



**FH AACHEN**  
UNIVERSITY OF APPLIED SCIENCES

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

Ziad Bougrine

30. November 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>11</b>
3.1	Was ist Proof-Of-Work ? . . . . .	11
3.2	Wie funktioniert Proof of Work bei einer Blockchain ? . . . . .	11
3.3	Wie genau funktionieren die Proof-of-Work-Berechnungen? . . . . .	13
3.4	Was hat es mit der Difficulty auf sich ? . . . . .	14
3.5	This is the algorithm side . . . . .	14
3.6	Sicherheit des Proof-Of-Work . . . . .	17
3.7	Vor- und Nachteile von Proof-Of-Work . . . . .	18
<b>4</b>	<b>Der Bitcoin-Markt und die Verwendung von Proof of Work</b>	<b>21</b>
4.1	Münzen . . . . .	21
4.2	Wie kann ich mit Kryptowährung Geld verdienen ? . . . . .	23
4.2.1	Krypto-Mining . . . . .	23
<b>5</b>	<b>Schluss</b>	<b>28</b>

# 1 Einleitung

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

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

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

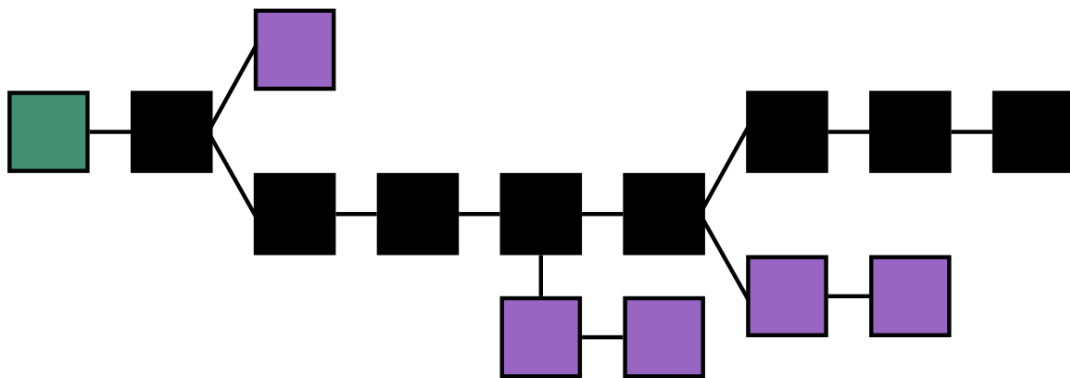
Das ist der Hauptgrund, warum Blockchain-Technologie erfunden worden. Indem es immer für alle sichtbar im Hauptbuch aufgezeichnet wird, wenn Geld von einem Konto auf ein anderes überwiesen wird.

## 2 Einführung in die Blockchain

### 2.1 Blockchain Definition

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

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



### 2.2 Konstruktion des Blocks

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

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

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

- **Version:** Sie ist benutzbar, um einen neuen Block zu erstellen und um eine neue Version von Software zu identifizieren. Es ist auf 4 Bytes ( $4 \times 8$  „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 interessieren sich für die Nonce, weil das Mining-Programm Zufallszahlen (Bruteforce) verwendet, um die Nonce im Hash zu erraten. Der Hash wird verifiziert, wenn die Nonce gelöst ist. Wenn die Nonce oder eine Zahl darunter erraten wird. Dann schließt das Netzwerk diesen Block, generiert einen neuen mit einem Header und der Prozess wiederholt sich.

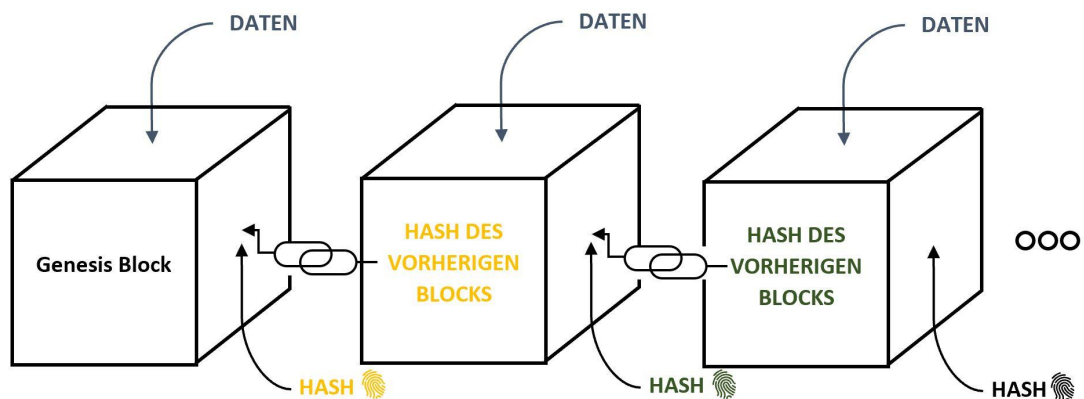


## Was sind Merkle-Bäume?

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

## 2.3 Blockchaining-Mechanismus

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



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

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

**Achtung :** ist dieser Mechanismus gesichert ?

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

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

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

### 3.1 Was ist Proof-Of-Work ?

Proof-Of-Work kam mit einem Grundprinzip, wenn ein Miner versucht, einen Block zur Kette von Blöcken im Blockchain-Netzwerk hinzuzufügen, macht es diese Methode schwierig. Der Miner sollte sich viel Mühe geben, um den Block zu erstellen. Diese Methode basiert auf vielen Grundlagen der Kryptowährung wie folgt:

- Die Schwierigkeit, einen gültigen Hash zu finden, um den Block dem Blockchain-Netzwerk hinzuzufügen, ist so gewählt, dass alle zehn Minuten ein neuer Block mit einer bestimmten Anzahl von BTC in unsere Kette kommt. Dies sichert das algorithmische Geldmengenwachstum.
- Mit Hilfe von PoW ist es für Nodes sehr einfach zu erkennen, welche Blockchain die richtige ist: vor allem diejenige, der er die meiste Arbeit in Form von Rechenkapazität leistet.
- Proof of Work sichert das Blockchain-Netzwerk vor allen Angreifern, denn diese müssten mehr Energie in das Netzwerk einspeisen als alle anderen insgesamt verfügbaren Miner – und das über einen langen Zeitraum. Das ist beim Bitcoin unmöglich.
- Proof of Work ist ferner der fairste Mechanismus der Neuverteilung von Geld, den wir kennen. Denn im Gegensatz zu Fiatgeld können frische Coins nicht mit einem Federstrich erzeugt werden, sondern erfordern einen realen Aufwand an Ressourcen.

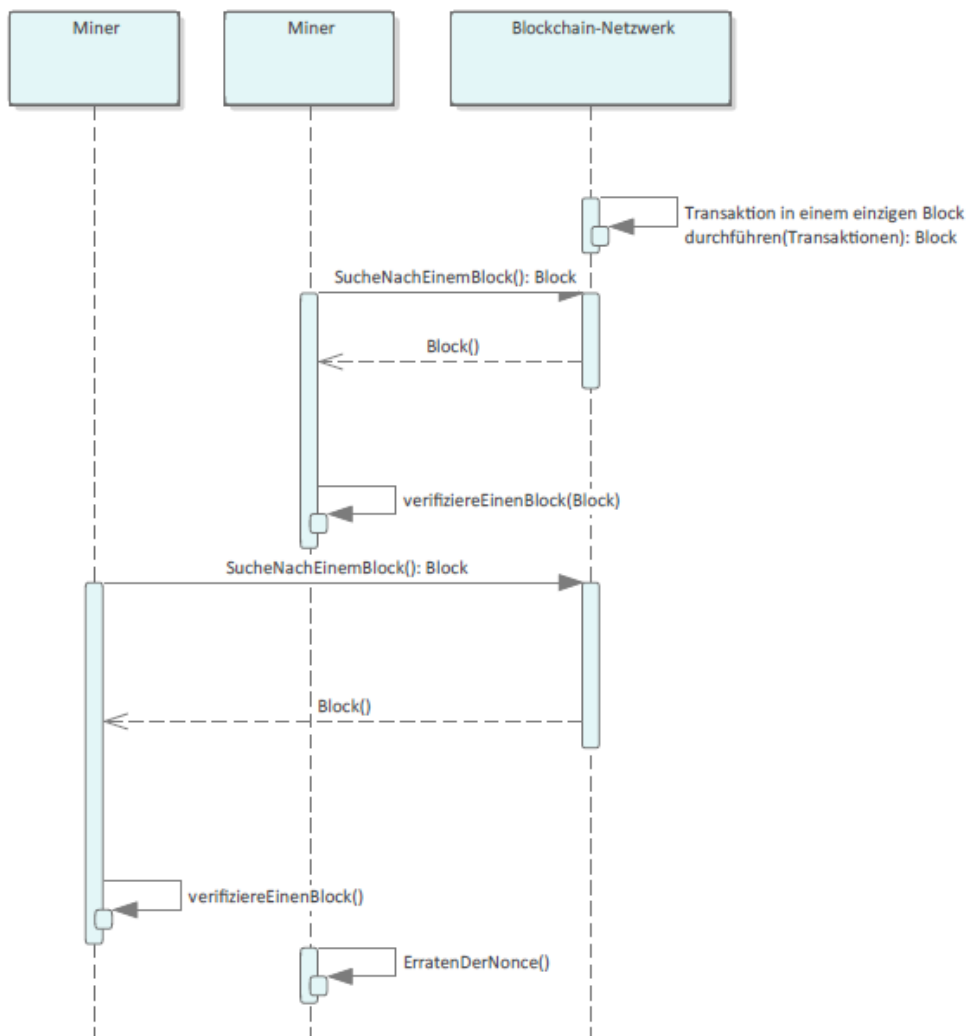
### 3.2 Wie funktioniert Proof of Work bei einer Blockchain ?

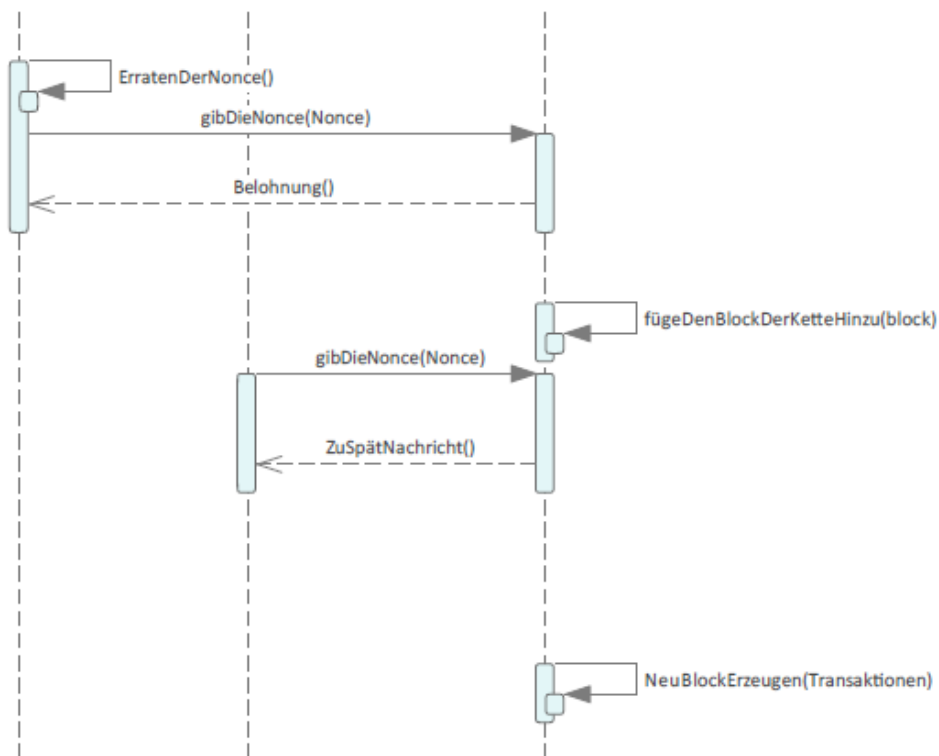
Dieser Mechanismus von PoW wird als Mining bezeichnet, was bedeutet, die Nonce mit bestimmten Eigenschaften zu erraten, indem Milliarden von Berechnungen durchgeführt werden. Wenn Sie ein solches Ergebnis erzielt haben, erhalten Sie eine Belohnung mit der sogenannten Blocksubvention.

Diese beschreiben den Vorgang einer Transaktion im Blockchain-Netzwerk

- Das Blockchain-Netzwerk erstellt einen Block, der alle Transaktionen enthält
- Der Miner wird überprüfen, ob die Transaktionen legitim sind
- Alle Bergleute beginnen zu versuchen, die Lösung zu finden (was bedeutet, erraten Sie die Nonce), und der erste, der sie findet, erhält eine Belohnung und auch die Transaktionsgebühren
- Der Block wird der Blockchain hinzugefügt
- Der Prozess wird wiederholt

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





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

- Die Miner verwenden Hash-Funktionen. Sie sind injektive mathematische Funktionen, die nicht rückgängig gemacht werden können. Sie erzeugen aus einer beliebig langen Zeichenfolge eine eindeutige Zeichenfolge fester Länge. Die Schwierigkeit liegt darin, ein Ergebnis mit bestimmten Eigenschaften zu finden, die sich aus der Hash-Funktion ergeben. Bitcoin verwendet beispielsweise die SHA-256-Hash-Funktion für das Mining.
- Die Hash-Funktion liefert ein unvorhersehbares Ergebnis, deshalb sollten wir die Frage stellen: "Welche Zeichenfolgen müssen der Hash-Funktion übergeben werden, um einen genauen Wert zu erzeugen?". Da die bekannteste Eigenschaft der Hash-Funktion ist, dass niemand die Operation einfach umkehren kann, kann der Miner auf andere Weise die erhaltene Zeichenfolge nicht einfach umkehren und die Eingabe der Hash-Funktion erhalten.
- Aus diesem Grund gibt es das Konzept des Mining, die Miner versuchen, die Nonce

und die Reihenfolge jedes Parameters zu erraten, die die Hash-Funktion als eine Zeichenfolge nimmt und ein Ergebnis liefert. Es gibt eine Billard von Operationen, die vom Bergmann durchgeführt werden, um den Wert der Eingabe zu erreichen.

- Wenn der Block abgebaut wird, überprüfen alle Teilnehmer des Blockchain-Netzwerks die präsentierte Lösung, um eine gültige Blockchain zu haben

### 3.4 Was hat es mit der Difficulty 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 This is the algorithm side

- Jetzt möchte ich darüber sprechen, wie der Arbeitsnachweis technisch funktioniert, sehen wir uns zuerst eine echte Blockstruktur von der offiziellen Website „blockchain.com“ an.

#### 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--"
  ]
}
```

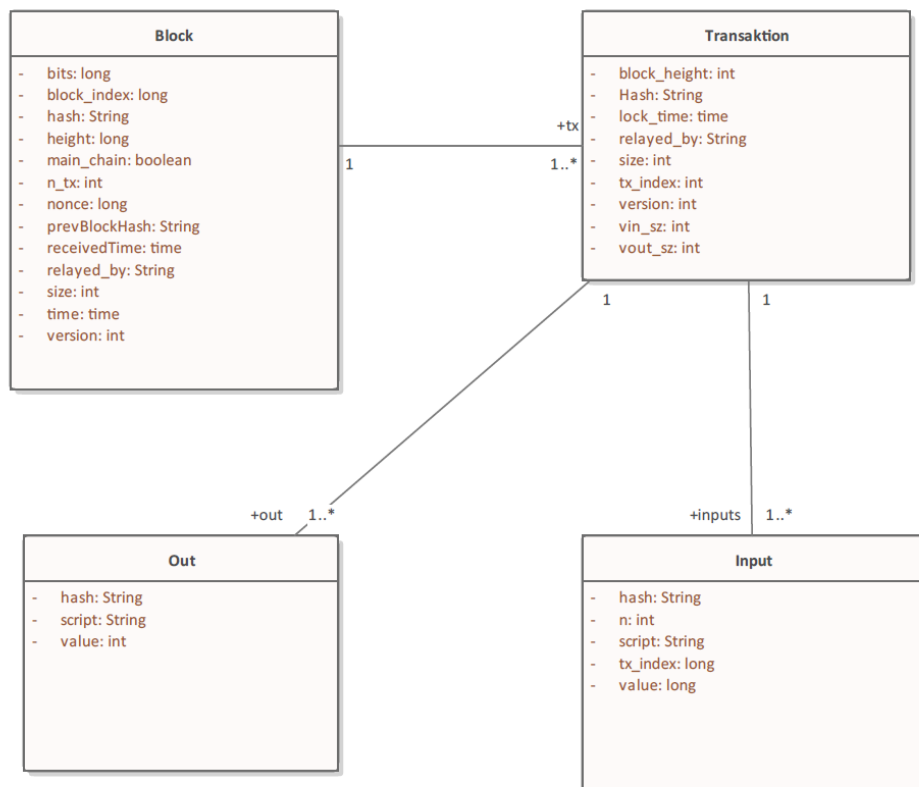
- Und dies ist eine echte Einzeltransaktionsstruktur

## 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`

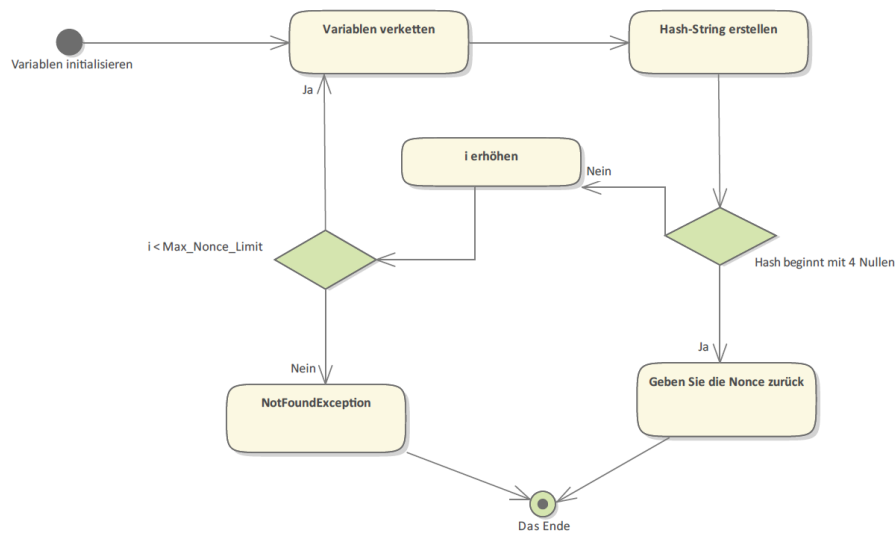
```
{
  "hash": "b6f6991d03df0e2e04daffcd6bc418aac66049e2cd74b80f14ac86db1e3f0da",
  "ver": 1,
  "vin_sz": 1,
  "vout_sz": 2,
  "lock_time": "Unavailable",
  "size": 258,
  "relayed_by": "64.179.201.80",
  "block_height": 12200,
  "tx_index": "12563028",
  "inputs": [
    {
      "prev_out": {
        "hash": "a3e2bcc9a5f776112497a32b05f4b9e5b2405ed9",
        "value": "100000000",
        "tx_index": "12554260",
        "n": "2"
      },
      "script": "76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
    }
  ],
  "out": [
    {
      "value": "98000000",
      "hash": "29d6a3540acfa0a950bef2bfdc75cd51c24390fd",
      "script": "76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
    },
    {
      "value": "2000000",
      "hash": "17b5038a413f5c5ee288caa64cfab35a0c01914e",
      "script": "76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
    }
  ]
}
```

- Das nächste Klassendiagramm zeigt die gesamten Daten aus dem realen Blockchain-Netzwerk. Es ist gut, es in Form eines Klassendiagramms zu sehen, um zu erkennen, wie Daten für die Implementierung miteinander in Beziehung stehen



- Und jetzt erklären wir unseren Algorithmus mit dem Aktivitätsdiagramm, zuerst sollten wir Daten initialisieren, die Initialisierung von `Max_Nonce_Limit`, Anzahl der Nullen, für dieses Beispiel werden wir berücksichtigen, dass der Hash mit 4 Nullen beginnen sollte (nur für Informationen, Anzahl von Nullen sind wichtig, es zeigt die Komplexität des Algorithmus, wenn die Zahl hoch ist wie 7 oder 6 Nullen, wird es ein Jahr dauern, die Nonce mit wenig Hardware-Material zu finden. Wir sollten auch unsere `i-Inkrement-Variable` für die `for-Schleife` initialisieren





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

```

i ← 1
MaxNonceLimit ← 1000000000
zeros ← 4
for i < MaxNonceLimit do
    data ← blockNumber + transactions + prvHash + i
    hashVariable ← SHA256(data)
    if hashVariable.startsWith('0'*4) then return i
    end if
end for
  
```

### 3.6 Sicherheit des Proof-Of-Work

Was die Sicherheit betrifft, so bietet diese Proof-Of-Work-Methode ein hohes Sicherheitsniveau, da Angreifer über eine größere Energiequelle als andere Blockchain-Knoten verfügen sollten, was im Falle von Bitcoin unmöglich ist.

### 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
Hohes Sicherheitsniveau.	Ineffizient mit langsamen Transaktionsgeschwindigkeiten und teuren Gebühren.
Bietet eine dezentrale Methode zur Überprüfung von Transaktionen.	Hoher Energieverbrauch.
Ermöglicht Bergleuten, Krypto-Belohnungen zu verdienen.	„Mining“ erfordert oft teures Equipment.

#### Eklärung :

- Für ein hohes Sicherheitsniveau müsste eine spekulative Person, die die Kontrolle über das auf Proof-of-Work basierende Blockchain-Netzwerk übernehmen möchte, 50 % des Blockchain-Netzwerks in Besitz nehmen, was unmöglich ist, und sie benötigt eine Menge Material.
- Proof-Of-Work bietet eine dezentralisierte Methode, weil wir keine dritte Partei brauchen, der wir vertrauen, um unsere Transaktionen und Daten zu speichern, was bedeutet, dass alle Transaktionen im öffentlichen Register verfügbar sind und alle Teilnehmer des Blockchain-Netzwerks darauf zugreifen können.
- Viele Leute mögen Bitcoin wegen der Mining-Operation, weil alle Miner einige spezielle Hardware "Rig Mining" einrichten können und mit dem Mining von Bitcoin beginnen können und für jede erfolgreiche Mining-Operation eine Belohnung erhalten.

**Wo immer es Vorteile gibt, gibt es auch Nachteile. Bei der Proof-Of-Work-Methode gibt es einige Nachteile dieser Methode:**

- 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.
- Um das auf Proof-Of-Work basierende Blockchain-Netzwerk weiterzuführen, ist es eine große Energieverschwendung, weil mindestens 10 Grafikkarten arbeiten und auf extreme Leistung gebracht werden, sie brauchen viel Energie, um rund um die Uhr zu arbeiten, und vergessen Sie nicht die Kühlsysteme, die die Grafikkarten vor hohen Temperaturen schützen. Eine neue Mining-Anlage sollte aber auch erneuerbare Energie erzeugen. Das kostet zwar mehr Material, ist aber mietbar, weil die Mining-Firma keinen externen Strom verbraucht, und der Besitzer kann auch Stromrechnungen sparen. Deshalb können erneuerbare Energien im Bergbau eine gute Rolle spielen. Ich empfehle wirklich die Nutzung von Wind- und Solarenergie, um die benötigte Energie für das Unternehmen bereitzustellen, und das ist auch gut für die Natur, denn man sollte nicht vergessen, dass die externe Energie aus Kernkraftwerken und erneuerbaren Energien stammt. Atomkraft zerstört den Himmel wegen des Gases und stellen Sie sich vor, wenn 30% der Menschen in Deutschland anfangen würden, Bitcoin ohne erneuerbare Energien zu minen, würden die Energiepreise steigen und auch die Produktion würde steigen.
- Das Mining von Bitcoin braucht ein teures Material, weil die Bitcoin-Schwierigkeit heute astronomisch ist, was einige teure Nvidia's Grafikkarten und ein teures Motherboard erfordert, das die Grafik verarbeiten kann, um einen Wettbewerb zu starten. Für meine Meinung auch die teuren Preise, aber es ist rentabel Betrieb, weil Sie das ausgegebene Geld sehr leicht zurück, wenn Sie eine gute Mining-Unternehmen haben. Später werde ich sprechen, wie man eine gute Mining-Unternehmen erstellen kann.

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

---

## 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

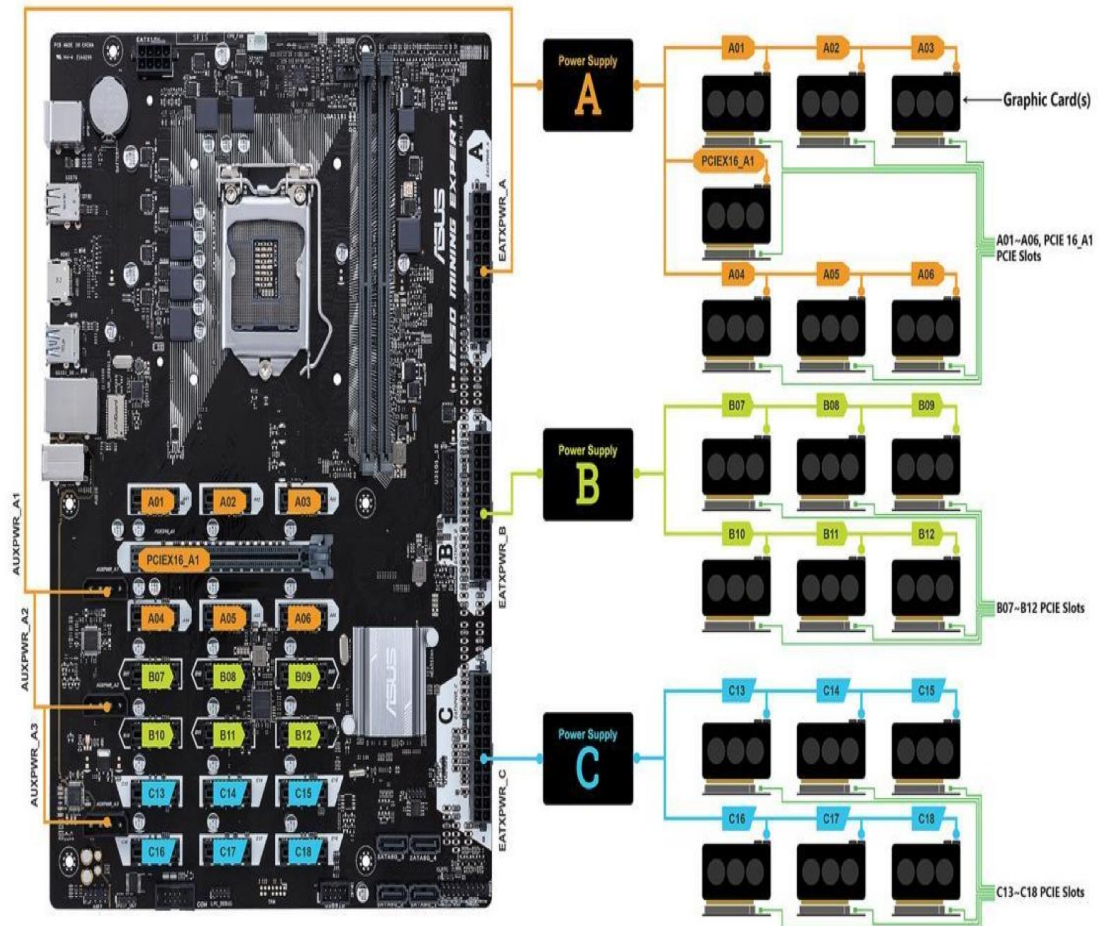
Im Jahr 2022 können wir die Preise der Währungen sehen, der Bitcoin liegt in diesem Monat bei 15.891 Euro, das ist ein astronomischer Preis für diese Währung. Also, wir sind daran interessiert, und wir wollen unsere Mining-Unternehmen zu starten.

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.

## Hardware

**Motherboard :** Asus B250 Mining Expert



Dieses Motherboard ist wirklich ein Biest, es wurde 2017 veröffentlicht und kann 19 angeschlossene Grafikkarten verarbeiten. Das ist wichtig für unser Setup. Das Unternehmen Asus hat empfohlene GPU-Layouts für 19 - 13 und 11 für dieses Board veröffentlicht. Es kann auch mit anderen Layouts umgehen, aber es wird empfohlen, sich an den Asus-Vorschlag zu halten.



**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



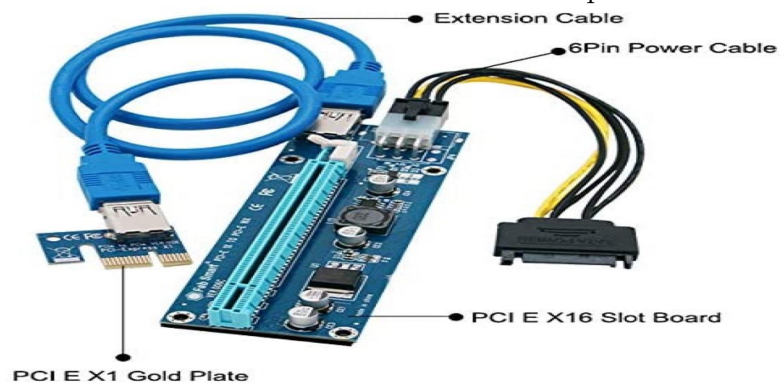
I ll prefer to install 4 of his ssd storage. They are fast and under 100\$

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



Diese SSegotep PSUsßind 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.

## 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

- [1] Donald E. Knuth (1986) *The T<sub>E</sub>X Book*, Addison-Wesley Professional.
- [2] Leslie Lamport (1994) *L<sup>A</sup>T<sub>E</sub>X: a document preparation system*, Addison Wesley, Massachusetts, 2nd ed.