# Proof of Useful Work: Eine Umsetzung des Proof of Work Protokolls mit Fokus auf Usefulness

Jean-Marc Hendrikse

## 1 Einführung

## 2 Grundlagen

### 2.1 Definition von Nutzen

Unterscheidung in gesellschaftlichen und privaten Nutzen. Unter Nutzen (Usefulness) verstehe ich im folgenden den Benefit, den man aus dem Gebrauch einer Sache ziehen kann[https://de.wiktionary.org/wi
Dadruch, dass es sich bei der Blockchain um ein verteiltest System in einer Community handelt, betrachte ich in meiner Arbeit die Sichtweise des gesellschaftlichen Nutzens. Mehrere Akteure handeln auf der Blockchain. Wieder unterscheide zwischen Sozialem oder wirtschaftlichen Nutzen. Die Betrachtung des gesellschaftlichen Nutzens führt sehr schnell zu einer Philosophischen Frage, auf die ich hier nicht genauer eingehende werde, sondern nur eine Definition ablegen, wie Nutzen im Rahmen meiner Arbeit gewählt wird.

### 2.2 Blockchain und Bitcoin

Eine Blockchain ist ein dezentrales Public Ledger (Hauptbuch). Um bislang Transaktionen durchzuführen vertrauten wir bisher dritten „vertrauenswürdigen“ Instanzen, denen wir unser Geld anvertrauten... Allerdings besitzen diese permanent Zugriff auf unsere Besitztümer, unseren Daten und können jeder Zeit, wenn diese nicht selbst kompromitiert sind angegriffen werden. Mithilfe der Blockchain Technologie wird eine neue Möglichkeit geschaffen vom zentralen Gedanken der Systeme auf ein dezentrales umzusteigen. Im wesentlichen handelt es sich bei der Blockchain um eine dezentrale Datenbank in einem peer-to-peer Netzwerk von Computersystemen. Was der Inhalt der Daten auf dieser Datenbank ist spielt dabei keine Rolle. Es kann sich um Transaktionsdaten einer Überweisung, digitale Ereignisse oder um Grundbucheinträge handeln. Anders als es bei herkömmlichen Datenbanken jedoch der Fall ist wird die Blockchain nicht auf einem einzelnen zentralen Server sondern verteilt auf mehreren Rechnern eines großen Netzwerks gehalten. Jeder Teilnehmer dieses Netzwerks erhält bei Eintritt in die Blockchain eine lokale Kopie von der Blockchain. Jede Transaktion wird zu einem Block zusammengefasst und mittels kryptographischer Berechnungen mit anderen Transaktionsblöcken zu einer Kette, der „Block-Chain“, verbunden. Ein einzelner Block besteht sowohl aus einem Zeitstempel, Transaktionsdaten und aus einem kryptographischen Hash des vorhergehenden gültigen Blocks bzw. der vorhergehenden Transaktion. Bei der Neuaufnahme eines neuen Blockes in die Blockchain muss per Konsens die Mehrheit aller Teilnehmer des Systems verifizieren, dass dieser Block gültig ist, also dass diese Transaktion tatsächlich stattgefunden hat. Nur und nur dann kann dieser Block aufgenommen werden. Dadurch dass jeder Teilnehmer/Miner eine Kopie der aktuellen Blockchain-Historie enthält, kann er diese mit der neuen abgleichen und verifizieren. Somit kann eine mehrheitliche Einigung zwischen den Knoten geschaffen werden. Die Blockchain erhält somit immer die gesamte

Historie an transaktionen, die jemals durchgeführt wurden und wird chronologisch linear erweitert. Die kryptographische Verkettung von Transaktionen bildet das Fundament vieler Kryptowährungen. Das wohl bekannteste Beispiel ist die digitale Währung Bitcoin, die im November 2008 mit dem Titel „Bitcoin: A Peer-to-Peer Electronic Cash System"1 von einer unbekannten Einzelperson oder Gruppe mit dem Pseudonym Satoshi Nakamoto entwickelt wurde. Viele bis dahin vorangehende Digitale Währungen scheiterten daran, dass sie durch eine zentrale Instanz verifiziert werden mussten, um das Double Spending Problem zu lösen. Nakamoto verhinderte das Double Spending-Problem mithilfe der Blockchain-Technologie.

## 2.3 Konsensmechanismus

In zentralisierten Organisationen werden Entscheidungen getroffen, in dem eine Entscheidungsinstanz eine Entscheidung trifft. In der Blockchain ist das nicht möglich, da keine zentrale Entschiedungsinstanz existiert bzw. auf diese Bewusst verzichtet werden soll. Somit müssen in der Blockchain Entscheidungen über einen Konsens getroffen werden, indem ein Konsensmechanismus eingeführt wird. Ein Konsensmechanismus bezeichnet einen Algorithmus, der eine Einigung über den Status des Netzwerks zwischen den Beteiligten (meistens anonymen) Netzwerkknoten schafft. Dies ist die Basis der Blockchain Technologie. Dabei wird sichergestellt, dass alle Teilnehmer eine identische Kopie der Blockchain besitzen. Wie bereits im vorangegangenen Kapitel erwähnt erschwert ein Konsensmechanismus die Manipulation von Daten erheblich. Der Hauptgedanke der dahinter steckt ist, dass durch einen dezentralen Konsens-Mechanismus ein zentrale Kontrollinstanz zur Integritätsbestätigung obsolet wird.

## 2.4 Difficulty

## 2.5 The Byzantine Fault Tolerance

## 2.6 Proof of Work

## 2.7 Primecoin

Der größte Kritikpunkt der immer wieder im Zusammenhang mit Bitcoin und dessen Proof of Work Protokoll unter Experten auftaucht ist, dass die Berechnung zum Minen von Blöcken, also das Lösen einer Challenge, keinen nachhaltigen Wert besitzt ■BELEGE■>. Wie schon bereits erwähnt hat das Minen keinen anderen Sinn als zu beweisen, dass Energieaufgewendet wurde und man sich so dafür qualifiziert Blöcke zur Blockchain hinzuzufügen. Trotzdem ist das Proof of Work Protokoll das Herzstück von Bitcoins Sicherheit. Denn würde es Proof of Work nicht geben, so könnte ein kompromitierter Angreifer sich als Millionen von Bitcoin Knoten zur selben Zeit ausgeben und somit ernsthaft Bitcoins Transaktionsblöcke angreifen oder austauschen. Allerdings werden lediglich SHA256 berechnet, wodurch eine große Menge an Energie verschwendet wird. Primecoin ist die erste Kryptowährung, die auf dem Proof of Work Ansatz basiert und eine effiziente Lösungen für Aufgaben generiert, die weiter verwendet werden können und somit einen Nutzen liefern [Primecoin paper]. Statt also einer nutzlosen Berechnung eines SHA256 Hashes1 müssen Miner beim Proof of Work Protokoll von Primecoin lange Primzahlenketten finden. Es gibt drei Arten von Primzahlenketten, die sich für das Proof of Work Protokoll eignen: Cunningham Chain (CC) 1. Art, CC 2. Art und Bi-twin chain.

Cunningham Chain 1. Art. Bei der Cunninghamchain muss jede Primzahl der Kette um ein größer als das doppelte der vorhergehenden Primzahl sein:

Beispiel Kette der Länge 5: 1531, 3061, 6121, 12241, 24481

Cunningham Chain 2. Art. Die Cunningham Chain 2. Art gibt vor, dass jede Primzahl um eins verringert als das doppelte des Vorgängers ist.

Beispiel-Kette der Länge 5: 2, 5, 11, 23, 47

Bi-Twin Chain. In der Bi-Twin chain werden Paare gehalten, deren Differenz 2 ergibt.

Beispiel-Kette: 211049, 211051, 422099, 422101, 844199, 844201

Nun könnte man sich hier die Frage stellen wo der Nutzen in Berechnungen von Primzahlen liegt oder ob es lediglich eine ebenso sinnlose Berechnung wie die Berechnung von SHA256 Hashes ist. Doch es gibt viele Anwendungsgebiete aus der Mathematik, die sich mit der Suche nach großen Ketten von Primzahlen beschäftigt. Unter anderem die Suche nach Mersenne Primzahlen oder das Primzahlen Theorem2. Nachfolgend seine Liste der University of Tennesseee erwähnt, die Gründe für die Suche nach Primzahlen liefert: http://primes.utm.edu/notes/faq/why.html

1 Dabei wird mit nutzlos im Sinne für Weiterverwendung gemeint 2 Fußnote

## 2.8 Permacoin

Einen ganz anderen Ansatz zur nützlichen Alternative zu Bitcoin im Vergleich zu Primecoin liefert Microsoft in Zusammenarbeit mit der University of Maryland mit Permacoin, bei dem die Blockchain als verteilter Speicher von Archivdaten dienen soll. Miner sollen nicht mehr nur reine Rechenleistung aufwenden sondern vielmehr ungenutzten Speicherplatz zur Verfügung stellen, weshalb er vielmehr dem Protokoll Proof of Retrievabilty ähnelt.

## Literatur