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

Ziad Bougrine

23. November 2022

FH Aachen: [redacted]

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

FH Aachen: [redacted]

Inhaltsverzeichnis

1 Einleitung

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

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

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

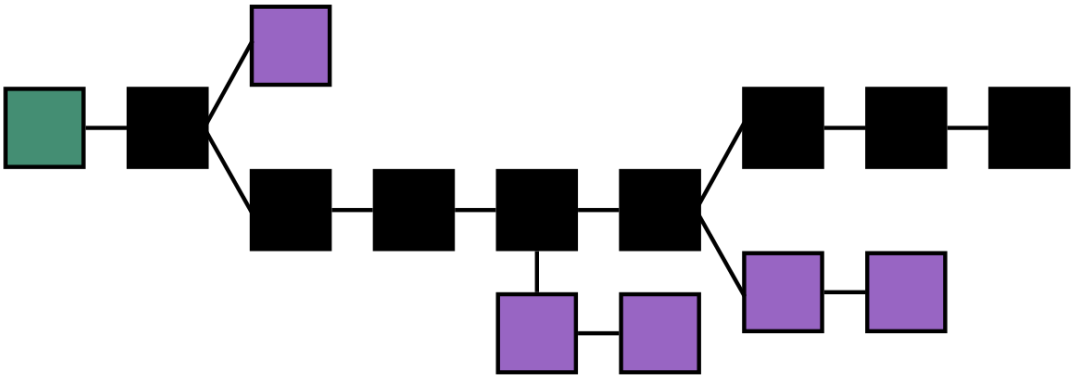
Das ist der Hauptgrund, warum Blockchain-Technologie erfunden worden. Indem es immer für alle sichtbar im Hauptbuch aufgezeichnet wird, wenn Geld von einem Konto auf ein anderes überwiesen wird.

2 Einführung in die Blockchain

2.1 Blockchain Definition

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

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



2.2 Konstruktion des Blocks

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

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

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

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

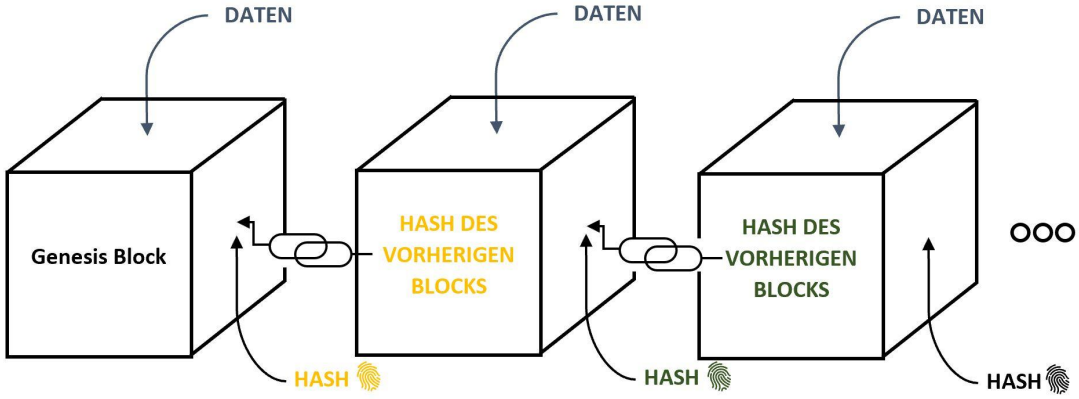
Information : Die Miner interessieren sich für die Nonce, weil das Mining-Programm Zufallszahlen (Bruteforce) verwendet, um die Nonce im Hash zu erraten. Der Hash wird verifiziert, wenn die Nonce gelöst ist. Wenn die Nonce oder eine Zahl darunter erraten wird. Dann schließt das Netzwerk diesen Block,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

Was sind Merkle-Bäume?

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

2.3 Blockchaining-Mechanismus

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



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

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

Achtung : ist dieser Mechanismus gesichert ?

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

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

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.

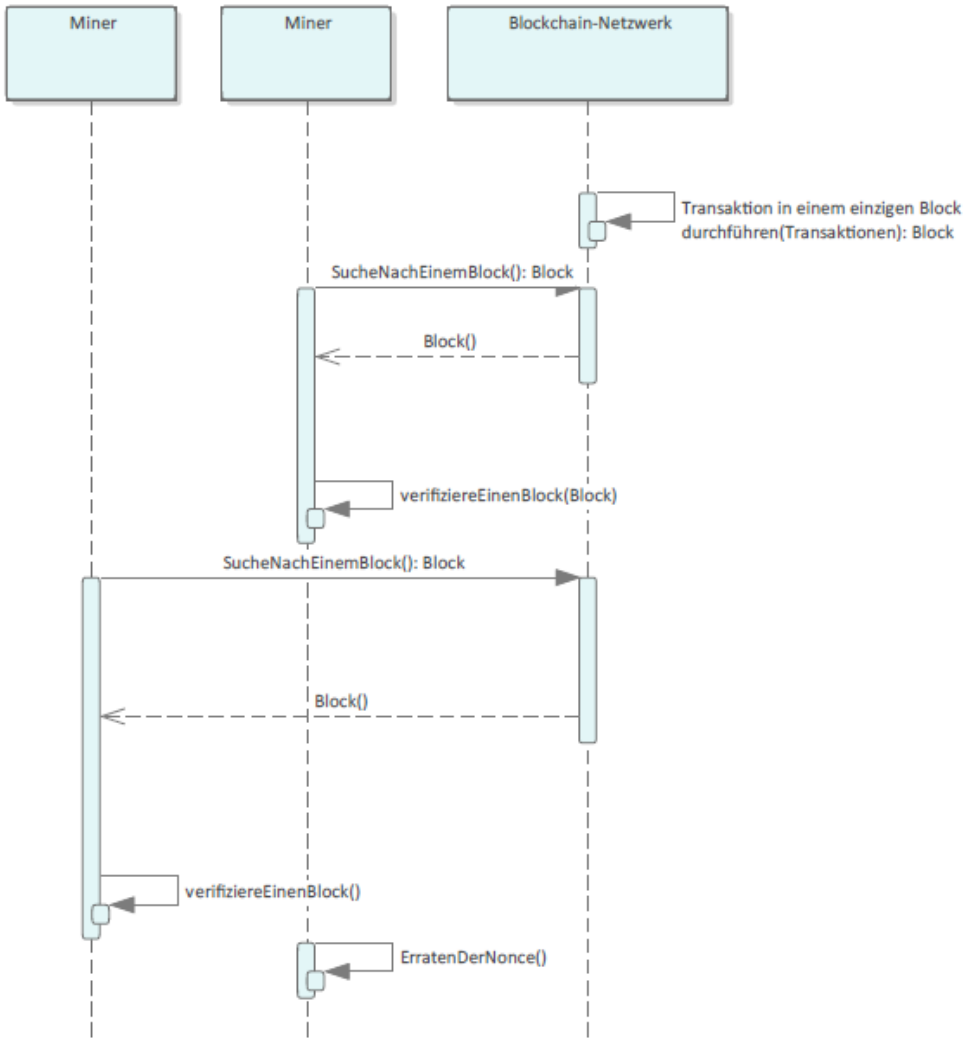
3.2 Wie funktioniert Proof of Work bei einer Blockchain ?

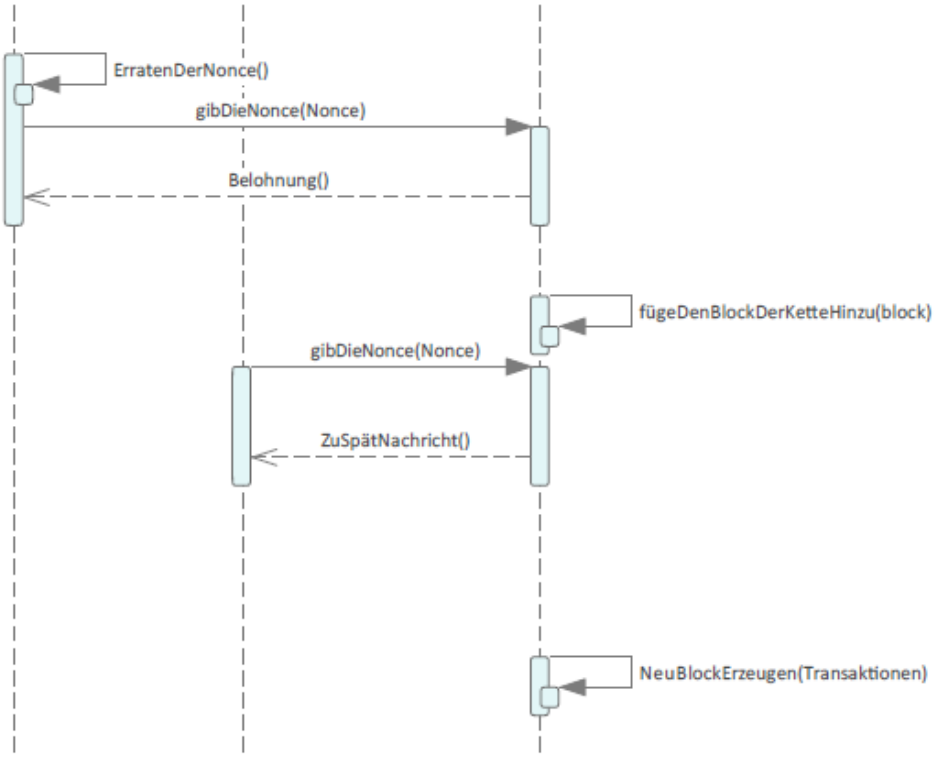
Dieser Mechanismus von PoW wird als Mining bezeichnet, was bedeutet, die Nonce mit bestimmten Eigenschaften zu erraten, indem Milliarden von Berechnungen durchgeführt werden. Wenn Sie ein solches Ergebnis erzielt haben, erhalten Sie eine Belohnung mit der sogenannten Blocksubvention.

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

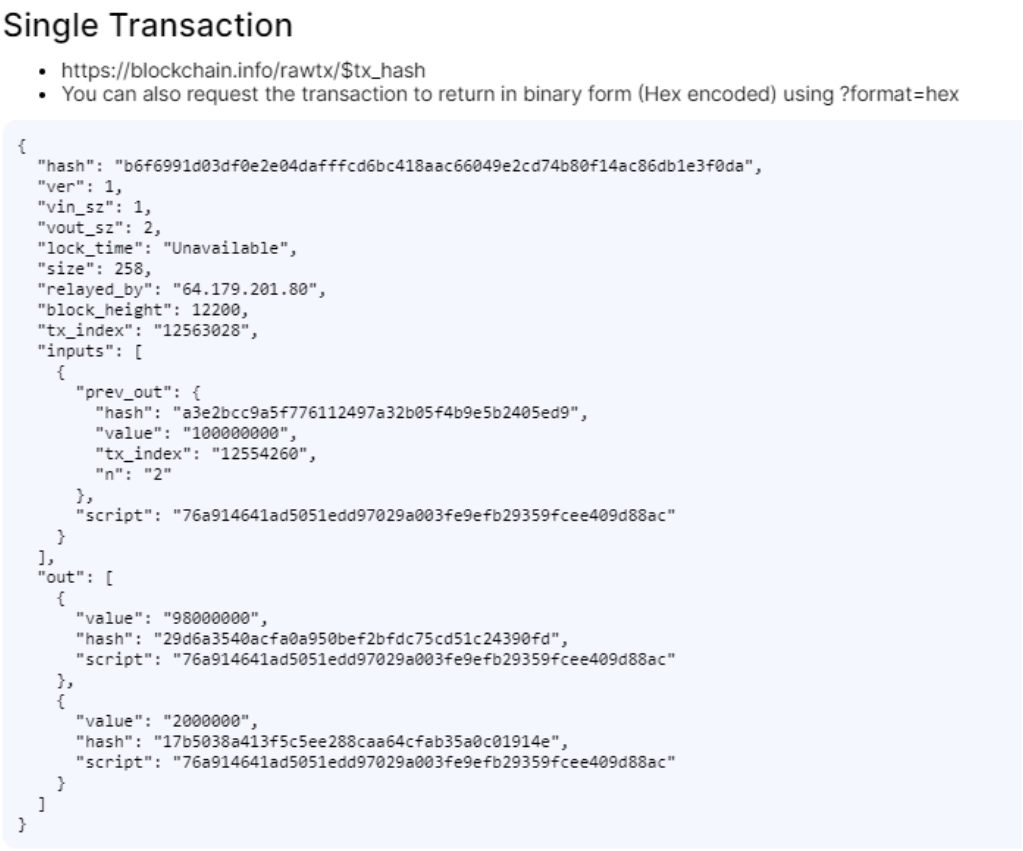
– Jetzt möchte ich darüber sprechen, wie der Arbeitsnachweis technisch funktioniert, sehen wir uns zuerst eine echte Blockstruktur von der offiziellen Website „blockchain.com“ an.

Single Block

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


```
{
  "hash": "0000000000000bae09a7a393a8acded75aa67e46cb81f7acaa5ad94f9eacd103",
  "ver": 1,
  "prev_block": "00000000000007d0f98d9edca880a6c124e25095712df8952e0439ac7409738a",
  "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

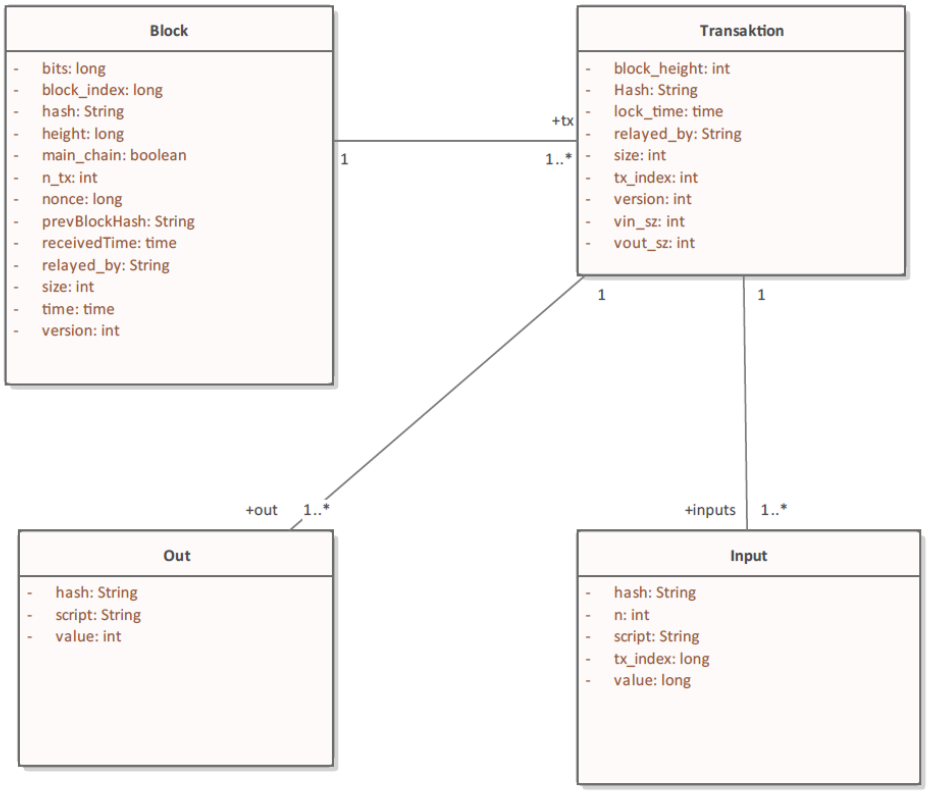


Single Transaction

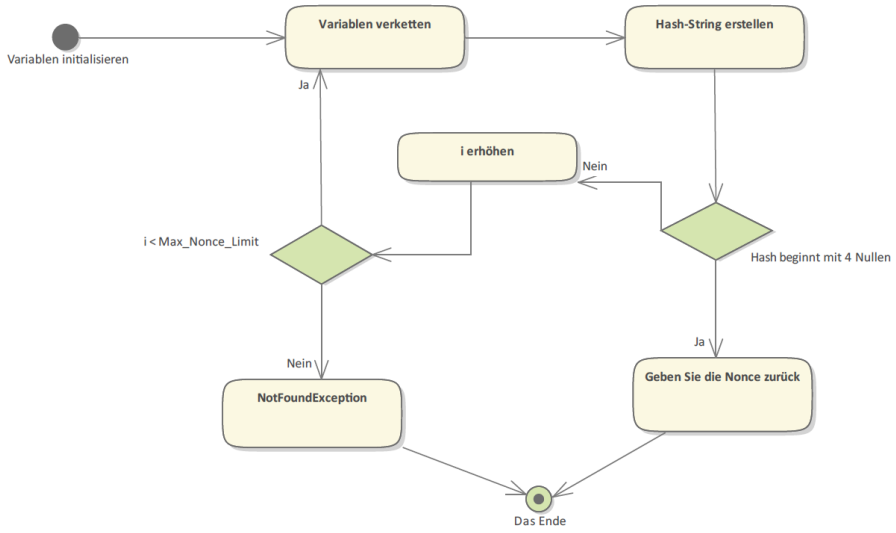
- https://blockchain.info/rawtx/$tx_hash
- You can also request the transaction to return in binary form (Hex encoded) using ?format=hex


```
{
  "hash": "b6f6991d03df0e2e04dafffcd6bc418aac66049e2cd74b80f14ac86db1e3f0da",
  "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

$i \leftarrow 1$
$MaxNonceLimit \leftarrow 100000000$
$zeros \leftarrow 4$
for $i < MaxNonceLimit$ **do**
    $data \leftarrow blockNumber + transactions + prvHash + i$
    $hashVariable \leftarrow SHA256(data)$
    if $hashVariable.startWith('0' * 4)$ **then return** i
    end if
end for

3.6 Sicherheit des Proof-Of-Work

3.7 Vor- und Nachteile von Proof-Of-Work

Nachteile	Vochteile
Hohes Sicherheitsniveau.	Ineffizient mit langsamen Transak
Bietet eine dezentrale Methode zur Überprüfung von Transaktionen.	Hoher Energieverbrauch.
Ermöglicht Bergleuten, Krypto-Belohnungen zu verdienen.	„Mining of Bitcoin“ erfordert oft

4 Proof-of-Work-Münzen

Hier sind die meisten Münzen, die sie Proof-Of-Work verwenden