HAW HAMBURG

BACHELORTHESIS
Ema Oprea

Vergleich verschiedener Konsensmechanismen für die Blockchain

FAKULTÄT TECHNIK UND INFORMATIK
Department Informatik

Faculty of Computer Science and Engineering
Department Computer Science

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Ema Oprea

Vergleich verschiedener Konsensmechanismen für die Blockchain

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang *Bachelor of Science Angewandte Informatik*
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Klaus-Peter Kossakowski
Zweitgutachter: Prof. Dr. Bettina Buth

Eingereicht am: 04. November 2021

Ema Oprea

Thema der Arbeit

Vergleich verschiedener Konsensmechanismen für die Blockchain

Stichworte

Blockchain, Konsensmechanismus, Konsensproblem

Kurzzusammenfassung

Die vorliegenden Bachelorarbeit befasst sich mit heute relevanten Konsensmechanismen für öffentliche Blockchain. Sie vergleicht diese bezogen auf Eigenschaften in den Bereichen Sicherheit und Nachhaltigkeit, um letztlich die beste Art von Konsensmechanismus zu ermitteln.
Hauptsächlich wurden die Konsensmechanismen Proof-of-Work (PoW) und Proof-of-Stake (PoS) miteinander verglichen, da sich die restlichen Konsensmechanismen als nicht sicher genug herausstellen.
PoW stellt sich zwar als sicherer als PoS heraus, allerdings ist PoS nachhaltiger als PoW, welches einen hohen Energieverbrauch hat. Da Sicherheit aber als wichtigste Eigenschaft festgelegt wurde, ist PoW die hier betrachtete beste Art von Konsensmechanismus. Ob der hohe Energieverbrauch von PoW auf Dauer hingenommen wird, ist allerdings fraglich.

Ema Oprea

Title of Thesis

Comparison of Consensus Mechanisms for Blockchain

Keywords

blockchain, consensus mechanism, consensus problem

Abstract

This bachelor thesis examines consensus mechanisms for public blockchain that are relevant today. It compares them in terms of properties in the areas of security and sustainability in order to ultimately determine the best type of consensus mechanism.

Mainly, the Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus mechanisms were compared, as the rest of the consensus mechanisms turn out to be insufficiently secure.

PoW turns out to be more secure than PoS, but PoS is more sustainable than PoW, which has a high energy consumption. However, since security was determined to be the most important property, PoW is the best type of consensus mechanism considered here. However, it is questionable whether the high energy consumption of PoW will be accepted in the long-term.

Inhaltsverzeichnis

Abbildungsverzeichnis **vii**

Tabellenverzeichnis **viii**

1 Einleitung **1**

1.1 Motivation 1
1.2 Problemstellung 2
1.3 Zielsetzung 2
1.4 Methodik 3
1.5 Aufbau der Bachelorarbeit 3

2 Grundlagen der Blockchaintechnologie **4**

2.1 Blockchain 4
2.1.1 Definition 4
2.1.2 Grundlegende Technologien 4
2.1.3 Aufbau und Funktionsweise der Blockchain 7
2.2 Private, Permissioned und Public Blockchains 7

3 Konsensmechanismen **9**

3.1 Das Konsensproblem 9
3.2 The Byzantine Generals Problem 9
3.3 Byzantine Fault Tolerance (BFT) 10
3.4 Practical Byzantine Fault Tolerance (PBFT) 10
3.5 Aktuelle Blockchains und Konsensmechanismen 11
3.5.1 Proof-of-Work (PoW) 12
3.5.2 Proof-of-Stake (PoS) 15
3.5.3 Proof-of-Staked-Authority (PoSA) 15
3.5.4 Byzantine Fault Tolerant (BFT) Konsensmechanismen 16
3.5.5 Tendermint BFT 16

3.5.6 HotStuff . . . 17
3.5.7 Verifiable Byzantine Fault Tolerance (VBFT) . . . 18

4 Vergleich der verschiedenen Konsensmechanismen 19
4.1 Sicherheit . . . 19
4.1.1 Angriffe gegen PoW-Blockchains . . . 20
4.1.2 Angriffe gegen PoS-Blockchains . . . 21
4.1.3 Angriffe gegen PoSA-Blockchains . . . 22
4.1.4 Angriffe gegen Tendermint BFT-Blockchains . . . 24
4.1.5 Angriffe gegen HotStuff-Blockchains . . . 24
4.1.6 Angriffe gegen VBFT-Blockchains . . . 25
4.1.7 Vergleich Sicherheit . . . 25
4.2 Skalierbarkeit . . . 27
4.2.1 Transactions per Secound (TPS) . . . 28
4.2.2 Vergleich Skalierbarkeit . . . 29
4.3 Nachhaltigkeit . . . 29
4.3.1 Energieverbrauch . . . 29
4.3.2 Vergleich Nachhaltigkeit . . . 30
4.4 Auswertung aller Aspekte . . . 31

5 Weitere Aspekte 32
5.1 Fairness als weiterer Aspekt . . . 32
5.2 Schwierigkeiten beim Wechsel des Konsensmechanismus . . . 33

6 Fazit 35

Literaturverzeichnis 38

Selbstständigkeitserklärung 46

Abbildungsverzeichnis

2.1 Aufbau eines Hash-Baums,Quelle:[59] 5
2.2 Erstellung einer Signatur,Quelle:[59] 6

3.1 Zwei Blöcke innerhalb einer Blockchain mit PoW, Quelle:[63] 14

4.1 Double-Spending-Angriff mit Hilfe des Cloning-Angriffs, Quelle:[23] 23
4.2 Gemeinsame Angriffe bei PoW und PoS, Quelle:[58] 26
4.3 Energieverbrauch einer Blockchain mit PoW, Quelle:[2] 30

Tabellenverzeichnis

3.1 Permissionless Blockchains in Forbes Blockchain 50 2021 12

4.1 Benötigte Kontrolle des Netzwerks für einen Angriff 25

1 Einleitung

1.1 Motivation

Die Blockchain-Technologie wird von der Industrie, aber auch von der Wissenschaft als grundlegender "Game Changer" für die Dezentralisierung digitaler Infrastrukturen bezeichnet, dies reicht von der Finanzindustrie bis hin zum Internet der Dinge (IoT) und der selbstorganisierten Netzwerkorchestrierung.[67] Jack Ma, Mitgründer der ANT Group und Gründer von Alibaba sagt folgendes über sie:

> „[Blockchain] will fundamentally change financial systems in the next 10, 15 years. A blockchain technology will be applied in many areas because it is about trust, credit, security - the security of data and the privacy of data."[14]

Doch die klassische Blockchain mit dem Proof-of-Work-Verfahren hat ein Energieproblem. Für das Betreiben der Kryptowährung Bitcoin, welches dieses Verfahren verwendet, wird aktuell mehr Strom pro Jahr benötigt, als Länder wie Argentinien, Malysien und Schweden verbrauchen.[7] Kürzlich hat Elektroautobauer Tesla Zahlungen mit Bitcoin aufgrund von Umweltbedenken gestoppt, mit folgender Begründung des Tesla-Geschäftsführers Elon Musk: „Kryptowährung ist auf vielen Ebenen eine gute Idee und wir glauben an eine vielversprechende Zukunft, aber dies kann nicht zu großen Lasten der Umwelt gehen."[39] Einen Monat später verkündet Musk allerdings, dass „Tesla [...] Bitcoin sehr wahrscheinlich wieder akzeptieren [wird]", was deutlich den Kurs der Kryptowährung beeinflusst hat.[20] Dies zeigt, dass das Energieproblem etwas ist, was bei den Anlegern, abgesehen davon, dass die Aussagen von Musk stammt, auf einen Nerv trifft. Doch es existieren Alternativen.[24] In dieser Arbeit soll es darum gehen, welche das sein könnten, was die Unterschiede zwischen den verschiedenen Mechanismen sind und welcher Mechanismus letztlich der unter den betrachteten Eigenschaften die Beste ist.

1.2 Problemstellung

Gibt es einen Konsensmechanismus für die Blockchain, der im Vergleich zu anderen Mechanismen unter den hier betrachteten Eigenschaften besser ist?

1.3 Zielsetzung

Das Ziel der Bachelorarbeit ist es unter relevanten, in der Praxis eingesetzten Konsensmechanismen für die Blockchain, anhand verschiedener Eigenschaften einen Vergleich herzustellen und letztlich im Hinblick auf die ausgewählten Eigenschaften den besten Konsensmechanismus zu finden. Hierbei werden nur öffentliche Blockchains (Public Blockchains) und keine privaten Blockchains, die in der Regel nur von bekannten beziehungsweise registrierten Benutzern verwendet werden, betrachtet. Eine Begründung ist in Abschnitt 2.2 zu finden, in welchem genauer auf die unterschiedlichen Arten von Blockchains eingegangen wird.

Um das Ziel zu erreichen, werden folgende Forschungsfragen bearbeitet:

Forschungsfrage 1 Welche Arten von Konsensmechanismen in der Blockchain sind heute relevant und wo werden diese eingesetzt?

Forschungsfrage 2 In Bezug auf welche Eigenschaften können unterschiedliche Arten von Konsensmechanismen miteinander verglichen werden?

Forschungsfrage 3 Welche der Arten von Konsensmechanismen ist die X? (X= sicherste, nachhaltigste, skalierbarste)

Forschungsfrage 4 Welches ist in Hinblick auf Sicherheit, Skalierbarkeit und Nachhaltigkeit die beste Art von Konsensmechanismen?

1.4 Methodik

Für diese Arbeit ist kein praktischer Versuch sinnvoll, da die zu untersuchenden Systeme bereits in Betrieb sind und wissenschaftliche Auswertungen existieren. Um das oben genannte Ziel zu erreichen, wird daher für das Thema relevante und aktuelle Literatur betrachtet.

1.5 Aufbau der Bachelorarbeit

Zu Beginn der Arbeit wird die grundlegende Funktionsweise der Blockchain und unterschiedliche Arten der Blockchain erläuter. Danach werden die Anfänge von Konsensmechanismen allgemein bis hin zu aktuellen Konsensmechanismen betrachtet. Hierbei wird das allgemeine Konsensproblem erläutert, das Problem der byzantinischen Generäle und konkrete und relevante Konsensmechanismen, die dieses Problem lösen sollen beschrieben. Danach werden die zuvor ausgewählten Konsensmechanismen anhand von ausgewählten Eigenschaften verglichen. Zum Schluss wird im Hinblick auf diese Ergebnisse ein Konsensmechanismus bestimmt, der insgesamt der Beste unter den betrachteten Eigenschaften und Mechanismen ist. Außerdem werden noch Fairness und Schwierigkeiten beim Wechsel des Konsensmechanismus als weitere Aspekte betrachtet. Die Arbeit endet mit einem Fazit.

2 Grundlagen der Blockchaintechnologie

2.1 Blockchain

2.1.1 Definition

> „Blockchains sind verteilte elektronische Register, die mithilfe kryptografischer Verfahren und Konsensalgorithmen vor Manipulationen geschützt sind und als vertrauenswürdige Quelle von Informationen dienen. Damit können sie insbesondere zur Betrugsprävention eingesetzt werden, unter Verzicht auf zentrale Überwachungsinstanzen.“[60]

2.1.2 Grundlegende Technologien

Zur Erstellung und Funktionsfähigkeit der Datenstruktur Blockchain sind folgende, grundlegende Konzepte der Informatik, speziell der Kryptographie, nötig: Hash-Funktionen, Hash-Bäume und digitale Signaturen.[59] Diese werden nachfolgend kurz erläutert.

Hash-Funktionen

Häufig möchte man in der Informatik, auf eine möglichst einfache Art und Weise die Vollständigkeit bzw. Integrität von Daten überprüfen und Daten schnell finden können.[60] Hier kommen Hash-Funktionen ins Spiel. Sie sind mathematische Funktionen, die eine beliebig große Menge an Eingabedaten auf einen vorher definierten Bereich fixer Größe, den sogenannten Hash-Wert, abbilden.[59][60] Ändert sich etwas an der Eingabe wird in der Regel ein völlig anderer Hash-Wert generiert.[59] Dadurch kann man sofort erkennen, ob sich etwas an der Eingabe geändert hat und kann Eingaben anhand des Hash-Werts vergleichen ohne die genauen Daten kennen zu müssen.[60] Deshalb besteht die Anforderung an Hash-Funktionen, dass aus dem Hash-Wert nicht auf die Eingabe

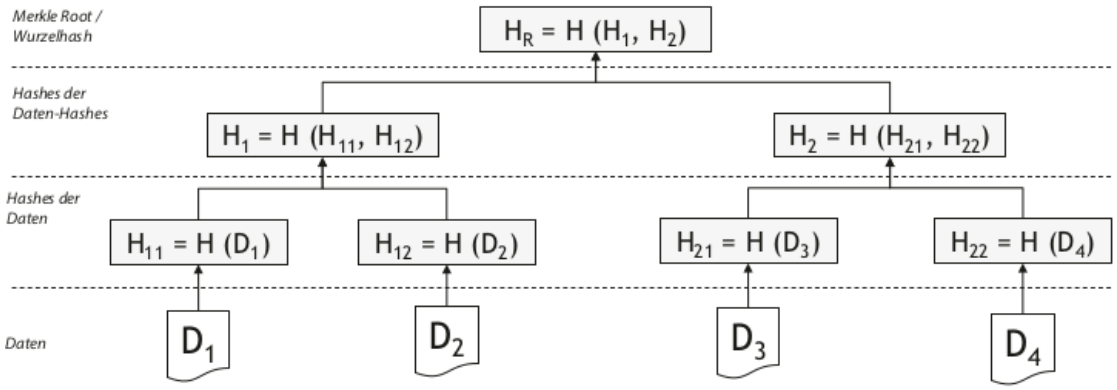

Abbildung 2.1: Aufbau eines Hash-Baums,Quelle:[59]

geschlossen werden kann.[59] Für die Blockchain werden sogenannte kryptographische Hash-Funktionen benötigt, die noch weitere Eigenschaften besitzen[59], auf die hier aber nicht weiter eingegangen wird.

Hash-Bäume

Hash-Funktionen sind ein zentraler Bestandteil der Blockchain und werden zum Aufbau bestimmter Datenstrukturen, den Hash-Bäumen oder Merkle-Bäumen, und zur Überprüfung von Transaktionen verwendet, da es in dieser Datenstruktur einfach ist das Vorhandensein bestimmter Informationen zu erkennen.[59] In "Blockchain kompakt: Grundlagen, Anwendungsoptionen und kritische Bewertung" werden Hash-Bäume beschrieben und in Abbildung 2.1. folgendermaßen dargestellt: Die Datenstruktur ist so aufgebaut, dass aus je zwei Eingaben die Hash-Werte gebildet werden. Danach werden die Hash-Werte aneinandergehängt und daraus wieder der Hash-Wert gebildet. Dies wird für alle Einträge durchgeführt und nebeneinderstehende Hash-Werte werden wieder zusammengeführt, bis ein einziger Hash-Wert übrig bleibt. Dies ist der Wurzel-Hash oder Merkle-Root.[60]

Nun kann einfach überprüft werden, ob sich in zugrundeliegenden Daten etwas geändert hat. Dazu müssen lediglich die Wurzel-Hashs überprüft werden, stimmen sie nicht überein, hat sich in dem darunterliegenden Zweig etwas geändert.[59] Darüber hinaus können die Hash-Werte des Hash-Baums dafür verwendet werden, zu überprüfen, ob ein bestimmtes Dokument im Baum vorhanden ist, ohne die genauen Inhalte zu kennen.[60] Dafür versucht man mit dem Hash-Wert des Dokuments und den übrigen Hash-Werten

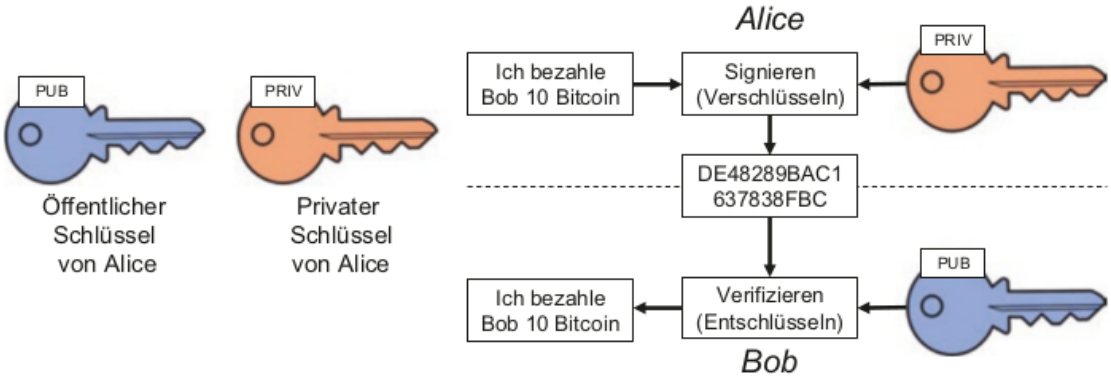

Abbildung 2.2: Erstellung einer Signatur,Quelle:[59]

einen gegebenen Wurzel-Knoten zu bilden.[59] Falls das funktioniert ist bewiesen dass das Dokument Teil der Datenstruktur ist (Merkle-Proof, Zero-Knowledge Proof).[60]

Digitale Signaturen

Eine digitale Signatur ist wie eine elektronische Unterschrift und schützt im Fall der Blockchain die Transaktionsdaten vor nicht zugelassenen Manipulationen.[60] In Abbildung 2.2 ist die Erstellung einer Signatur für Alice Nachricht zu sehen und wird in "Blockchain : Grundlagen, Anwendungsszenarien und Nutzungspotenziale" folgendermaßen erläutert: Digitale Signaturen für Nachrichten basieren auf asymmetrischer Kryptografie. Ein Benutzer hat jeweils zwei zusammengehörige Schlüssel. Einen öffentlichen, den er beliebig verteilen kann und einen privaten, der nur ihm bekannt ist und auf den nur er Zugriff hat. Alice möchte nun Bob eine Nachricht senden und Bob möchte am Ende Alice als Urheberin dieser Nachricht erkennen. Damit dies möglich ist, signiert Alice ihre Nachricht mit ihrem privaten Schlüssel. Dafür verschlüsselt sie den Hash-Wert ihrer Nachricht mit ihrem privaten Schlüssel. Anschließend sendet sie die Nachricht im Klartext und den entstandenen Wert an Bob. Bob kann nun Alice öffentlichen Schlüssel verwenden, um zu verifizieren, dass die Nachricht tatsächlich von Alice stammt. Dafür bildet Bob den Hash-Wert der Nachricht und vergleicht ihn mit dem entschlüsselten Wert. Wenn diese übereinstimmen, hat Alice die Nachricht geschrieben.[59]

2.1.3 Aufbau und Funktionsweise der Blockchain

Die Blockchain ist eine verteilte Datenbank, die von Nodes[1] im Netzwerk gemeinsam gepflegt wird.[31] Sie ist vom Aufbau her eine Kette von Datenblöcken.[60] Digitale Signaturen werden verwendet, um ihre Integrität und Sicherheit zu gewährleisten.[60] Die Integrität innerhalb der Blockchain wird gewährleistet, da minimale Änderungen weitreichende Folgen haben[60]. Falls es sich um eine korrekte Änderung handelt, „ziehen die davon betroffenen Teile der Datenstruktur die Änderungen im Konsens nach."[60] Hier kommt der Konsensmechanismus zum Einsatz. Wie diese funktionieren wird in Kapitel 3 dargelegt. Handelt es sich hingegen um einen Angriff, „wird die Blockchain den Missbrauch aufgrund klarer und verschlüsselter Eigentumsansprüche aufdecken und die Daten schützen."[60] Die Blockchain sorgt ständig für die Konsistenz ihrer Hash-Referenzen und prüft diese auf Korrektheit. Ist eine Hash-Referenz nicht gültig, zieht das eine Ungültigkeit der gesamten Datenstruktur ab diesem Punkt nach sich[60], wie dies beim Hash-Baum beschrieben wird (Abschnitt 2.1.2). Konsensmechanismen sind dafür verantwortlich, dass die Blockchain wieder in einen konsistenten Zustand kommt. Unterschiedliche Konsensmechanismen lösen dies auf unterschiedliche Art und Weise. Einige werden in Kapitel 3 genauer vorgestellt.

2.2 Private, Permissioned und Public Blockchains

Public Blockchains, auch Permissionless oder öffentliche Blockchains geannt, sind „Blockchains, bei denen alle Teilnehmer unabhängig von ihren Rechten vollen Zugriff auf das Netzwerk haben".[65] Die Teilnehmer können dem Netzwerk jederzeit beitreten oder es wieder verlassen.[55]

Es gibt allerdings auch Blockchains, die an zahlreiche Bedingungen geknüpft sind. Sie werden **Permissioned Blockchains** genannt und bei diesen ist z. B. die Anzahl der Teilnehmer bekannt und muss authentifiziert sein, allerdings ist dies für ein dezentrales Netzwerk wie das Internet, welches ein permissionless System ist, sehr ineffizient oder sogar nicht realisierbar.[55]

[1] Knoten (engl. Nodes) sind Computer, auf denen die Software zur Unterstützung der Blockchain läuft[18]

Darüber hinaus gibt es noch **Private Blockchains**. Diese werden von einer zentralen Organisation, die ebenfalls Eigentümer ist, verwaltet. Sie bestimmt „[w]er am Netzwerk teilnehmen oder Daten erfassen oder lesen darf“.[65]

Da es sich hier um drei verschiedene Umsetzungen der Blockchain handelt und alle drei unterschiedliche Voraussetzungen mit sich bringen wird sich diese Arbeit auf eine dieser Arten beschränken. Es wird im Folgenden um Public Blockchains gehen, da Private und Permissioned Blockchains für ein System wie das Internet nicht funktioniert.

Wenn von der Blockchain gesprochen wird, ohne explizit zu sagen, um welche es sich handelt, ist in dieser Arbeit die Public Blockchain gemeint. Die beschriebene Offenheit dieser Blockchain-Technologien wird durch spezielle Konsensmechanismen ermöglicht, auf die im nächsten Kapitel näher eingegangen wird.

3 Konsensmechanismen

3.1 Das Konsensproblem

Eine der größten Herausforderungen in einem dezentralen System wie der Blockchain ist die Identifizierung eines Zustands, der für alle als richtig gilt, das heißt konkret, in welcher Reihenfolge was stattfindet und welche Inhalte korrekt sind und welche nicht.[55] Einen wesentlichen Teil leistet hier der Konsensmechanismus, welcher sicherstellt, dass Transaktionen nicht doppelt durchgeführt und invalide Daten, die die Integrität der Blockchain verletzen könnten, nicht gespeichert werden.[65] Der Konsensmechanismus sorgt dafür, dass es im Netzwerk auch bei Fehlern zu einer Einigung kommt, was entscheidend für einen Vertrauensaufbau unter Nutzern in einem verteilten System ist.[53]

3.2 The Byzantine Generals Problem

Im Jahr 1982 beschrieben Leslie Lamport, Robert Shostak und Marshall Pease dieses mit dem Problem der byzantinischen Generäle (engl. The Byzantine Generals Problem). Der Ausgangspunkt ist, dass zuverlässige Computersysteme in der Lage sein müssen mit nicht vertrauenswürdigen Komponenten, die fehlerhafte Informationen an Teile des Systems übergeben, umzugehen. Dieses Szenario kann abstrakt als Gruppe von Generälen der byzantinischen Armee betrachtet werden, welche mit ihren Truppen um eine feindliche Stadt herum lagern. Über Boten müssen sich die Generäle auf einen Schlachtplan einigen. Allerdings könnte einer oder mehrere der Boten und Generäle Verräter sein. Das Problem hier ist es einen Algorithmus zu finden, der den Generälen hilft sich auf eine gemeinsame Strategie zu einigen.[61]

Je mehr Verräter "ein dezentrales System unter realen Bedingungen tolerieren kann, desto robuster ist die Lösung."[55] Die "Verräter" werden auch als **byzantinischen Fehler** (engl. Byzantine fault) bezeichnet. Es handelt sich dabei um „Fehler, bei dem die

teilnehmenden Knoten technisch einwandfrei arbeiten, der Inhalt der Nachrichten aber inkonsistent ist und manipuliert sein könnte“[65].

Das Problem der byzantinischen Generäle wird auch als Konsens- oder “agreement“-Problem bezeichnet.[38]

3.3 Byzantine Fault Tolerance (BFT)

Byzantine Fault Tolerance (BFT) ist die Eigenschaft eines Systems, widerstandsfähig gegenüber der Klasse von Fehlern, die sich aus dem Beispiel des Problems der byzantinischen Generäle, wie oben beschrieben, ergeben, d. h. es ist in der Lage trotz byzantinischer Fehler korrekt weiterzuarbeiten.[6]

3.4 Practical Byzantine Fault Tolerance (PBFT)

Als eine mögliche Lösung wird von Miguel Castro und Barbara Liskov 1999 die Practical Byzantine Fault Tolerance (PBFT) vorgestellt. Die Practical Byzantine Fault Tolerance ist ein Konsensmechanismus bei dem ein Drittel der Teilnehmer Verräter sein können und das System sich trotzdem auf die richtige Lösung einigt.[54]

Lamport, Shostak und Pease zeigten 1982 bereits in ihrem Paper, dass das folgende theoretisch korrekt ist.[61]

„Eine mathematische Herleitung dieses Problems führt zur nachstehenden Formel, mittels der die Anzahl der notwendigen Knoten im gesamten Netz unter der Annahme einer zu erwartenden Anzahl an bösartigen Knoten ermittelt werden kann“[65]:

$$n > 3 \cdot f + 1 \tag{3.1}$$

n – Anzahl der Knoten insgesamt
f – Anzahl der bösartigen Knoten

Das hier beschriebene Problem heißt **Replicated-State-Machine-Problem** und wird in “Blockchain und maschinelles Lernen : Wie das maschinelle Lernen und die Distributed-Ledger-Technologie voneinander profitieren“ von Sigurd Schacht und Carsten Lanquillon wie folgt beschrieben: Einzelne Maschinen besitzen State-Variablen, die ihren Zustand

beschreiben und auf denen nur die Operationen Lesen und Schreiben ausführbar sind. „Der Zustand der einzelnen Maschinen wird über alle beteiligten Maschinen synchronisiert“. Allerdings können sich Maschinen auch betrügerisch verhalten, indem sie einen anderen Zustand speichern und an die anderen Maschinen kommunizieren, als sie eigentlich haben. „Ziel ist es, alle Maschinen in den gleichen Status zu bringen, sodass sie konsistent sind, und zwar unter dem Gesichtspunkt der Effizienz in Bezug auf die notwendigen Kommunikationswege“[65].

Schacht und Lanquillon beschreiben den PBFT-Algorithmus folgendermaßen: Alle Knoten im Netzwerk müssen sich auf einen Zustand einigen, bei der Blockchain wäre das z. B. einer Transaktion zustimmen. Dies gelingt, indem die Mehrheit den Zustand bestätigt. Dieser gilt dann „als der aktuelle [Zustand] des gesamten Netzwerks“. „Alle Knoten kommunizieren miteinander, wobei für eine Transaktionsverifizierung ein Knoten die Führung übernimmt. Dieser Knoten ist der Prime-Node, auch Leader genannt, während die anderen die Replicas oder auch Backup-Knoten des Prime-Knoten darstellen.“[65]

Die größte Schwäche dieser Lösung ist allerdings die Skalierbarkeit, da bei mehr Teilnehmern im System auch mehr Nachrichten zwischen diesen ausgetauscht werden müssen, um einen Konsens zu erreichen, was zu einer Laufzeit führt, die quadratisch zur Anzahl der Teilnehmer steigt.[55] Daher sind diese Art von Konsensmechanismen für Public Blockchains so erst mal ungeeignet.

Doch es gibt Konsensmechanismen, wie z. B. HotStuff, die BFT mit einer anderen Kommunikationsstrategie verfolgen, so dass deutlich weniger Nachrichten ausgetauscht werden müssen und sich BFT so, in dieser abgewandelten Form, auch für Public Blockchains eignet.[16]

3.5 Aktuelle Blockchains und Konsensmechanismen

Zur Beantwortung der Forschungsfrage 1 “Welche Arten von Konsensmechanismen in der Blockchain sind heute relevant und wo werden diese eingesetzt?“ werden aktuell eingesetzte Blockchain-Lösungen, die Branche, in der sie eingesetzt werden und die dazugehörigen Konsensmechanismen ermittelt. Dazu wird die Liste “Forbes Blockchain 50“ aus dem Jahr 2021 betrachtet. In dieser haben Journalist:innen führende Unternehmen im Bereich Distributed-Ledger-Technologie vorgestellt, welche mit mindestens einer Milliarde US-Dollar bewertet werden.[14] In der Tabelle 3.1 sind Blockchain-Lösungen, die Branche

Tabelle 3.1: Permissionless Blockchains in Forbes Blockchain 50 2021

Blockchain	Anwendungsgebiete	Konsensmechanismus
Binance Chain	Finanzen	Tendermint BFT
Binance Smart Chain	Finanzen	Proof-of-Staked-Authority (PoSA)
Bitcoin	Finanzen	Proof-of-Work (PoW)
Bitcoin Cash	Finanzen	Proof-of-Work (PoW)
Ethereum	Finanzen, Erstellen und Tauschen im Bereich Business-Services, Applikationen	Proof-of-Work (PoW) (Wechsel zu Proof-of-Stake (PoS) ist geplant)
Flow	Transaktionen für Applikationen, Spiele und NFTs	HotStuff
Litecoin	Finanzen	Proof-of-Work (PoW)
MoveX (basiert auf Ontology[11])	Mobilität	Verifiable Byzantine Fault Tolerance (VBFT)
Zcash	Finanzen	Proof-of-Work (PoW)

und die verwendeten Konsensmechanismen zu sehen, bei denen es sich nicht um Private oder Permissioned Blockchains handelt und welche nicht auf einer anderen, bereits genannten Blockchain-Lösung basieren. Aktuell werden die meisten Public Blockchains im Bereich Finanzen, genauer zum Austausch von Kryptowährungen[1], eingesetzt.[40] Weitere Anwendungsgebiete sind Transaktionen für Applikationen, Spiele, Non-Fungible Tokens (NFTs) und mehr.

3.5.1 Proof-of-Work (PoW)

Proof-of-Work (PoW) ist der meistgenutzten Konsensmechanismen für Blockchains.[31] Ein zentraler Bestandteil sind kryptografische Puzzle, daher werden diese nachfolgend erläutert, bevor auf die Funktionsweise von PoW eingegangen wird.

Kryptografische Puzzles

Für die aktuelle Umsetzung der Blockchain mit Proof-of-Work werden Hash-Funktionen für kryptografische Puzzles verwendet. Diese werden in “Blockchain : Grundlagen, An-

[1] digitale Währungen, die meist ohne zentrale Einheit, wie z. B. eine Bank, bestehen

wendungsszenarien und Nutzungspotenziale“ folgendermaßen beschrieben: Ein kryptografisches Puzzle ist ein Rätsel, bei dem mit einer kryptografischen Hash-Funktion ein bestimmter Hash-Wert oder Hash-Wert aus einem vorgegebenen Wertebereich erzielt werden soll. Die Lösung soll dabei durch das Einsetzen von Werten in die Hash-Funktion, also durch das Durchprobieren von Werten (Brute Force) gefunden werden. Kryptografische Hash-Funktionen, wie z. B. die SHA-256-Funktion haben die dafür benötigten Eigenschaften, da nicht vorherbestimmt werden kann, wie ein bestimmter Hash-Wert erzielt werden kann. Es muss also der Arbeitsaufwand betrieben und Werte durchprobiert werden, um eine Lösung zu finden. Durch das Variieren des Wertebereichs, in dem sich der Hash-Wert am Ende befinden soll, kann die Schwierigkeit des Puzzles angepasst werden. Ein kryptografisches Puzzle lässt sich dazu verwenden eine zufällige Auswahl unter den Teilnehmern zu treffen, ohne dass an einer zentralen Stelle eine Auswahl getroffen wird, indem das Puzzle öffentlich gemacht wird und der erste Teilnehmer, der es löst “gewonnen“ hat.[59]

Funktionsweise von PoW

Das Grundprinzip des Proof-of-Work-Verfahrens ist, dass konkurrierende Miner[2] ein kryptografisches Puzzle lösen müssen, um den nächsten Block erstellen und der Blockchain hinzufügen zu können, um dann dafür eine Belohnung zu bekommen.[34]

Im Folgenden wird die genau Funktionsweise von Proof-of-Work, wie sie im Bitcoin Whitepaper beschrieben wird, dargestellt, da dies die am weitesten verbreitete Implementierung von PoW ist[31].

Proof-of-Work beinhaltet die Suche nach einem Wert, der wenn er gehasht wird, mit einer bestimmten Anzahl von Bits mit dem Wert null, beginnt. Die Miner versuchen diesen Wert zu finden. Der durchschnittliche Arbeitsaufwand ist exponentiell zu den Nullen, die gefunden werden müssen. Das Ergebnis kann dann durch das einmalige Ausführen der Hash-Funktion überprüft werden.

Um das kryptografische Puzzle zu lösen bzw. das Ergebnis zu finden, wird ein Nonce in dem betreffenden Block so lange inkrementiert und daraus der Hash-Wert gebildet, bis der gesuchte Hash-Wert mit der entsprechenden Anzahl an Nullen gefunden wurde. Sobald die Leistung der CPU erbracht wurde, kann der Block nicht mehr verändert

[2] Nodes, welche an der Verifikation der Transaktionen einer Blockchain mitarbeiten[31]

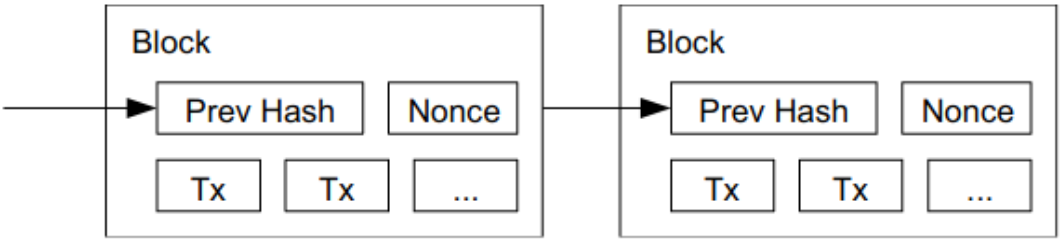

Abbildung 3.1: Zwei Blöcke innerhalb einer Blockchain mit PoW, Quelle:[63]

werden ohne die Arbeit von vorne zu beginnen, da andere Blocks angehängt werden und so die Arbeit für alle angehängten Blöcke auch wiederholt werden müsste.

Dieses Prinzip wird in Abbildung 3.1 veranschaulicht. Zu sehen ist, wie jeder Block einen Hash mit der dazugehörigen Nonce hat, der aus dem vorherigen Block gebildet wurde.

Zudem löst PoW das Problem der mehrfachen Abstimmung. Wäre das System so aufgebaut, dass eine IP-Adresse eine Stimme hat, könnte eine Partei viele IP-Adressen erstellen und so das Ergebnis verfälschen. Doch bei PoW ergibt sich eine Stimme durch eine CPU-Leistung. Dies wird dadurch sichergestellt, dass die Mehrheitsentscheidung durch die längste Kette getroffen wird, für welche gleichzeitig auch der meiste PoW-Aufwand betrieben wurde. Wenn ein Großteil der CPU-Leistung von vertrauenswürdigen Knoten gesteuert wird, wird die Blockchain mit den richtigen Einträgen am schnellsten wachsen und jede andere Kette übertreffen. Um einen älteren Block zu manipulieren, müsste ein Angreifer das aufwändige PoW-Verfahren für diesen und alle nachfolgenden Blocke wiederholen und die längste Kette der vertrauenswürdigen Knoten überbieten. Dies ist sehr unwahrscheinlich und die Chancen für einen langsamen Angreifer nehmen exponentiell ab, wenn ein weiterer Block hinzugefügt wird. Um das System in Balance zu halten und z. B. leistungsstärkere Hardware und die verschiedene Anzahl von Knoten zu berücksichtigen, wird die Schwierigkeit (Anzahl der Nullen im gesuchten Hash-Wert) angepasst um dadurch eine durchschnittliche Anzahl von neuen Blöcken pro Stunde angestrebt. Werden also neue Knoten zu schnell erzeugt, wird die Schwierigkeit erhöht.[63]

3.5.2 Proof-of-Stake (PoS)

Das Proof-of-Stake-Verfahren wird in “Blockchain und maschinelles Lernen : Wie das maschinelle Lernen und die Distributed-Ledger-Technologie voneinander profitieren“ folgendermaßen beschrieben:

Das Vertrauen unter den Teilnehmern in einem Netzwerk, das seine Konsistenz über das PoS-Verfahren sicherstellt, wird über einen Anteilsnachweis hergestellt. Wer als nächstes einen Block erstellen darf wird auf Basis der Anteile an dem Stake, bei Kryptowährungen z. B. Anzahl der Coins, auch Token genannt, die jeder Teilnehmer besitzt, entschieden. Daher muss zu Beginn jeder Teilnehmer eine gewisse Anzahl des verfügbaren Stakes besitzen, um teilzunehmen. Für die Teilnehmer muss ein Anreiz zur Beteiligung am Konsensmechanismus geschaffen werden. Daher gibt es eine Belohnung für die Erstellung eines Blocks. Dies geschieht über eine Transaktionsgebühr, die für die Validierung und die Konsensbildung erhoben wird. Diese Gebühr wird von dem jeweiligen Knoten, der die Validierung der Transaktion durchgeführt hat, einbehalten. Eine oft verwendete Implementierung ist die eines Pools von Knoten, die Validierungen durchführen. Jeder, der Token der Blockchain besitzt und einen oder mehrere davon als Einlage für das Verfahren bereitstellt, kann daran teilnehmen. Die Einlage wird hinterlegt und dient als Absicherung für ein korrektes Verhalten, da sie im Falle eines betrügerischen Verhaltens eingezogen werden kann. Zur Erstellung und Validierung eines Blocks wird zufällig ein Teilnehmer aus dem Pool der Validierer[3] ausgewählt, wobei die Wahrscheinlichkeit ausgewählt zu werden mit höheren Einlagen steigt. „Der PoS-Algorithmus ist also eigentlich ein Kautionssystem. Die hinterlegten Tokens, die jeder als Sicherheit einlegen kann, werden Stake genannt.“ Das Problem, was sich mit dem Fokus auf die Anzahl der Token ergibt, ist dass die Entscheidung darüber, ob eine Transaktion korrekt ist und ausführt werden darf auf wenige Teilnehmer beschränkt ist. Damit dies verhindert wird, werden von unterschiedlichen Implementierungen, unterschiedliche Ansätze verfolgt. [65]

3.5.3 Proof-of-Staked-Authority (PoSA)

Proof-of-Staked-Authority (PoSA) kombiniert Delegated-Proof-of-Stake (DPoS) und Proof-of-Authority (PoA).[1]

[3] Validierer sind Knoten, welche die Validierung des nächsten Blocks innerhalb einer Blockchain durchführen können.

Delegated-Proof-of-Stake (DPoS) ist ähnlich wie PoS, verfügt aber über einen Abstimmungs- und Delegationsmechanismus, der den Prozess demokratischer macht.[42]

Proof-of-Authority (PoA) ist eine Variante von PoS, bei der die Teilnehmer anstelle des Stakes ihre Identität und Reputation einsetzen.[32]

Im Whitepaper der Binance Smart Chain wird PoSA folgendermaßen beschrieben: Neue Blöcke der Blockchain werden von einer begrenzten Anzahl an Validierern erzeugt. Validierer erzeugen, nach dem Prinzip von PoA, abwechselnd neue Blöcke. Diese werden, auf Basis ihres Einsatzes, in die Menge der Validierer ein- und abgewählt.[1]

Wenn ein Validierer einen gültigen Block vorschlägt, erhält er die Transaktionsgebühren für die im Block enthaltenen Transaktionen als Belohnung.[17]

3.5.4 Byzantine Fault Tolerant (BFT) Konsensmechanismen

Eine für die Blockchain interessante Familie von State-Machine-Replikationsprotokollen ist die Familie der Byzantine Fault Tolerant (BFT) Konsensmechanismen, die, wie in Abschnitt 3.3 beschrieben, trotz böswilliger (byzantinischer) Knoten zu einem Konsens kommen können.[66] Byzantine Fault Tolerant (BFT) Konsensmechanismen gehen auf mehr als 30 Jahre Forschung zurück.[8]

Theoretisch kann aus jedem Konsensmechanismus für eine Permissioned Blockchain ein Konsensmechanismus für eine Permissionless Blockchain gemacht werden, egal ob BFT oder nicht, doch aufgrund der Gefahr für Sybill-Angriffe (siehe Abschnitt 4.1.1), wird meist PoS oder PoW hinzugenommen, um das System öffnen zu können.[25] Im restlichen Teil dieses Kapitels werden die Konsensmechanismen Tendermint BFT (Abschnitt 3.5.5), HotStuff (Abschnitt 3.5.6) und VBFT (Abschnitt 3.5.7) vorgestellt, die zur Absicherung PoS verwenden und zur Familie der BFT-Konsensmechanismen gehören.

3.5.5 Tendermint BFT

Tendermint BFT ist ein auf Byzantine Fault Tolerance (BFT)-basierender Proof-of-Stake (PoS) Konsensmechanismus und wird im Cosmos Blog folgendermaßen beschrieben: Tendermint, welches im Jahr 2014 entstand, ist der erste Proof-of-Stake (PoS) Konsensmechanismus, der von der Practical Byzantine Fault Tolerance (PBFT) abstammt. Auf BFT-basierende PoS Konsensmechanismen weisen einem Validierer pseudozufällig das

Recht zu, während eines mehrstufigen Abstimmungsprozesses neue Blöcke vorzuschlagen. Nichtsdestotrotz hängt das Commiten[4] und Finalisieren von Blöcken von einem Mehrheitsbeschluss, ein >2/3-Quorum aller Validierer, die den vorgeschlagenen Block signieren, ab. Es kann mehrere Polkas[5], dauern bis ein Block finalisiert wird. Im Kern funktioniert Tendermint wie ein rundenbasierter Abstimmungsmechanismus, welcher den Konsensmechanismus bildet. Eine Runde besteht aus drei Schritten, in welchen Validierer Blöcke vorschlagen; signalisieren, dass sie commiten wollen und die Blöcke signieren, um dann einen neuen Block zu commiten zu können. Dieser Mechanismus führt zu einem Zustandsreplikationsmaschine (State Replication Machine) für atomare Übertragungen.[8]

Tendermint läuft, ähnlich wie bei einem gewichteten Round Robin, über ein Set von Validierern, welche den nächsten Block vorschlagen.[38] Je mehr Stake, bzw. Stimmmrecht ein Validierer hat, desto mehr wird er gewichtet und proportional öfter als Leader ausgewählt.[38]

3.5.6 HotStuff

Das OntologyNetwork beschreibt HotStuff folgendermaßen: HotStuff ist ein leader-basiertes Byzantine Fault Tolerant Replikationsprotokoll. Es kann somit ebenfalls als eine Erweiterung der Practical Byzantine Fault Tolerance (PBFT) betrachtet werden. Zu Beginn wird ein Leader bestimmt, welcher am Ende seine Anfrage zur Änderung des Zustands der Blockchain an andere Knoten im Netzwerk sendet. Wenn genug andere Knoten diese Anfrage erhalten und dem Leader bestätigt haben, kann er die Anfrage als gültig erklären. [16]

HotStuff ist ähnlich wie Tendermint[45] und verwendet ebenfalls Proof-of-Stake (PoS).[13] Es kann als Erweiterung von Tendermint betrachtet werden, schreibt Ittai Abraham, im Blogpost „What is the difference between PBFT, Tendermint, SBFT and HotStuff ?“ und nennt als einen Unterschied, dass HotStuff sowohl eine lineare Komplexität, als auch Responsive [6] ist. Dafür hat HotStuff eine höhere Latenz, da es aus drei Runden, anstatt zwei Runden wie Tendermint, besteht.[45]

[4] Ein Commit ist das Freischalten von Änderungen
[5] Runden, die der Tendermint BFT-Konsensmechanismus durchläuft
[6] Responsiveness ist die spezifische Fähigkeit eines Systems oder einer Funktionseinheit, zugewiesene Aufgaben innerhalb einer bestimmten Zeit zu erledigen.[68]

3.5.7 Verifiable Byzantine Fault Tolerance (VBFT)

Verifiable Byzantine Fault Tolerance (VBFT) ist eine Kombination aus Proof-of-Stake (PoS), Verifiable Random Function (VRF) und Byzantine Fault Tolerance (BFT).[29] Bei einer Blockchain, die VBFT als Konsensmechanismus verwendet, wird eine Menge von Block-Herstellern, Validierern auf Basis von Verifiable Random Functions (VRF)[7] ausgewählt.[69] Diese Zufälligkeit und PoS bieten Schutz vor Angriffen.[30] Der finale Status der Blockchain wird mit Hilfe von BFT hergestellt.[30]

[7] VRFs generieren Zufallszahlen, welche z. B. verwendet werden, um für jede neue Runde von VBFT Validierer zu bestimmen.[29]

4 Vergleich der verschiedenen Konsensmechanismen

Zur Beantwortung der Forschungsfrage 2 “In Bezug auf welche Eigenschaften können unterschiedliche Arten von Konsensmechanismen miteinander verglichen werden“ werden zunächst Kategorien definiert, in denen sich die jeweiligen Eigenschaften befinden können. Diese sind: Sicherheit, Skalierbarkeit und Nachhaltigkeit. Wie diese genauer definiert sind und wieso sie ausgewählt wurden ist den entsprechenden Abschnitten zu entnehmen. In diesen Abschnitten werden dann auch, die in Abschnitt 3.5 für relevant befundenen Konsensmechanismen auf diese Eigenschaften hin untersucht.

4.1 Sicherheit

Der Aspekt Sicherheit wird betrachtet, da Blockchains dazu da sind, um „Transaktionen zwischen Parteien in vertrauenswürdiger Art und Weise dezentral zu speichern und nachvollziehbar zu machen“.[59] In dieser Arbeit werden Public Blockchains betrachtet, d. h. die Teilnehmer kennen sich nicht und können dem Netzwerk jederzeit beitreten oder es wieder verlassen. Wäre die Blockchain nicht sicher und jeder könnten z. B. beliebige, vom Netzwerk nicht zugelassene Änderungen an der Blockchain vornehmen, würde das ganze Prinzip hinter der Blockchain keinen Sinn ergeben und sie wäre ungeeignet als Grundlage für Währungen und andere Anwendungsfälle, die es heute schon gibt.

Verschiedene Angriffe gegen die Blockchain und die jeweiligen Konsensmechanismen sind möglich. Betrachtet werden im Folgenden nur Angriffe, die für die Sicherheit des jeweiligen Konzepts relevant sind. Das sind nicht Angriffe, die aufgrund von Implementierungs- oder Konfigurationsfehlern möglich sind, auch Insider-Angriffe werden nicht betrachtet. Der Grund wieso diese nicht betrachtet werden ist, dass die Angriffe, die dann möglich sind, nichts mit dem jeweiligen Konzept hinter dem Konsensmechanismus zu tun haben und somit für einen Vergleich irrelevant sind.

Zudem werden DoS-Angriffe, die nichts mit dem Konzept zu tun haben, sondern bei jeder Blockchain durchführbar sind, wie z. B. das Überfluten von Knoten mit Daten, um so den Betrieb der Blockchain zu stören[41], hier ebenfalls nicht genauer betrachtet.

4.1.1 Angriffe gegen PoW-Blockchains

In einem Blockchain-Netzwerk, welches Proof-of-Work verwendet, muss ein Angreifer mehr als 50% der Rechenpower im Netzwerk kontrollieren, um einen **51%-Angriff** durchzuführen und Transaktionen zu fälschen.[31] Ein 51%-Angriff ist möglich, wenn 51% der Rechenpower des Netzwerks durch einen Miner oder einen Mining Pool kontrolliert wird, da dann Blöcke mit gefälschten Transaktionen erstellen oder Transaktionen anderer Teilnehmer in Netzwerk als ungültig erklärt werden können.[35] Bei großen Netzwerken ist der Angriff allerdings technisch schon kaum zu stemmen.[34] Dennoch ist er möglich und bei kleineren Netzwerken entsprechend einfacher auszuführen. Eine Variante des 51%-Angriffs ist der **Sybil-Angriff**, bei dem nicht vertrauenswürdige Knoten versuchen die vertrauenswürdigen zu überstimmen, indem sie gefälschte Identitäten erstellen.[37]

Es existiert ein **Denial-of-Service (DoS)-Angriff**, der schon mit 25% der Rechenpower möglich ist.[52] Der Angriff, der dies ermöglicht, nennt sich **Selfish Mining** und wurde von Ittay Eyal und Emin Gün Sirer in "Majority is not Enough: Bitcoin Mining is Vulnerable" folgendermaßen beschrieben: Miner behalten neu entdeckte Blöcke für sich und führen damit wissentlich einen Fork[1] durch. Die neuen Blöcke werden später veröffentlicht, was dazu führt, dass die vertrauenswürdigen Miner ihre Blöcke aufgeben und die Arbeit an der Blockchain des Angreifers weiter durchführen, da die Blockchain des Angreifers wahrscheinlich die längste Kette ist und somit die richtige zu sein scheint. Ittay Eyal und Emin Gün Sirer konnten zeigen, dass der Angreifer dadurch einen Vorteil hat, da er, im Gegensatz zu den anderen Teilnehmern, größere Gewinne aufgrund weniger verschwendeter Energie macht.[57]

Zudem kann **Selfish Mining** mit der Zeit zu Mining Pools führen, welche immer größer werden, da sich Miner dem Angreifer, aufgrund der Länge seiner Kette, anschließen.[36] Sie können nicht erkennen, dass ihre Aktionen durch den Angreifer ausgenutzt werden können. Wenn der Mining Pool 51% der Rechenpower erreicht, kann er vom Angreifer für einen 51%-Angriff ausgenutzt werden können.[36]

[1] Spaltung der Blockchain, wodurch dann zwei Versionen der Blockchain existieren[34]

4.1.2 Angriffe gegen PoS-Blockchains

In einem Blockchain-Netzwerk, welches Proof-of-Stake verwendet, muss ein Angreifer mindestens 51% des Stakes (z. B. der Währung) kontrollieren, um einen 51%-Angriff durchzuführen und eine Transaktion zu fälschen.[52]

Ein möglicher Angriff gegen PoS-Netzwerke ist der **Nothing-at-Stake-Angriff**, der auf "heise online" folgendermaßen beschrieben wird: Wenn es zu einer Spaltung der Blockchain (Fork) kommt, halten Validierer ihren Einsatz in beiden Varianten der Blockchain, falls sie diesen vor dem Fork bereits gesetzt haben und können sich dadurch an beiden Blockchains gleichzeitig beteiligen. Daher wird der Angriff übersetzt auch "nichts steht auf dem Spiel"genannt, da Angreifer versuchen können zu betrügen, ohne einen Schaden zu erleiden, wenn am Ende eine Variante der Blockchain gewinnt. [34]

Dieses Problem macht es für eine PoS-Blockchain in einigen Fällen schwierig, wenn nicht sogar unmöglich Forks aufzulösen[26], genauer gesagt, zu wissen, welche Blockchain die aktuell Richtige ist. Zudem verursachen **Double-Spending-Angriffe** im Falle einer Fork-Auflösung viel weniger Kosten.[26] Was genau ein Double-Spending-Angriff ist, wird in Abschnitt 4.1.3 genauer beschrieben.

Ein weiterer Angriff ist der **Long-Range-Angriff**, der vom Ethereum-Mitgründer Vitalik Buterin folgendermaßen beschrieben wird: Angenommen ein Angreifer hat 1% des Stakes beim oder kurz nach dem Genesis-Block[2]. Dann erstellt der Angreifer eine eigenen Kette der Blockchain und fängt an, an ihr zu arbeiten. Auch wenn der Angreifer nur 1% der Zeit ausgewählt wird, um einen neuen Block zu produzieren, kann er ohne große Mühe 100 Mal mehr Blöcke produzieren und so die längste Kette erstellen.[21]

Bei PoS können so viele Blöcke ohne große Mühe produziert werden, da die Rechenkosten für die Erstellung eines Blocks in der Regel trivial sind und kein Mining nötig ist.[26]

Aktuell gibt es keine fundamentale Lösung, die den Long-Range-Angriff verhindert.[64][69]

Ein Angriff, der ähnlich zum Long-Range Angriff ist, nennt sich **Short-Range-Angriff**. Ein Beispiel dafür ist der **Bribe-Angriff**, welcher ähnlich wie der Long-Range Angriff durchgeführt wird, allerdings beginnt der Angreifer nicht wie beim Long-Range-Angriff ab dem Genesis-Block an seiner eigenen Blockchain zu arbeiten, sondern ab einem späteren Block innerhalb der Blockchain.[41]

[2] erster Block innerhalb einer Blockchain

Zudem gibt es eine Klasse von Angriffen, die sich "**Stake Grinding**"nennt. Dabei manipuliert ein Angreifer die Zufälligkeit innerhalb der Blockchain, um dadurch für sich die Wahrscheinlichkeit zu erhöhen, den nächsten Block generieren zu können.[33]

Ein weiterer Angriff ist der **Coin-Age-Accumulation-Angriff**, welcher im Artikel "Robust Proof of Stake: A New Consensus Protocol for Sustainable Blockchain Systems" von Aiya Li, Xianhua Wei und Zhou He folgendermaßen beschrieben wird: In den frühen Versionen war die Schwierigkeit des Minings nicht nur mit dem aktuellen Anteil des Stakes, sondern auch mit dessen Haltezeit verbunden. In diesem Fall können Angreifer ihre Münzen halten und mit der Zeit einen immer größer werdenden Vorteil haben und so leichter die benötigten Anforderungen erfüllen, um den nächsten Block generieren zu können. Wodurch sie letztlich unter Umständen einen 51%-Angriff durchführen und so das ganze Netzwerk kontrollieren können.[49]

Ein Angreifer kann zudem einen **Precomputing-Angriff** durchführen, wenn er ausgewählt wurde, um als nächstes einen Block zu erstellen. Er beeinflusst den Hash dieses Blocks dann so, dass er beim Generieren des nächsten Blocks einen Vorteil gegenüber den anderen Teilnehmern hat und diesen ebenfalls erstellen kann.[58]

Darüber hinaus sind auch bei PoS Sybil- und Denial-of-Service-Angriffe möglich.[41]

Projekte haben allerdings schon Abwehrmechanismen entwickelt, wie z. B. Ethereum, welches das "Casper"-Protokoll entwickelt hat, das böswillige Teilnehmer bestraft, indem es ihre eingesetzte Kryptowährung konfisziert und sie in Zukunft von der Teilnahme ausgeschlossen werden.[31] Dies wird **Slashing** genannt. Eine weitere Möglichkeit ist eine „[erzwungene] Verzögerung zwischen der Einräumung des Rechts, neue Blöcke anzufertigen, und der Möglichkeit, den eigenen Einsatz, der dabei benötigt wird, wieder zurückzuerhalten. Vereinfacht gesagt ist die Idee, dass bösartiges Verhalten so rechtzeitig auffällt und bestraft werden kann."[34]

4.1.3 Angriffe gegen PoSA-Blockchains

In einem Blockchain-Netzwerk, welches Proof-of-Staked-Authority verwendet, muss ein Angreifer mindestens 1/3 der Validierer kontrollieren, um einen Cloning-Angriff durchzuführen. Der **Cloning-Angriff** wird in "The Attack of the Clones Against Proof-of-Authority" von Parinya Ekparinya, Vincent Gramoli und Guillaume Jourjon folgendermaßen vorgestellt: Ein bösartiger Validierer dupliziert (engl. clone) seinen Knoten und

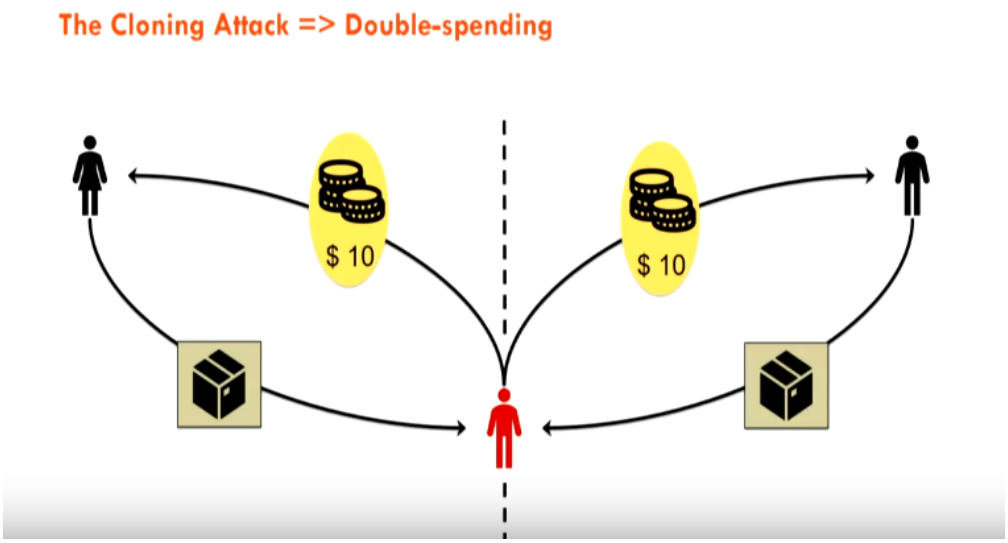

Abbildung 4.1: Double-Spending-Angriff mit Hilfe des Cloning-Angriffs, Quelle:[23]

erstellt somit zwei oder mehr Instanzen mit dem selben kryptographischen Schlüssel. Nun erstellt der Angreifer zwei Instanzen der selben Blockchain mit jeweils Teilen der duplizierten Knoten, z. B. indem er Routen und somit den Netzwerkverkehr zwischen den beiden Gruppen manipuliert. Beide Gruppen glauben nun, dass sie eine ehrliche Mehrheit bilden. Nun kann der Angreifer einen **Double-Spending-Angriff** durchführen, indem er z. B. wie in Abbildung 4.1 zu sehen ist, in beide Netze Transaktionen sendet, die auf den gleichen Token zurückzuführen sind. Beide Netze denken, sie seinen die einzigen, legitimen Partitionen und werden beide die Transaktion akzeptieren und entsprechend handeln. Der Angriff ist damit erfolgreich. Danach kann der Angreifer eine Partition vernachlässigen und es wird mit der längeren Blockchain der beiden weitergearbeitet.[56]

Die Binance Smart Chain führt zudem Strafen ein, wie im Whitepaper beschrieben wird. Dazu gehört z. B. Slashing, bei dem der Angreifer nicht mehr als Validierer teilnehmen kann und etwas vom Stake abgezogen wird, wenn er sich schädlich verhält. Gemeldet wird der Angreifer von anderen Teilnehmern, die daraufhin eine Belohnung bekommen, allerdings auch etwas im Voraus auslegen müssen, um jemanden zu melden. Der Hersteller empfiehlt darauf zu warten, dass ein Block von mehr als 2/3*N+1 verschiedenen Validierern signiert wurde, dann würde ein Angreifer mehr als 1/2*N+1 der Validierer einnehmen müssen, um die Blockchain anzugreifen.[1]

4.1.4 Angriffe gegen Tendermint BFT-Blockchains

Ein Blockchain-Netzwerk, welches Tendermint BFT verwendet, kann mit bis zu 1/3 Fehlern umgehen, diese können beliebiges Verhalten, wie z. B. Ausfälle, aber auch böswillige Angriffe beinhalten.[8] In der Tendermint-Dokumentation wird dies folgendermaßen genauer erläutert: Wenn weniger als 1/3 der Validierer betrügerisch oder fehlerhaft sind, garantiert Tendermint Sicherheit, genauer bedeutet das, dass Validierer Blöcke, die sich widersprechen, nicht auf der selben Höhe commiten können. Dies wird durch einige Regeln und dazugehörige Locks durchgesetzt. Sobald ein Validierer einen Block precommited, wird er für diesen Block festgesetzt. Dann muss er für diesen Block eine Vorentscheidung treffen. Die Festsetzung auf diesen Block für den Validierer kann nur aufgehoben werden und er kann erst für einen neuen Block eine Vorentscheidung treffen, wenn ein Polka für den Block in einer späteren Entscheidungsrunde getroffen wird. Ein Polka findet dann statt, wenn mehr als 2/3 der Validierer eine Vorentscheidung für einen Block treffen. Jeder Pre-Commit muss durch einen Polka (siehe Abschnitt 3.5.5) in der selben Runde bestätigt werden.[44]

Zudem forkt Tendermint bei Asynchronität nicht, wenn mehr als 1/3 der Prozesse sich fehlerhaft oder böswillig verhalten und kommt zum Stillstand bis eine Mehrheit, z. B. mehr als 2/3 der Validierer zu einem Konsens kommen - Sicherheit wird vor Betriebsfähigkeit (engl. Liveness) gestellt.[38]

4.1.5 Angriffe gegen HotStuff-Blockchains

Ein Blockchain-Netzwerk, welches HotStuff verwendet, kann mit weniger als 1/3 böswilligen Validierern umgehen, auch im asynchronen Modell.[51][50]

Es besteht die Gefahr, dass zu viele byzantinische Knoten in einem Cluster enthalten sind, was das Einfügen gefälschter Transaktionen oder das Zurückhalten von Informationen ermöglicht, was wiederum das Erstellen neuer Blöcke verhindert, wie in “Flow: Separating Consensus and Compute – Block Formation and Execution“ von Alexander Hentschel, Yahya Hassanzadeh-Nazarabadi, Ramtin Seraj, Dieter Shirley und Layne Lafrance beschrieben wird. Allerdings wird auch genannt, dass die Blockchain Flow dies durch verschiedene Mechanismen erschwert.[50]

Tabelle 4.1: Benötigte Kontrolle des Netzwerks für einen Angriff

Konsens-mechanismus	PoW	PoS	PoSA	Tendermint	HotStuff	VBFT
Benötigter Prozentsatz	>50% der Rechen-power	>50% des Stakes	>1/3 der Va-lidierer	>1/3 der Validierer	>1/3 der Va-lidierer	>1/3 der Va-lidierer

4.1.6 Angriffe gegen VBFT-Blockchains

In einem Blockchain-Netzwerk, welches Verifiable Byzantine Fault Tolerance (VBFT) verwendet, muss ein Angreifer mindestens 1/3 der Knoten, die an der Konsensfindung beteiligt sind, kontrollieren, um die Blockchain anzugreifen.[29]

In "All roads lead to Rome: Many ways to double spend your cryptocurrency" von Zhiniang Peng und Yuki Chen wird zudem ein Angriff beschrieben, mit dem ein Angreifer den selben VRF-Wert für beliebige Blockdaten generieren kann, wenn er einen privaten Schlüssel hat, der 0 ist. Dadurch ist der generierte VRF-Wert nicht mehr zufällig und der Angreifer kann dies nutzen, um die "Zufälligkeit" des Konsensmechanismus und damit der Generierung neuer Blöcke für eine lange Zeit zu kontrollieren.[69]

Auch hier ist der in Abschnitt 4.1.2 beschriebene, Long-Range-Angriff möglich, allerdings wird dieser erschwert, indem durch die Verifiable Random Functions (VRF) Validierer ausgewählt werden und so die Wahrscheinlichkeit, dass der Angreifer, wenn er nicht einen großen Teil des Stakes hält, eine priorisierte Rolle für seinen Fork aufrechterhalten kann, sehr gering ist.[64]

4.1.7 Vergleich Sicherheit

In der Tabelle 4.1 ist dargestellt wie viel Prozent eines Netzwerks ein Angreifer kontrollieren muss, um die Integrität der Blockchain anzugreifen. Deutlich zu sehen ist, dass die Konsensmechanismen Proof-of-Work und Proof-of-Stake mit jeweils mehr als 50% herausstechen, daher werde ich im Folgenden auf diese beiden eingehen, um Forschungsfrage 3 "Welche der Arten von Konsensmechanismen ist die X? (X= **sicherste**, nachhaltigste, skalierbarste)" zu beantworten. PoW ist sicherer als PoS[31] und damit der sicherste

	Vulnerability	
Attack type	PoW	PoS
Short range attack (e.g., bribe)	−	+
Long range attack	−	+
Coin age accumulation attack	−	maybe[4]
Precomputing attack	−	+
Denial of service	+	+
Sybil attack	+	+
Selfish mining	maybe[5]	−

Abbildung 4.2: Gemeinsame Angriffe bei PoW und PoS, Quelle:[58]

Konsensmechanismus in diesem Vergleich. Im Folgenden wird begründet wieso dies der Fall ist.

Ein Vorteil von PoW ist, dass es für viele Kryptowährungen verwendet wird und deshalb bereits über eine längere Zeit angegriffen und getestet wurde.[31] Dennoch gibt es mehr mögliche Angriffe auf eine Blockchain, die PoS verwendet, wie in Abbildung 4.2 zu sehen ist.

Hugo Nguyen beschreibt im Blogeintrag "Work is Timeless, Stake is Not" wie der hohe Energieverbrauch von PoW die Blöcke der Blockchain schützt folgendermaßen: Der Wert eines jeden Blocks, bei Kryptowährungen z. B., wird vor allem durch den hohen Energieaufwand, der zur Herstellung jedes Blocks verwendet wird, sichergestellt. Allerdings werden auch rückblickend alle Blöcke gesichert, da es nicht möglich ist vorherige Blöcke zu widerrufen, ohne alle nachfolgenden Blöcke zurückzuziehen und für den veränderten und die zurückgezogenen Blöcke den Energieaufwand erneut zu betreiben. Jeder neue Block "begräbt" sozusagen die vorherigen Blöcke unter sich.[48]

Veranschaulicht wird das Ganze von Tuur Demeester im Blogeintrag "Critique of Buterin's "A Proof of Stake Design Philosophy"" mit dem Beispiel eines Mannes, der im Mai 2010 für 10.000 BTC (Stand 22.09.21: 360.288.219,90 Euro) eine Pizza gekauft hat ('Pizza Man') und diese Transaktion nun rückgängig machen möchte. Um dies zu erreichen, müsste er es schaffen 100% der Bitcoin-Mining-Anlagen über 200 Tage (oder einen kleineren Prozentsatz, der über 51% liegt für eine längere Zeit) zu infiltrieren und kontrollieren, um die Blockchain mit gültigem PoW bis zu seiner Transaktion zurückzudrehen. Neben der milliardenschweren Anschaffungskosten für die Hardware, würde das

betreiben des Bitcoin-Netzwerks für 200 Tage über 700 Millionen US-Dollar (7.5 TWh bei 10 Cent/KWh) kosten.[9]

Angriffe gegen PoS, die dieses Problem ebenfalls deutlich machen, sind Long-Range-Angriffe, welche zeigen, dass PoS nicht in der Lage ist die Vergangenheit abzusichern und auf lange Sicht die Integrität der Blockchain zu gewährleisten, wie es bei PoW der Fall ist.[48]

Proof-of-Stake versucht verschiedene Angriffe zu verhindern, indem es einen Betrug für Teilnehmer unattraktiv macht. Auch wenn es schwierig, und bei Kryptowährungen teuer ist, 51% des Stakes zu kontrollieren, wäre es in der Regel nicht im Interesse des Angreifers ein Blockchain-Netzwerk anzugreifen, bei dem er den größten Teil des Stakes hält, da es bei einem Angriff zu einem Wertverlust kommen kann, unter dem der Angreifer dann selbst leidet.[35] Dies ist z. B. der Fall, wenn es sich um eine Kryptowährung handelt, bei der ein Angreifer sich einen größeren Teil der Währung zusichern möchte, als ihm zusteht. Falls der Angreifer kein Interesse an dem hat, was die Blockchain hält, ist auch ein reiner Reputationsschaden denkbar, dann würde dieses Argument nicht gelten.

Allerdings wurden vermutlich noch nicht alle potenziellen Angriffe gegen Konsensmechanismen entdeckt. Ein Beispiel hierfür ist, dass lange angenommen wurde, dass bei Proof-of-Work 51% des Netzwerks von einem Angreifer kontrolliert werden müssen, um es anzugreifen, allerdings stellte sich später heraus, dass auch die Hälfte ausreichend ist.[52]

Zudem sollte beachtete werden, dass Network Partitioning, wie es in Abschnitt 4.1.3 beim Double-Spending-Angriff erwähnt wird, ebenfalls bei PoW und PoS möglich ist. Ein Angreifer kann Network Partitioning nutzen, um Mehrheitsverhätnisse zu ändern und so mit faktisch weniger als 50% Kontrolle über das Netzwerk einen Angriff durchzuführen.

4.2 Skalierbarkeit

Skalierbarkeit ist ein wichtiger Aspekt für die Public Blockchain. Begründet wird dies durch die möglichen Anwendungsszenarien, z. B. als digitale Währung. Deutlich wird der Bedarf nach skalierbaren Lösungen, wenn man einen Vergleich zwischen einer digitalen Währung und anderen, nicht dezentralen Lösungen zieht. Bitcoin z. B. verarbeitet aktuell 4,6 Transaktionen pro Sekunde, Visa im Durchschnitt 1700.[5]

Ist bei Public Blockchains von Skalierbarkeit die Rede, dann ist nicht die Anzahl der teilnehmenden Computer gemeint, sondern die „Skalierbarkeit in Bezug auf die Geschwindigkeit pro Transaktion“.[65]

4.2.1 Transactions per Secound (TPS)

Eine häufig verwendete Metrik ist dabei Transactions per Secound (TPS), die Transaktionen, die vom Blockchain-Netzwerk pro Sekunde ausgeführt werden können. Frank Edwood beschreibt diese in einem Blogpost folgendermaßen: Sie setzt sich zusammen aus der Block Size und der Block Generation Speed. Die Block Size ist die Größe der jeweiligen Datenblöcke, aus der die Blockchain besteht. Diese beinhalten die Transaktionsdaten und je mehr Daten in die Blöcke passen, desto mehr Transaktionen können mit einem neuen Block abgewickelt werden. Die Block Generation Speed ist die Geschwindigkeit in der ein neuer Block zur Blockchain hinzugefügt wird. Diese beiden Faktoren haben großen Einfluss auf die Geschwindigkeit und die Kapazität des Blockchain-Netzwerks.[4]

Die Frage, die sich als nächstes stellt ist inwiefern der Konsensmechanismus Einfluss auf die TPS hat. Sowohl Bitcoin als, auch auch Bitcoin Cash verwenden Proof-of-Work. Allerdings kommt Bitcoin auf 3-7 TPS und Bitcoin Cash auf 61 TPS.[10] Der Grund hierfür ist, dass Bitcoin Cash im Jahr 2017, als es sich von Bitcoin durch einen Hard Fork[3] abspaltete, die Block Size erhöht hat, von 1 MB, wie bei Bitcoin, auf 8 MB und später auf 32 MB.[4] Auch Ethereum verwendet Proof-of-Work und hat mit 15-25 TPS einen höheren Wert als Bitcoin.[10] Der Grund hierfür liegt unter Anderem in der höheren Block Generation Speed, welche bei Bitcoin gedrosselt ist, indem festgelegt wird, dass alle 10 Minuten ein neuer Block generiert werden soll.[22] Bei Ethereum können mehr Blöcke in 10 Minuten generiert werden und es hat weitere Optimierungen implementiert, unter Anderem einen nicht so speicherintensiven Hash-Algorithmus.[46]

Daraus ergibt sich, dass der Konsensmechanismus allgemein nicht über Metriken, wie TPS oder Block Generation Speed, untersucht werden kann, sondern die einzelnen Parameter, sowohl der Blockchain (z. B. Block Size) und des Konsensmechanismus (z. B. Hash-Algorithmus) entscheidend für die Skalierbarkeit des Blockchain-Netzwerks sind.

[3] Der größte Unterschied zu den Forks, über die hier bisher gesprochen wurde, ist, dass ein Hard Fork nicht rückgängig gemacht werden kann und unabhängig vom System, von welchem er sich abgespaltet hat, existiert.[15]

4.2.2 Vergleich Skalierbarkeit

Um die Forschungsfrage 3 „Welche der Arten von Konsensmechanismen ist die X? (X= sicherste, nachhaltigste, **skalierbarste**)“ zu beantworten muss eine Normalisierung der Konsensmechanismen erfolgen. Dies bedeutet, dass jeder Mechanismus auf eine gemeinsamen Nenner gebracht werden muss, um sie im Bezug auf Skalierbarkeit vergleichbar zu machen. Dann erst könnten Metriken, wie z. B. TPS eine Aussagekraft über die verwendeten Konsensmechanismen haben. Dies ist allerdings nicht im Rahmen dieser Abschlussarbeit zu beantworten.

4.3 Nachhaltigkeit

Der Aspekt Nachhaltigkeit wird betrachtet, da aktuell eingesetzte Konsensmechanismen viel Energie verbrauchen und somit eine starke Belastung für die Umwelt sind.[31] Zudem ist der Aspekt allgemein relevant, da wir uns in einer Klimakrise befinden, die aufgehalten werden kann, indem unter Anderem die Weltweite CO_2-Emission stark reduziert wird.[62]

Um die Nachhaltigkeit der verschiedenen Blockchains zu betrachten, wird ihr jeweiliger Energieverbrauch, soweit dies möglich ist, ermittelt. Bei den meisten betrachteten Blockchains und ihren Konsensmechanismen werden als Sicherung entweder Proof-of-Work oder eine Variante von Proof-of-Stake verwendet, wie in Kapitel 3 beschrieben wird. Daher wird sich dieser Teil des Vergleichs, mit Hinblick auf Forschungsfrage 4, auf diese beiden Konsensmechanismen, die sich auch als die sichersten Konsensmechanismen rausstellen, konzentrieren.

4.3.1 Energieverbrauch

Der Energieverbrauch von Proof-of-Work ist hoch und stellt eine starke Belastung für die Umwelt da.[31] Es ist PoW, das bei einer entsprechenden Blockchain große Mengen an Energie benötigt, da die Transaktionen der Blockchain selbst nicht besonders rechenintensiv sind.[12] Wissenschaftlich wurde der Energieverbrauch bereits untersucht.[7] Er liegt aktuell pro Jahr für Bitcoin z. B. bei 166.76 TWh, was vergleichbar mit dem Energieverbrauch von Polen ist.[2] Der Grund für diesen hohen Energieverbrauch ist, dass mehrere Millionen Miner auf der ganzen Welt alle zehn Minuten darum konkurrieren, als

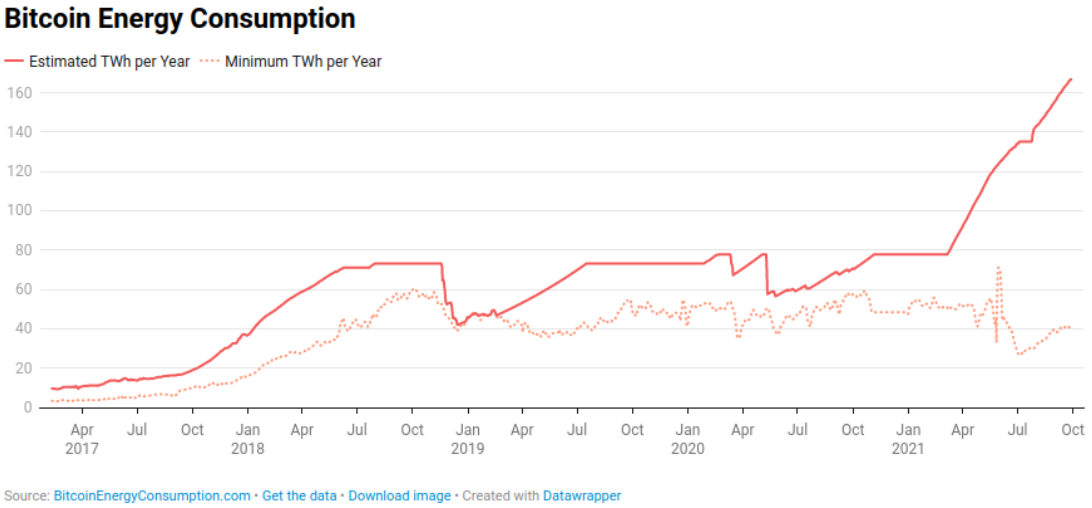

Abbildung 4.3: Energieverbrauch einer Blockchain mit PoW, Quelle:[2]

erste den gesuchten Wert zu erwürfeln, um den nächsten Block generieren zu dürfen und dafür dann aktuell ungefähr 150.000 Euro zu bekommen.[34] Zudem wird das mathematische Puzzle, welches die Miner lösen müssen, bei mehr Teilnehmern schwieriger, um die Blockzeit von 10 Minuten zu erhalten, was dazu führt, dass mehr Rechenleistung für ein Puzzle aufgewendet werden muss.[22] Beschleunigt wird diese Dynamik auch dadurch, dass mehr Menschen in Bitcoin investieren.[3] Zu sehen ist dieser steigende Energieverbrauch über die Zeit in Abbildung 4.3. Letztlich wird 99,9% der aufgewendeten Energie verschwendet, da das Ergebnis verworfen wird, wenn der Miner nicht der schnellste war.[3]

Bei Blockchains, die Proof-of-Stake verwendet existiert der gesamte 'Stake' bereits[31], weshalb es keinen Mining-Prozess gibt, was weniger Rechenleistung und damit weniger Energieverbrauch bedeutet.[34] Zudem fällt der Wettbewerb, um die Erzeugung des nächsten Blocks weg, wodurch jede Maschine an einem Problem zur Zeit arbeiten kann.[3] Allerdings existieren noch keine genauen Zahlen aus der Wissenschaft zum Energieverbrauch von PoS.[34]

4.3.2 Vergleich Nachhaltigkeit

Somit ist die Antwort auf die Forschungsfrage 3 „Welche der Arten von Konsensmechanismen ist die X? (X= sicherste, **nachhaltigste**, skalierbarste)“ Proof-of-Stake. PoW hat

einen hohen Energieverbrauch und stellt eine stärkere Belastung für die Umwelt da als PoS.[31]

Das Cosmos-Netzwerk schätzt den Energieverbrauch seiner PoS-basierten Blockchain über ein Jahr gerechnet auf weniger als Bitcoin und Ethereum an einem Tag zusammen verbrauchen (0.00046647 TWh). Selbst 100.000 Cosmos-Blockchains würden nach ihrer Rechnung zusammen weniger Energie verbrauchen als Ethereum pro Jahr (46.647 TWh).[47] Allerdings beruht dies auf einer Schätzung des Herstellers selbst und muss nochmal wissenschaftlich überprüft werden.

4.4 Auswertung aller Aspekte

Um die Forschungsfrage 4 „Welches ist in Hinblick auf Sicherheit, Skalierbarkeit und Nachhaltigkeit die beste Art von Konsensmechanismen?“ zu beantworten, müssen zunächst die verschiedenen Kategorien priorisiert werden. Da im Rahmen dieser Arbeit keine Aussage über die Skalierbarkeit getroffen werden kann, bleiben die Kategorien Sicherheit und Nachhaltigkeit übrig. Sicherheit ist für die Blockchain wichtiger als Nachhaltigkeit, da die Blockchain ohne Sicherheit nicht als das dienen kann, was sie nach Definition ist, nämlich als „vor Manipulationen geschützt [...] und als vertrauenswürdige Quelle von Informationen“.[60] Ebenso ist Nachhaltigkeit ein wichtiger Aspekt, allerdings gilt er zur Zeit als noch nicht entschieden. Bewiesen wird dies dadurch, dass Blockchains mit erheblicher Umweltbelastung noch im Einsatz sind. Demnach ist im Hinblick auf die hier gewählten Kriterien Proof-of-Work die beste Art von Konsensmechanismus. Doch der Nachhaltigkeitsaspekt könnte aufgrund zu erreichender Klimaziele[62] immer wichtiger werden und so Proof-of-Work von der Gesellschaft nicht mehr toleriert werden. Zu sehen ist diese Entwicklung in der medialen Berichterstattung, in der die Umweltbelastung von PoW immer wieder kritisiert wird.[31] So wird das, was PoW so sicher macht, der erhebliche Aufwand der investiert werden muss, zu einem großen Nachteil im Bezug auf den Energieverbrauch. Proof-of-Stake gilt als der „designierter Nachfolger“ von PoW und soll dessen Nachteile, vor allem das Problem bezüglich des hohen Energieverbrauchs, ausgleichen.[34] Es gibt viele Bemühungen PoS sicherer zu machen. Einige werden in Abschnitt 4.1.2 beschrieben, allerdings ist es immer noch unsicherer als PoW. Mit der Zeit wird sich herausstellen, welche Implementierung langfristig die bessere ist.[34]

5 Weitere Aspekte

5.1 Fairness als weiterer Aspekt

Mit Fairness ist hier nicht Fairness, wie z. B. bei Protokollen gemeint, sondern ein gleichberechtigter Zugang und fairer Wettbewerb um den nächsten Block einer Blockchain. Der Aspekt Fairness wird hier betrachtet, da ohne diesen die Gefahr für eine Zentralisierung der Blockchain höher ist, sich Monopole bilden können und so die Definition der Blockchain als „verteilte [...] Register“[60] verletzt wird.[31] Betrachtet werden auch hier aus den zuvor genannten Gründen, zum Abschluss noch einmal Proof-of-Work und Proof-of-Stake.

Bei PoW und PoS besteht die Gefahr einer Zentralisierung und damit weniger Fairness.

Bei PoS kann dies durch die Belohnung, die bei einer erfolgreichen Validierung vergeben wird, durch den Zinseszinseffekt kommen, da die Belohnungen reinvestiert werden können, wodurch der Validierer wieder mehr Stimmgewicht erhält.[34] Deshalb gibt es bei PoS die Befürchtung, dass Besitzer des Stakes kein Interesse daran haben, diesen an Dritte abzugeben, da ihr Stake, wie beschrieben, einen direkten Beitrag zu einem noch größeren Stake leistet.[58]

Bei Blockchains, die auf PoW basieren gibt es dieses Problem nicht, da bei jedem Block, von der Blockchain aus betrachtet, alle am gleichen Punkt stehen.[58] Doch bei diesen Blockchains ist zu sehen, dass sich Miner zentralisieren.[34] Es ist schwierig für einzelne Miner fortlaufend ihre Hardware zu verstärken, um immer aufwändigere Puzzle lösen zu können und den dafür benötigten Strom zu bezahlen.[31] „Neueinsteiger haben dort kaum eine Chance, erfolgreich in das Streben nach immer mehr Rechenkapazität einzusteigen.“[34]

Bei PoS existiert der gesamte Stake bereits, es bedarf keines Minings und es besteht auch kein Grund die Hardware immer weiter aufzurüsten, um immer komplexere Puzzle zu

lösen.[31] Insgesamt sei PoS in dieser Hinsicht weniger anfällig und „erlaube durch die Abkehr vom Ressourcenzwang einen leichteren Einstieg.“[34] Zudem führen Blockchains, die PoS verwenden, Mechanismen ein, die den vorhandenen Stake unter den Teilnehmern besser verteilen.[58] Ein Beispiel hierfür ist allerdings die Verwendung von PoW, um neuen Stake zu erzeugen.[58]

5.2 Schwierigkeiten beim Wechsel des Konsensmechanismus

> „Consensus mechanisms can be changed, but that also requires a consensus.“[43]

Dies bedeutet, dass ebenso wie für gültige Transaktionen der Blockchain, der Konsensmechanismus verwendet werden kann, um Konsens über Änderung an der Funktionsweise der Blockchain selbst herzustellen.[63] Dafür wird ein Hard Fork benötigt.[15] Ein Beispiel für die Änderung an der Funktionsweise einer Blockchain, welches in dieser Arbeit vorkommt, ist Bitcoin Cash, welches sich von Bitcoin abspaltete und infolgedessen eine höhere Block Size hat (siehe Abschnitt 4.2.1).[15] Von Bitcoin existieren viele Abspaltungen[15]. Dies zeigt, dass verschiedene Ansichten darüber existieren, wie Bitcoin letztlich umgesetzt werden soll.

Die technische und operative Komplexität, die mit einem Wechsel des Konsensmechanismus einhergeht, macht einen Hard Fork zu einem schwierigen Unterfangen.[7] Ein dezentralisiertes Netzwerk muss eine systemkritische Aktualisierung in Abwesenheit einer zentralen Autorität koordinieren, die möglicherweise Milliarden von Dollar an Nutzergeldern in Gefahr bringt.[7]

Ethereum möchte mit Ethereum 2.0 auf Proof-of-Stake umschalten, doch dies wird schon lange angekündigt und immer weiter nach hinten verschoben, der aktuelle Termin ist Ende 2021.[34] Doch schon jetzt werden weitreichende Folgen sichtbar. Ein Beispiel hierfür ist NVIDIA, welche Grafikkarten herstellen, die in hohen Mengen von Minern gekauft und für das PoW-Verfahren verwendet werden.[28] Wenn nun Ethereum auf PoS umsteigt, werden die GPUs nicht mehr benötigt, die Nachfrage sinkt und die alten Grafikkarten landen auf dem Gebrauchtwarenmarkt, wo sie für einen günstigeren Preis angeboten werden, was zusätzlich die Nachfrage nach neuen Karten senkt.[27] Dies wiederum hat einen spürbaren, negativen Einfluss auf die NVIDIA-Aktie.[28]

Zudem existiert bei einigen Konsensmechanismen, dadurch, dass sie in der Praxis nicht weit verbreitet sind, die Frage, wie sie sich auf die Sicherheit und Eigenschaften des Netzwerks auswirken.[7]

6 Fazit

Das Ziel der vorliegenden Bachelorarbeit war es, heute relevante Konsensmechanismen für Public Blockchains zu ermitteln, diese im Bezug auf verschiedene Eigenschaften (Sicherheit, Skalierbarkeit, Nachhaltigkeit) zu vergleichen und letztlich den, auf diese Eigenschaften bezogen, besten Konsensmechanismus zu bestimmen. Dies geschah, indem aktuelle Literatur ausgewertet wurde.

Zusammenfassend kann man sagen, dass Public Blockchains meist im Bereich Finanzen, vor allem für Kryptowährungen, eingesetzt werden. Für heute relevante Blockchains werden meist die Konsensmechanismen Proof-of-Work (PoW) und Proof-of-Stake (PoS) verwenden. Einige Projekte verwenden auch Proof-of-Staked-Authority (PoSA) oder auf Byzantine Fault Tolerance (BFT)-basierende Konsensmechanismen, welche aber zur Absicherung vor Angriffen zusätzlich PoS verwenden.

Ein Vergleich im Bereich Sicherheit, der die möglichen Angriffe gegen die jeweiligen Blockchains, mit den jeweils betrachteten Konsensmechanismen, betrachtet, konnte zeigen, dass PoW der, unter den hier betrachteten Aspekten, sicherste Konsensmechanismus ist.

Im Bereich Skalierbarkeit konnte gezeigt werden, dass ein Vergleich dieser Eigenschaft anhand der jeweiligen Transactions per Secound (TPS) der Blockchains für einen Vergleich der Konsensmechanismen unzureichend ist. Der Grund hierfür ist, dass andere Eigenschaften, welche unabhängig vom Konsensmechanismus sind, wie z. B. die Block Size oder die Block Generation Speed, einen deutlichen Einfluss auf die Skalierbarkeit der Blockchain haben. Weiterführende Arbeiten müssten zur Untersuchung der Skalierbarkeit anhand der TPS eine Normalisierung der Konsensmechanismen vor dem Heranziehen dieser Metrik durchführen.

Ein Vergleich im Bereich Nachhaltigkeit, anhand des Energieverbrauchs der jeweiligen Konsensmechanismen, konnte zeigen, dass unter den zwei sichersten Konsensmechanismen (PoW und PoS), PoS nachhaltiger ist. Allerdings gibt es keine genauen wissenschaft-

lichen Untersuchungen für PoS, im Umfang wie diese für PoW existieren, daher müssten weiterführende Arbeiten dies genauer untersuchen, eventuell auch für die restlichen, hier genannten Konsensmechanismen.

Sicherheit wurde hier als wichtigster Aspekt eingestuft, da die Blockchain ohne Sicherheit nicht als das dienen kann, was sie nach Definition ist, nämlich eine vor Manipulationen geschützte, vertrauenswürdige Quelle von Informationen.[60] Dies ergibt PoW als beste Art von Konsensmechanismus. Der Aspekt Nachhaltigkeit ist allerdings auch wichtig und könnte mit der Zeit immer relevant werden und somit ein umweltbelastendes Verfahren wie PoW von der Gesellschaft nicht mehr toleriert werden. Dann wäre mehr Sicherheit bei PoS nötig, damit dies besser wird oder ein ganz anderer Konsensmechanismus, der beide Herausforderungen in den Griff bekommt.

Zudem sollten Zusammenhänge zwischen den Eigenschaften genauer betrachtet werden. Ein Beispiel hierfür wäre der Zusammenhang zwischen Block Size, welcher Einfluss auf die Skalierbarkeit hat, und Sicherheit.

Außerdem sollte der Aspekt Fairness nicht aus den Augen gelassen werden, da sowohl bei PoW, als auch bei PoS die Gefahr einer Zentralisierung, was dem Grundgedanken der Blockchain widerspricht, besteht.

Allerdings sollte beim Betrachten von besseren Alternativen auch beachtet werden, dass es für etablierte Blockchain-Projekte nicht trivial ist ihren Konsensmechanismus zu wechseln.

Public Blockchains sind eine relativ neue Technologie, mit der ersten Anwendung mit Bitcoin im Jahr 2009. Daraus folgen auch relativ wenige wissenschaftliche Betrachtungen und Beobachtungen in der Praxis, vor allem der weniger etablierten Konsensmechanismen, abseits von PoW und PoS. Dies kann mit der Zeit nachgeholt werden.

Bei einigen hier herangezogenen Quellen handelt es sich um Blogartikel oder Whitepaper der Hersteller selbst. Diese wurden nach bestem Wissen und Gewissen auf Plausibilität geprüft, dennoch wäre wissenschaftliche Literatur an dieser Stelle besser geeignet. Da diese oft fehlt könnte dies in Zukunft ebenfalls Gegenstand wissenschaftlicher Betrachtungen sein.

Ein Beispiel hierfür ist die Blockchain XRP, welche angibt, dass sie dezentral ist, sich dies aber bei genauerer Betrachtung als falsch herausstellt.[19]

Welche Konsensmechanismen, ob die hier betrachteten, oder ein ganz anderer auf lange Sicht die Besten oder überhaupt gut sind, wird sich mit der Zeit herausstellen, wenn es mehr Beobachtungen in der Praxis und wissenschaftliche Untersuchungen gibt.

Literaturverzeichnis

[1] *Binance Smart Chain.* https://github.com/binance-chain/whitepaper/blob/master/WHITEPAPER.md. – Letzter Zugriff am: 21.10.2021

[2] *Bitcoin Energy Consumption Index.* https://digiconomist.net/bitcoin-energy-consumption. – Letzter Zugriff am: 01.10.2021

[3] *Bitcoin's Energy Usage, Explained.* https://www.forbes.com/advisor/investing/bitcoins-energy-usage-explained/. – Letzter Zugriff am: 02.10.2021

[4] *Block size and scalability, explained.* https://cointelegraph.com/explained/block-size-and-scalability-explained. – Letzter Zugriff am: 27.07.2021

[5] *The Blockchain Scalability Problem the Race for Visa-Like Transaction Speed.* https://towardsdatascience.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44. – Letzter Zugriff am: 11.10.2021

[6] *Byzantine Fault Tolerance Explained.* https://academy.binance.com/en/articles/byzantine-fault-tolerance-explained. – Letzter Zugriff am: 09.09.2021

[7] *Cambridge Bitcoin Electricity Consumption Index.* https://cbeci.org/index/comparisons. – Letzter Zugriff am: 11.10.2021

[8] *Consensus Compare: Casper vs. Tendermint.* https://blog.cosmos.network/consensus-compare-casper-vs-tendermint-6df154ad56ae. – Letzter Zugriff am: 31.08.2021

[9] *Critique of Buterin's "A Proof of Stake Design Philosophy".* https://tuurdemeester.medium.com/critique-of-buterins-a-proof-

of-stake-design-philosophy-49fc9ebb36c6. – Letzter Zugriff am: 22.09.2021

[10] *Cryptocurrency Transaction Speeds in 2021.* https://blog.tezro.com/cryptocurrency-transaction-speeds/. – Letzter Zugriff am: 28.07.2021

[11] *Daimler reveals several blockchain identity projects.* https://www.ledgerinsights.com/daimler-reveals-several-blockchain-identity-projects/. – Letzter Zugriff am: 06.08.2021

[12] *Ethereum Plans to Cut Its Absurd Energy Consumption by 99 Percent.* https://spectrum.ieee.org/ethereum-plans-to-cut-its-absurd-energy-consumption-by-99-percent. – Letzter Zugriff am: 04.10.2021

[13] *Flow blockchain using Proof-of-Stake mechanism.* https://nederob.medium.com/flow-blockchain-using-proof-of-stake-mechanism-ca53be9c8b8c. – Letzter Zugriff am: 24.10.2021

[14] *Forbes Blockchain 50 2021.* https://www.forbes.com/sites/michaeldelcastillo/2021/02/02/blockchain-50/?sh=66e2bf7231cb. – Letzter Zugriff am: 07.06.2021

[15] *Guide to Bitcoin Forks.* https://hedgetrade.com/guide-to-bitcoin-forks/. – Letzter Zugriff am: 01.11.2021

[16] *HotStuff: the Consensus Protocol Behind Facebook's LibraBFT.* https://medium.com/ontologynetwork/hotstuff-the-consensus-protocol-behind-facebooks-librabft-a5503680b151. – Letzter Zugriff am: 11.09.2021

[17] *An Introduction to Binance Smart Chain (BSC).* https://academy.binance.com/en/articles/an-introduction-to-binance-smart-chain-bsc. – Letzter Zugriff am: 20.10.2021

[18] *Is XRP Decentralized? Ripple's Involvement in the Cryptocurrency.* https://cryptobriefing.com/is-xrp-decentralized-ripples-involvement-cryptocurrency/. – Letzter Zugriff am: 21.10.2021

[19] *Is XRP Decentralized? Ripple's Involvement in the Cryptocurrency.* https://cryptobriefing.com/is-xrp-decentralized-ripples-involvement-cryptocurrency/. – Letzter Zugriff am: 28.10.2021

[20] *Kryptowährung im Plus: Elon Musks nächste Bitcoin-Volte*. https://www.tagesschau.de/wirtschaft/finanzen/bitcoin-kryptowaehrung-musk-kurse-bewegen-tesla-101.html. – Letzter Zugriff am: 04.10.2021

[21] *Long-Range Attacks: The Serious Problem With Adaptive Proof of Work*. https://blog.ethereum.org/2014/05/15/long-range-attacks-the-serious-problem-with-adaptive-proof-of-work/. – Letzter Zugriff am: 24.09.2021

[22] *The Mystery Behind Block Time*. https://medium.facilelogin.com/the-mystery-behind-block-time-63351e35603a. – Letzter Zugriff am: 28.07.2021

[23] *NDSS 2020 The Attack of the Clones Against Proof-of-Authority*. https://www.youtube.com/watch?v=o00RoKdephQ. – Letzter Zugriff am: 17.09.2021

[24] *Neue Kryptowährung - Chia Bitcoin in Grün*. https://www.manager-magazin.de/finanzen/boerse/chia-network-neue-kryptowaehrung-will-bitcoin-in-gruen-sein-a-c854ac15-9d16-498c-b90c-eab05e28485c. – Letzter Zugriff am: 10.05.2021

[25] *Not all HotStuff is the same*. https://coinrivet.com/not-all-hotstuff-is-the-same/. – Letzter Zugriff am: 24.10.2021

[26] *Nothing-at-Stake Problem*. https://smithandcrown.com/glossary/nothing-stake-problem/. – Letzter Zugriff am: 28.10.2021

[27] *Nvidia: Ethereum's shift to proof-of-stake could reduce demand for GPUs*. https://www.theblockcrypto.com/linked/106229/nvidia-ethereums-shift-to-proof-of-stake-could-reduce-demand-for-gpus. – Letzter Zugriff am: 20.10.2021

[28] *Nvidia Stock Is Falling. Blame Bitcoin and Ethereum*. https://www.barrons.com/articles/nvidia-stock-chips-mining-bitcoin-ethereum-51626799762. – Letzter Zugriff am: 20.10.2021

[29] *Ontology Launches VBFT, a Next-Generation Consensus Mechanism, Becoming one of the First VRF-Based Public Chains*. https://medium.com/ontologynetwork/ontology-launches-vbft-a-next-generation-consensus-mechanism-becoming-one-of-the-first-vrf-based-91f782308db4. – Letzter Zugriff am: 06.08.2021

[30] *Ontology Open-Sources VBFT Consensus Mechanism and new Version of Underlying Framework*. https://medium.com/ontologynetwork/ontology-open-sources-vbft-consensus-mechanism-and-new-version-of-underlying-framework-2257530c5504. – Letzter Zugriff am: 21.10.2021

[31] *POW vs. PoS: a comparison of two blockchain consensus algorithms*. https://medium.com/@EdChain/pow-vs-pos-a-comparison-of-two-blockchain-consensus-algorithms-f3effdae55f5. – Letzter Zugriff am: 19.09.2021

[32] *Proof of Authority Explained*. https://limechain.tech/blog/proof-of-authority-explained/. – Letzter Zugriff am: 20.10.2021

[33] *Proof of Stake FAQs*. https://eth.wiki/concepts/proof-of-stake-faqs. – Letzter Zugriff am: 25.09.2021

[34] *Proof of Stake: klimafreundlicheres Kryptogeld*. https://www.heise.de/hintergrund/Proof-of-Stake-klimafreundlicheres-Kryptogeld-6147207.html. – Letzter Zugriff am: 19.09.2021

[35] *Proof of Stake (PoS)*. https://www.investopedia.com/terms/p/proof-stake-pos.asp. – Letzter Zugriff am: 29.08.2021

[36] *Selfish Mining Explained*. https://academy.binance.com/en/articles/selfish-mining-explained. – Letzter Zugriff am: 28.08.2021

[37] *Sybil Attacks Explained*. https://academy.binance.com/en/articles/sybil-attacks-explained. – Letzter Zugriff am: 04.10.2021

[38] *Tendermint Explained — Bringing BFT-based PoS to the Public Blockchain Domain*. https://blog.cosmos.network/tendermint-explained-bringing-bft-based-pos-to-the-public-blockchain-domain-f22e274a0fdb. – Letzter Zugriff am: 06.09.2021

[39] *Tesla stoppt Autoverkauf für Bitcoins – wegen des Stromverbrauchs*. https://www.spiegel.de/wirtschaft/unternehmen/tesla-stoppt-autoverkauf-fuer-bitcoins-laut-elon-musk-der-umwelt-zuliebe-a-4826c6a1-f67c-4498-9e4e-d67d130e2918. – Letzter Zugriff am: 13.05.2021

[40] *Types of Blockchain: Public, Private, or Something in Between.* https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between. – Letzter Zugriff am: 24.10.2021

[41] *Vulnerability: Proof of Work vs. Proof of Stake.* https://robertgreenfieldiv.medium.com/vulnerability-proof-of-work-vs-proof-of-stake-f0c44807d18c. – Letzter Zugriff am: 27.09.2021

[42] *What Are Proof of Stake (PoS) and Delegated Proof of Stake (DPoS)?* https://www.gemini.com/cryptopedia/proof-of-stake-delegated-pos-dpos. – Letzter Zugriff am: 20.10.2021

[43] *What is a Consensus Mechanism?* https://hedgetrade.com/what-is-a-consensus-mechanism/. – Letzter Zugriff am: 01.11.2021

[44] *What is Tendermint.* https://docs.tendermint.com/master/introduction/what-is-tendermint.html. – Letzter Zugriff am: 17.09.2021

[45] *What is the difference between PBFT, Tendermint, SBFT and HotStuff ?* https://decentralizedthoughts.github.io/2019-06-23-what-is-the-difference-between/. – Letzter Zugriff am: 21.10.2021

[46] *Why are ETH confirmations so much faster than BTC?* https://www.reddit.com/r/ethereum/comments/5lzif2/why_are_eth_confirmations_so_much_faster_than_btc/. – Letzter Zugriff am: 28.07.2021

[47] *Why Blockchains Need Cosmos Proof-of-Stake for a Sustainable Environment.* https://blog.cosmos.network/why-blockchains-need-cosmos-proof-of-stake-for-a-sustainable-environment-878b3edd2e85. – Letzter Zugriff am: 04.10.2021

[48] *Work is Timeless, Stake is Not.* https://hugonguyen.medium.com/work-is-timeless-stake-is-not-554c4450ce18. – Letzter Zugriff am: 22.09.2021

[49] Aiya Li, Xianhua Wei und Zhou H.: Robust Proof of Stake: A New Consensus Protocol for Sustainable Blockchain Systems. In: *Sustainability* 12 (2020), Nr. 7. – URL https://www.mdpi.com/2071-1050/12/7/2824#metrics. – ISSN 2071-1050

[50] Alexander Hentschel, Ramtin Seraj Dieter Shirley Layne L.: Flow: Separating Consensus and Compute – Block Formation and Execution. (2020). – URL https://arxiv.org/abs/2002.07403

[51] Alqahtani, Salem ; Demirbas, Murat: Bottlenecks in Blockchain Consensus Protocols. (2021). – URL https://arxiv.org/abs/2103.04234

[52] Bach, L. M. ; Mihaljevic, B. ; Zagar, M.: Comparative analysis of blockchain consensus algorithms. In: *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (2018), S. 1545–1550. – URL https://ieeexplore.ieee.org/document/8400278

[53] Cao, Bin ; Zhang, Zhenghui ; Feng, Daquan ; Zhang, Shengli ; Zhang, Lei ; Peng, Mugen ; Li, Yun: Performance analysis and comparison of PoW, PoS and DAG based blockchains. In: *Digital Communications and Networks* 6 (2020), Nr. 4, S. 480–485. – URL https://www.sciencedirect.com/science/article/pii/S2352864819301476. – ISSN 2352-8648

[54] Castro, Miguel ; Liskov, Barbara: Practical Byzantine Fault Tolerance. In: *Proceedings of the Third Symposium on Operating Systems Design and Implementation* (1999), S. 173–186. – URL http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.127.6130. – ISSN 1880446391

[55] Christoph Meinel, Tatiana G.: *Blockchain : Hype oder Innovation*. Springer, 2020. – URL https://link.springer.com/book/10.1007%2F978-3-662-61916-2. – ISBN 978-3-662-61916-2

[56] Ekparinya, Parinya ; Gramoli, Vincent ; Jourjon, Guillaume: The Attack of the Clones Against Proof-of-Authority. (2019). – URL https://arxiv.org/abs/1902.10244

[57] Eyal, Ittay ; Sirer, Emin G.: Majority is not Enough: Bitcoin Mining is Vulnerable. (2013). – URL https://arxiv.org/abs/1311.0243

[58] Group, BitFury: Proof of Stake versus Proof of Work. (2015). – URL https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf

[59] Hans-Georg Fill, Andreas Meier H.: *Blockchain : Grundlagen, Anwendungsszenarien und Nutzungspotenziale*. Springer Vieweg, 2020. – URL https://link.springer.com/book/10.1007%2F978-3-658-28006-2. – ISBN 978-3-658-28006-2

[60] Hans-Georg Fill, unter Mitwirkung von Matthias Egli Mark Fenwick Daniel Gerber Felix Härer Tim Niemer Edy Portmann Sarah Röthlisberger Anton Sentic Bernd Teufel und Stefan W.: *Blockchain kompakt : Grundlagen, Anwendungsoptionen und kritische Bewertung*. Springer Vieweg, 2020. – URL https://link.springer.com/book/10.1007%2F978-3-658-27461-0. – ISBN 978-3-658-27461-0

[61] Lamport, Leslie ; Shostak, Robert ; Pease, Marshall: The Byzantine Generals Problem. In: *ACM Transactions on Programming Languages and Systems* (1982), S. 382–401. – URL https://www.microsoft.com/en-us/research/publication/byzantine-generals-problem/

[62] Masson-Delmotte, P. Zhai A. Pirani S.L. Connors C. Péan S. Berger N. Caud Y. Chen L. Goldfarb M.I. Gomis M. Huang K. Leitzell E. Lonnoy J.B.R. Matthews T.K. Maycock T. Waterfield O. Yelekçi R. Y. ; (eds.), B. Z.: Climate Change 2021: The Physical Science Basis. Contribution of Working Group I to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change. In: *Cambridge University Press* (2021). – URL https://www.ipcc.ch/report/ar6/wg1/#FullReport

[63] Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System. (2008). – URL https://bitcoin.org/bitcoin.pdf

[64] Peng, Zhiniang ; Chen, Yuki: All roads lead to Rome: Many ways to double spend your cryptocurrency. (2018). – URL https://arxiv.org/abs/1811.06751

[65] Sigurd Schacht, Carsten Lanquillon (.: *Blockchain und maschinelles Lernen : Wie das maschinelle Lernen und die Distributed-Ledger-Technologie voneinander profitieren*. Springer Vieweg, 2019. – URL https://link.springer.com/book/10.1007%2F978-3-662-60408-3. – ISBN 978-3-662-60408-3

[66] Vukolić, Marko: *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*. Springer International Publishing, 2016. – URL https://link.springer.com/chapter/10.1007/978-3-319-39028-4_9. – ISBN 978-3-319-39028-4

[67] Wang, Wenbo ; Hoang, Dinh T. ; Hu, Peizhao ; Xiong, Zehui ; Niyato, Dusit ; Wang, Ping ; Wen, Yonggang ; Kim, Dong I.: A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. In: *IEEE Access* 7 (2019), S. 22328–22370. – URL https://ieeexplore.ieee.org/document/8629877

[68] Weik, Martin H.: *Computer science and communications dictionary*. Springer Science Business Media, 2000. – URL https://books.google.at/books?id=0JILayOfSA4C&pg=PA1484&redir_esc=y. – ISBN 978-0-7923-8425-0

[69] Zhiniang Peng, Yuki C.: All roads lead to Rome: Many ways to double spend your cryptocurrency. (2018). – URL https://arxiv.org/abs/1811.06751

Erklärung zur selbstständigen Bearbeitung einer Abschlussarbeit

Gemäß der Allgemeinen Prüfungs- und Studienordnung ist zusammen mit der Abschlussarbeit eine schriftliche Erklärung abzugeben, in der der Studierende bestätigt, dass die Abschlussarbeit „— bei einer Gruppenarbeit die entsprechend gekennzeichneten Teile der Arbeit [(§ 18 Abs. 1 APSO-TI-BM bzw. § 21 Abs. 1 APSO-INGI)] — ohne fremde Hilfe selbständig verfasst und nur die angegebenen Quellen und Hilfsmittel benutzt wurden. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich zu machen."

Quelle: § 16 Abs. 5 APSO-TI-BM bzw. § 15 Abs. 6 APSO-INGI

Erklärung zur selbstständigen Bearbeitung der Arbeit

Hiermit versichere ich,

Name: _____

Vorname: _____

dass ich die vorliegende Bachelorarbeit – bzw. bei einer Gruppenarbeit die entsprechend gekennzeichneten Teile der Arbeit – mit dem Thema:

Vergleich verschiedener Konsensmechanismen für die Blockchain

ohne fremde Hilfe selbständig verfasst und nur die angegebenen Quellen und Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht.

_____	_____	_____
Ort	Datum	Unterschrift im Original