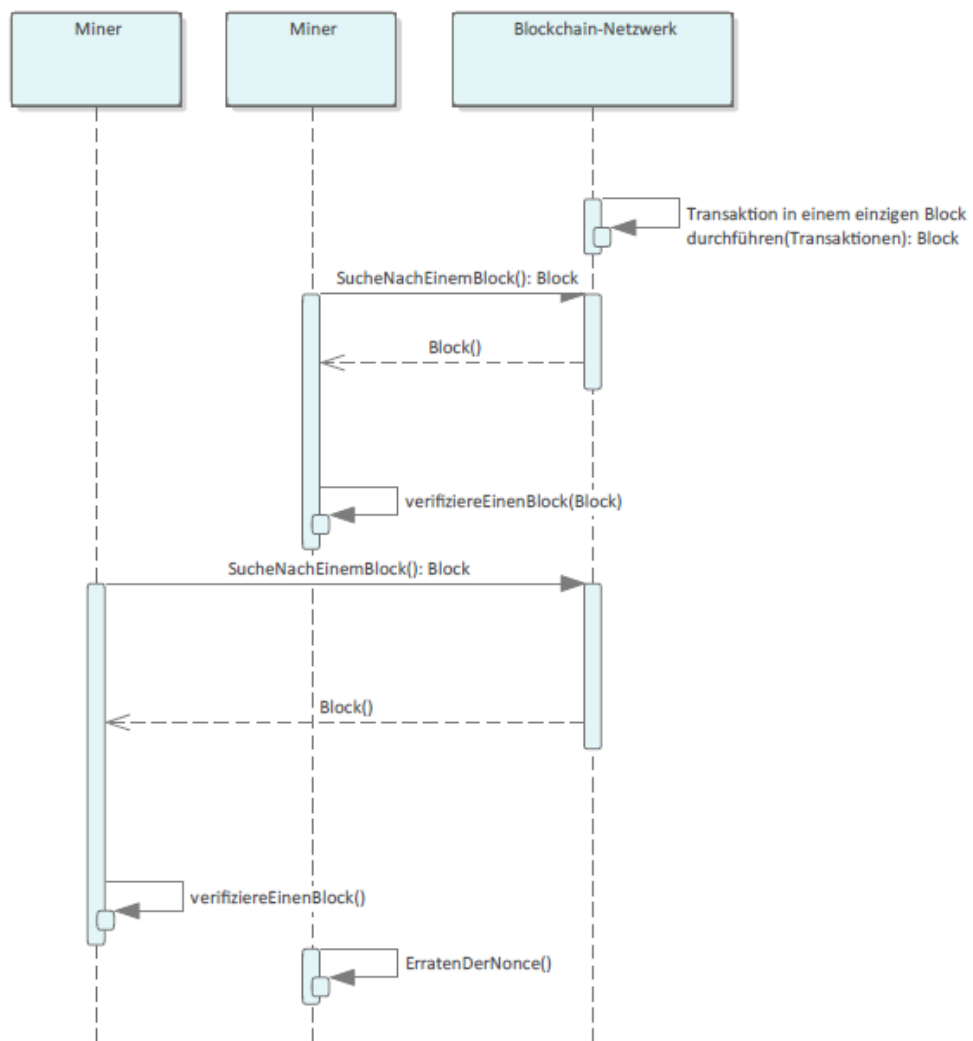
Der Proof-of-Work-Mechanismus erfordert, dass Miner mithilfe von Brute-force-Methoden versuchen, eine Nonce zu finden, die bestimmte Eigenschaften aufweist, wodurch Milliarden von Berechnungen durchgeführt werden. Sobald ein solches Ergebnis erzielt wurde,

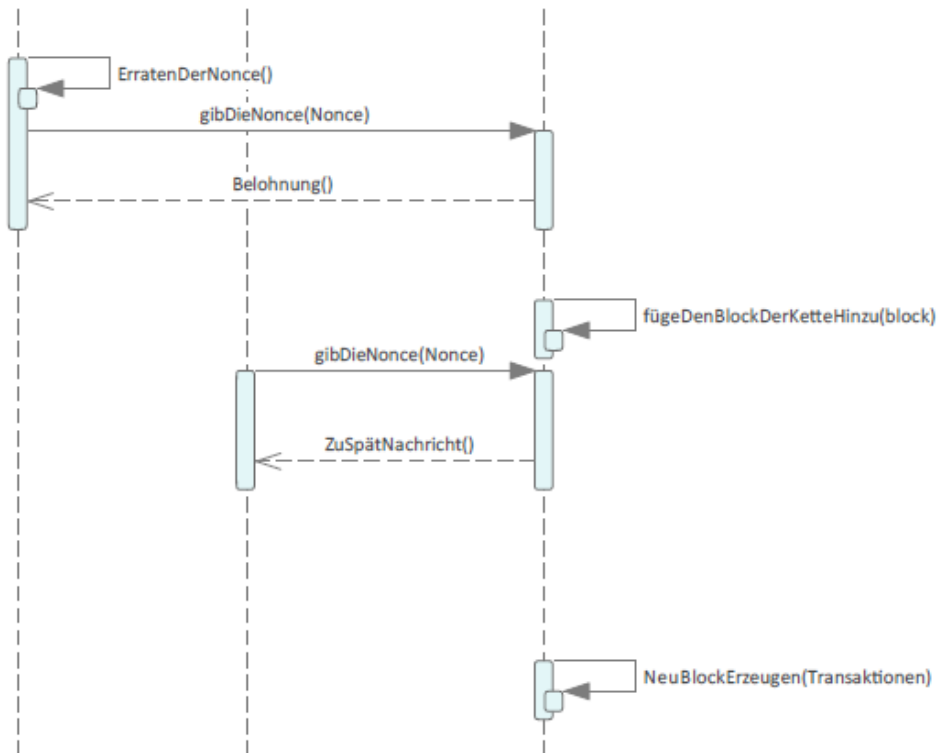
wird den Minern eine Belohnung in Form einer Blocksubvention gewährt. Dieser Prozess wird als Mining bezeichnet.

**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.
- 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.
- 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.
- 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.

- 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.

### 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.
- 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. (check it)

### 3.5 Algorithmus zum Finden einer Nonce

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

## 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": "935aa0ed2e29a4b81e0c995c39e06995ecce7ddbabb26ed32d550a72e8200bf5",
  "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--"
  ]
}
```

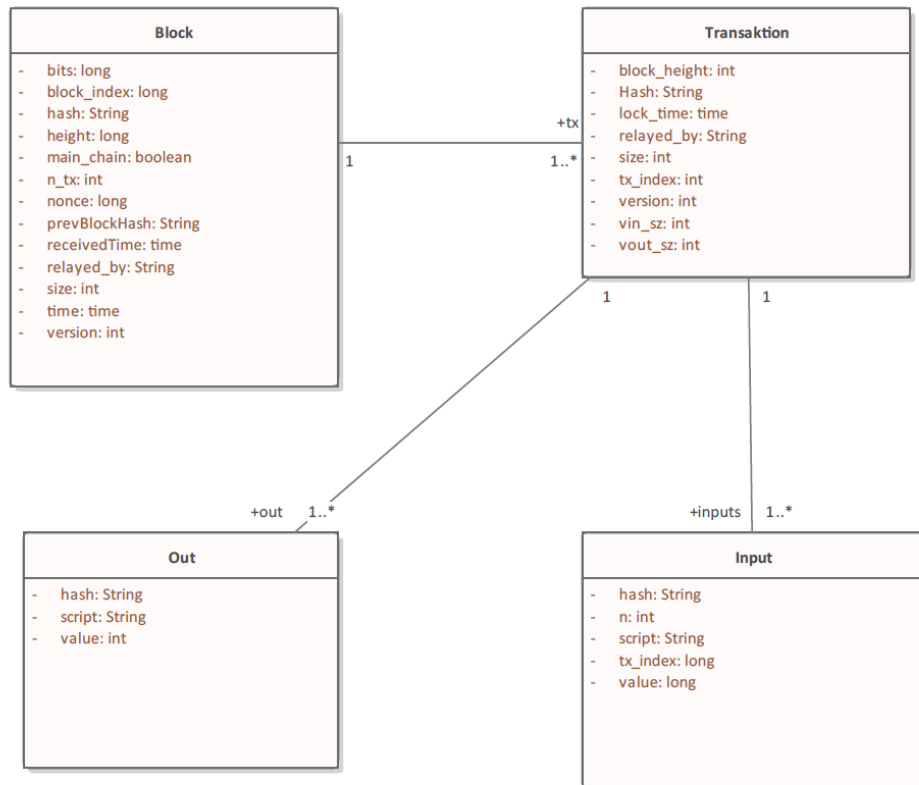
- Und dies ist eine echte Einzeltransaktionsstruktur

## 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

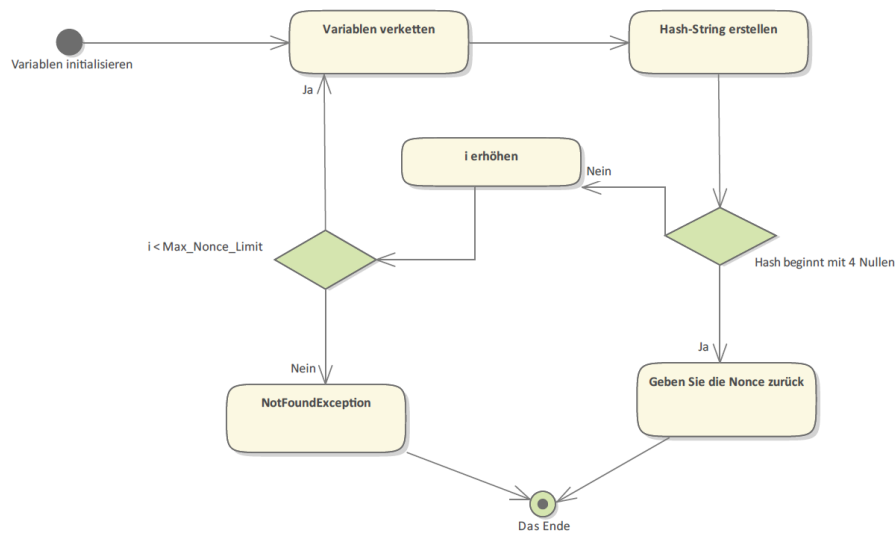
```
{
  "hash": "b6f6991d03df0e2e04daffcfd6bc418aac66049e2cd74b80f14ac86db1e3f0da",
  "ver": 1,
  "vin_sz": 1,
  "vout_sz": 2,
  "lock_time": "Unavailable",
  "size": 258,
  "relayed_by": "64.179.201.80",
  "block_height": 12200,
  "tx_index": "12563028",
  "inputs": [
    {
      "prev_out": {
        "hash": "a3e2bcc9a5f776112497a32b05f4b9e5b2405ed9",
        "value": "10000000",
        "tx_index": "12554260",
        "n": "2"
      },
      "script": "76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
    }
  ],
  "out": [
    {
      "value": "98000000",
      "hash": "29d6a3540acfa0a950bef2b9dc75cd51c24390fd",
      "script": "76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
    },
    {
      "value": "2000000",
      "hash": "17b5038a413f5c5ee288caa64cfab35a0c01914e",
      "script": "76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
    }
  ]
}
```

- Das nächste Klassendiagramm zeigt die gesamten Daten aus dem realen Blockchain-Netzwerk. Es ist hilfreich, diese Daten in Form eines Klassendiagramms darzustellen, um die Implementierung zu verstehen.



- 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
  
```

---

### 3.6 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.

### 3.7 Vor- und Nachteile von Proof-Of-Work

Ich habe diese Tabelle erstellt, um die Vor- und Nachteile dieser Methode genau zu erklären :

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 CO<sub>2</sub>-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 Verwendung von Segregated Witness (SegWit) oder Lightning-Netzwerken. Diese Technologien können die Größe von Transaktionen reduzieren und somit die Geschwindigkeit erhöhen.
- Die heutige Schwierigkeit ist :

Depth	1
Size	1695479
Version	0x2a152000
Merkle Root	d7-3b 
Difficulty	36950494067222,41
Nonce	1117283344
Bits	386375189
Weight	3993569WU
Minted	6,25 BTC
Reward	6.35686843 BTC
Mined on	Nov 28, 2022, 6:06:41 PM
Height	765066
Confirmations	1
Fee Range	0-1274 sat/vByte
Average Fee	0.00006392
Median Fee	0.00002340
Miner	Unknown

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

### 4.1 Münzen

- Bevor ich anfangen, mit Ihnen darüber zu sprechen, wie Sie mit Bitcoin Geld verdienen können, möchte ich Ihnen zunächst einige Münzen vorstellen, die die Proof-Of-Work-Methode verwenden

- Bitcoin Cash



- Bitcoin SV



- Litecoin



- Dogecoin



- Bitcoin Gold



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

- Ethereum Classic



- Monero



- Zcash



- Kadena





## 4.2 Wie kann ich mit Kryptowährung Geld verdienen ?

### 4.2.1 Krypto-Mining

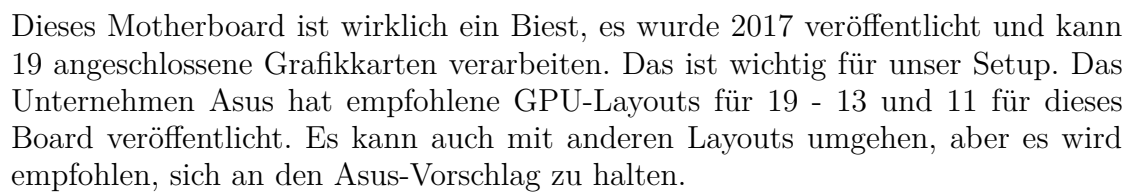
#### Konzept

Im Jahr 2022 können wir die Preise der Währungen sehen, der Bitcoin liegt in diesem Monat bei 15.891 Euro, das ist ein astronomischer Preis für diese Währung. Also, wir sind daran interessiert, und wir wollen unsere Mining-Unternehmen zu starten.

Schauen wir uns an, was ein gutes Krypto-Mining-Rig ausmacht und welche Hardware man braucht, wenn man es mit dem Mining ernst meint. Und bevor wir direkt mit den notwendigen Materialien beginnen, möchte ich zuerst über ein sehr wichtiges Wort sprechen, das in dieser Branche verwendet wird. Was ist Krypto-Mining-Rig.

Also, Rig Computer enthält eine extrem leistungsstarke Materialien, die es eine Menge von Versorgungsmodulen enthält. Zum Beispiel: wenn jemand Bitcoin minen will, mit der riesigen Konkurrenz auf diese Kryptowährung, und die große Schwierigkeit. Ein normaler oder leistungsfähiger Computer wird für diese Aufgabe nicht ausreichen. Deshalb steht das Rig an erster Stelle, denn es enthält eine Hauptplatine, die eine oder mehrere Grafikkarten gleichzeitig bedienen kann. Wir verwenden GPU in dieser Operation, weil wir für die hohe mögliche Geschwindigkeit suchen, aber wenn es eine Menge von Grafikkarten, wird es auch notwendig sein, eine robuste Stromversorgung zu haben, um diese Operation auf das hohe Niveau zu schieben.

**Motherboard :** Asus B250 Mining Expert

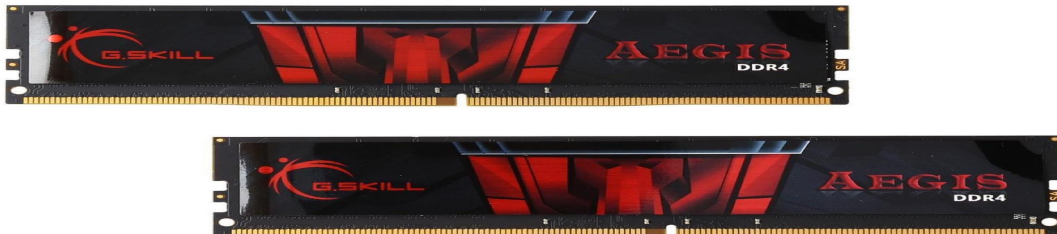


**CPU :** Intel Core i5-6500



Alle unsere massiven Operationen werden von der GPU ausgeführt, so dass wir kein Geld für eine leistungsstarke CPU ausgeben müssen, diese CPU hier eignet sich sehr gut für unser Setup und ist auch mit dem Motherboard kompatibel.

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



Es besteht auch keine Notwendigkeit, Geld für 128 GB RAM auszugeben, diese 16 GB (DDR4) reichen für unser Unternehmen aus und sind gut, um die Mission zu erfüllen.

**Storage :** SanDisk SSD Plus 1TB



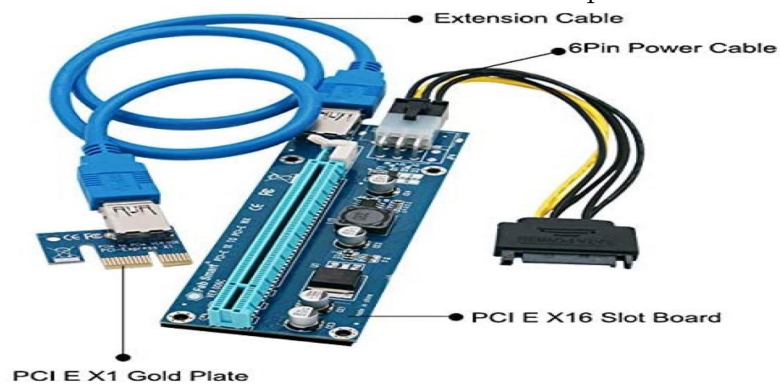
Ich werde es vorziehen, 4 seiner ssd-Speicher zu installieren. Sie sind schnell und unter 100\$

**PSU :** Segotep 850W Full-Modular PSU



Diese Segotep PSUs sind gut, denn sie bieten eine zuverlässige Leistung, die davon abhängt, wie viele Grafikkarten Sie installiert haben, benötigen Sie möglicherweise mehrere PSUs. Aber wenn Sie Ihr Bitcoin-Mining auf extreme Leistung bringen wollen, ist es notwendig, mehr zu bezahlen

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



Dies ist der eigentliche Unterschied zwischen Rig und normalem Computer, denn man kann nicht alle Grafikkarten direkt an das Motherboard anschließen, aber mit diesem Modul kann man sie indirekt anschließen.

Ich empfehle die Verwendung von powered risers für jede Grafikkarte, da sie eine großartige und stabile Stromversorgung für die Grafikkarten bieten

### Nvidia graphics card : MSI Ventus 3X GeForce RTX 3090



Dies ist eine großartige Karte für ein Mining-Rig, fähig zur Übertaktung, stabil und gut gekühlt. Es ist eine ziemlich effiziente Karte, die niedrigeren Stromverbrauch und reduzierte Bergbaukosten bedeutet.

### 4.3 Wo sollte ich mein Geld in Kryptowährungen investieren?

Diejenigen Investoren, die in den ersten Tagen in Bitcoin investiert haben, sind jetzt so reich und extrem wohlhabend geworden. Der Blockchain-Markt wird immer größer und mächtiger, vor allem mit dem Web 3. Die Anleger suchen nach der nächsten digitalen Währung, um reich zu werden. Es wird nun die Frage gestellt, wie man die nächste große Kryptowährung finden kann.

- Der Preis ist entscheidend  
Das wichtigste Element, auf das man bei der Suche nach Kryptowährungen achten sollte, ist der Preis des Tokens. Für die Investoren, die nicht über ein großes Budget verfügen, um in die Kryptowährungen zu investieren, sollten einige Kryptos mit einem niedrigen Preis kaufen.
- Aussichten auf Annahme  
Wenn jemand eine Kryptowährung finden kann, die einen Vorteil gegenüber anderen hat (und die mehr angenommen wird). Es wird die beste Kryptowährung sein, in die Sie Ihr Geld investieren sollten.
- Die Versorgung ist ein Faktor  
Die meisten Kryptowährungen haben ein vorher festgelegtes maximales Angebot. Wenn das Maximum durch die Mining-Operationen erreicht wird. Wenn das Interesse aufrechterhalten wird, während das Angebot festgelegt ist, könnte der Preis steigen. Behalten Sie also immer im Hinterkopf, dass das Angebot ein wichtiger Faktor ist, bevor Sie investieren
- Preis und Volumen Im Jahr 2022 gibt es viele Plattformen, die das Investieren so einfach machen, es speichert die wechselnde Geschichte der Kryptowährungen und die Preise über den Blockchain-Markt. Es ist also besser, den Markt sehr sorgfältig zu scannen und eine Entscheidung über die Erhöhung der Währungen zu treffen. Es gibt auch einige künstliche intelligente Modelle, die auf alten Kryptowährungsdaten basieren und die es leicht machen, vorherzusagen, ob der Preis einer Kryptowährung in Zukunft steigen oder fallen wird. Aber Sie sollten bedenken, dass der Preis nicht gehalten werden kann, und es gibt immer eine Chance zu verlieren.

## 5 Schluss

Die Methode „Proof-Of-Work“ ist ein Konsensmechanismus, der es den Netzwerkteilnehmern ermöglicht zu bestätigen, dass die von ihnen durchgeführten Transaktionen gültig sind. Dies geschieht, indem andere Miner versuchen, eine gültige Nonce zu finden. Der erste, der die Nonce findet, erhält eine Belohnung, und die anderen Teilnehmer überprüfen die Gültigkeit des Hashs. Das Mining erfordert eine starke Hardware-Ausstattung, aber alles wird mietbar sein.

Nach diesem Bericht haben wir viele Informationen über bitcoin und seine Funktionsweise und die grundlegende Funktion des Proof of Work gesehen. Wir verstehen auch die Bedeutung des Blockchain-Netzwerks und alle anderen Definitionen. Lassen Sie uns beginnen, in Bitcoin oder in andere Kryptowährungen zu investieren.

# Literatur

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

<https://www.softwaretestinghelp.com/wp-content/qa/uploads/2019/06/structure-of-a-singly-png>

[https://en.wikipedia.org/wiki/Proof\\_of\\_work](https://en.wikipedia.org/wiki/Proof_of_work)

<https://en.wikipedia.org/wiki/Blockchain>

<https://www.iotforall.com/blockchain-use-cases-in-2022>

<https://www.btc-echo.de/academy/bibliothek/proof-of-work/>

<https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stock-proof-of-work/>

[https://www.blockchain.com/explorer/api/blockchain\\_api](https://www.blockchain.com/explorer/api/blockchain_api)

<https://bitcoin.org/img/icons/opengraph.png>

[https://upload.wikimedia.org/wikipedia/commons/5/58/Bitcoin\\_Cash.png](https://upload.wikimedia.org/wikipedia/commons/5/58/Bitcoin_Cash.png)

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

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

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

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

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

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

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

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



<https://s2.coinmarketcap.com/static/img/coins/200x200/2577.png>

<https://s2.coinmarketcap.com/static/img/coins/200x200/1042.png>

<https://s2.coinmarketcap.com/static/img/coins/64x64/1698.png>

<https://s2.coinmarketcap.com/static/img/coins/200x200/109.png>

<https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-s proof-of-work/#:~:text=The%20proof%2Dof%2Dwork%20algorithm,too%20slowly%2C%20they%20get%20easier.>

[https://www.blockchain.com/explorer/api/blockchain\\_api](https://www.blockchain.com/explorer/api/blockchain_api)

<https://bitcoin.org/img/icons/opengraph.png?1666775325>

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

<https://www.creativefabrica.com/wp-content/uploads/2021/06/16/Cryptocurrency-Litecoin-Lo jpg>

<https://www.creativefabrica.com/wp-content/uploads/2021/06/16/Cryptocurrency-Litecoin-Lo jpg>

<https://www.investopedia.com/terms/p/proof-stake-pos.asp#:~:text=What%20Is%20Proof%2Dof%2DStake%20vs.,new%20blocks%20to%20the%20blockchain.>

<https://www.businessinsider.com/personal-finance/proof-of-work>

<https://smartasset.com/investing/how-to-invest-in-cryptocurrency#:~:text=The%20most%20popular%20place%20to,Ethereum%20with%20a%20debit%20card.>

<https://www.zdnet.com/article/how-to-build-a-cryptomining-rig/>

<https://www.investopedia.com/news/how-identify-next-big-cryptocurrency/>