Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

GRUNDLEGENDE HERAUSFORDERUNGEN IN ÖFFENTLICHEN BLOCKCHAINS

Version 1.0 vom 05.07.2021
Alexander Marsalek – amarsalek@iaik.tugraz.at

Abstract/Zusammenfassung: In dieser Kurzstudie werden einige Eigenschaften von öffentlichen Blockchains am Beispiel von Bitcoin vorgestellt. Je nach Anwendungsfall können diese Eigenschaften zu Nachteilen werden, die den Einsatz der Blockchain-Technologie verhindern, oder zumindest erschweren. Anschließend werden Weiterentwicklungen aber auch Forschungsansätze vorgestellt, die diese Probleme beheben oder zumindest verringern.

Inhaltsverzeichnis

© A-SIT, Partner für Sicherheitsfragen

1. Einleitung

Blockchains werden von vielen als eine sehr vielversprechende Technologie gesehen. Speziell in den Bereichen Finanz, Logistik, Gesundheit und Infrastruktur könnte die Blockchain-Technologie Vorteile bringen. In diesem Bericht werden wir die Vor- und Nachteile von öffentlichen Blockchains, anhand von Bitcoin diskutiert. Bitcoin ist der Name der ersten Kryptowährung, die eine öffentliche Blockchain als „Buchführungssystem“ verwendet.
In diesem Bericht wird davon ausgegangen, dass ein Grundverständnis von Bitcoin vorhanden ist. Für die Grundlagen wird auf das Bitcoin Whitepaper [2] verwiesen. Im nächsten Abschnitt werden einige Herausforderungen vorgestellt und in Abschnitt 3 werden ausgewählte Lösungsansätze diskutiert.

2. Herausforderungen

In diesem Abschnitt stellen wir einige Eigenschaften von Bitcoin vor, die je nach Anwendungsfall einen Nachteil darstellen können.

2.1. Energieverbrauch

Bitcoin verwendet einen Konsensus-Algorithmus namens Proof-of-Work. Bei Proof-of-Work muss eine schwierige Rechenaufgabe gelöst werden. Dessen Lösung wird benötigt um einen neuen Block zu erstellen. Personen, die diese Rechenaufgabe lösen, bzw. die Hardware und Software betreiben um neue Blöcke zu erstellen, werden Miner genannt. Als Belohnung dürfen sie sich neue Währungseinheiten ausschütten. Der Schwierigkeitsgrad der Rechenaufgabe wird an die verfügbare Rechenleistung angepasst. In den letzten Jahren sind der Bekanntheitsgrad und auch die Popularität von Bitcoin enorm gestiegen, wodurch auch der Kurs gestiegen ist. Die steigenden Kurse erhöhten die Gewinnspanne von Minern, wodurch einerseits bestehende Miner mehr Mining-Hardware angeschafft haben und andererseits auch neue Miner zu minen begonnen haben. Dadurch erhöhte sich der Energieverbrauch des Bitcoin-Netzwerkes. Da alle Miner gleichzeitig dieselbe Rechenaufgabe lösen probieren, sich aber nur ein Block durchsetzen kann und die Lösung der Rechenaufgabe auch keinen Zweck außerhalb des Bitcoin-Netzwerkes erfüllt sehen einige Kritiker das schürfen nach neuen Währungseinheiten als Energieverschwendung. Abbildung 1 zeigt den minimalen, maximalen und geschätzten Energieverbrauch des Bitcoin-Netzwerkes an. Der Verbrauch kann nur geschätzt werden, da unklar ist welche Mining-Hardware verwendet wird. Neue Hardware ist wesentlich effizienter als ältere, wodurch es eine große Schwankungsbreite beim geschätzten Verbrauch gibt. Das schürfen und auch der Wettkampf unter den Minern ist jedoch ein wesentlicher Bestandteil von Bitcoin und dessen Sicherheitsmodells. In Abschnitt 3.1 stellen wir verschiedene Lösungen vor, die den Energieverbrauch entweder verringern probieren oder sinnvolle Rechenaufgaben vorsehen.

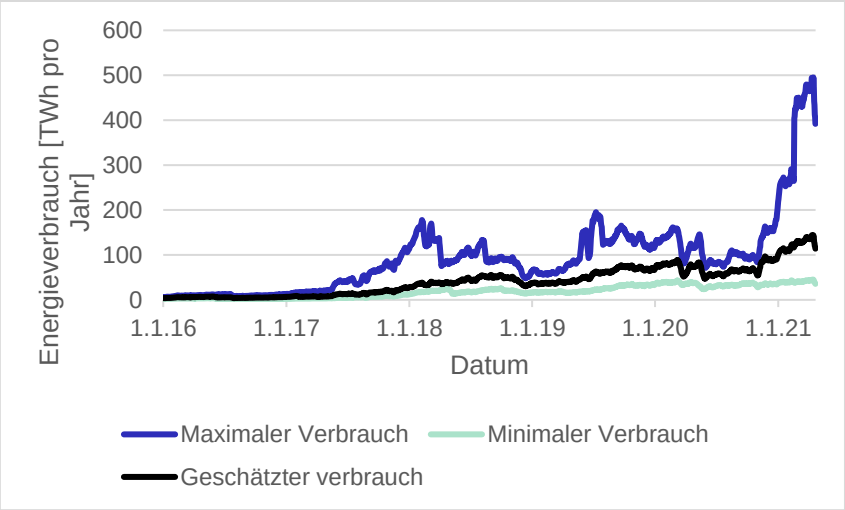

Abbildung 1: Minimaler, maximaler und geschätzter Energieverbrauch des Bitcoin-Netzwerkes

2.2. Zentralisierung

Durch den starken Wettbewerb und der steigenden Schwierigkeit der Rechenaufgabe haben einzelne Miner kaum eine Chance einen Block zu finden. Deswegen schließen sich kleinere Miner meist einem sogenannten Mining-Pool an. Der Pool bündelt die Rechenleistung und erhöht dadurch die Chance einen Block zu finden. Die einzelnen Miner bekommen dann einen Anteil proportional zur bereitgestellten Rechenleistung minus einer kleinen Gebühr. Dies führt zwar zu kleineren, dafür aber zu kontinuierlicheren Einnahmen. In der Praxis hat dies dazu geführt, dass nur fünf Pools ca. 50% der gesamten Rechenleistung kontrollieren. Wenn sich diese Pools zusammenschließen, könnten sie beispielsweise Transaktionen zensieren oder dieselben Bitcoins, im Zuge eines sogenannten „Double Spending“ Angriffes mehrmals ausgeben. Verschärfend kommt dazu, dass sich alle fünf Pools im selben Land befinden.
Durch den starken Wettbewerb ist es für Miner zudem essentiell Ihre Kosten zu minimieren. Die Hauptkosten ergeben sich durch den hohen Stromverbrauch. Deswegen betreiben Miner ihre Hardware normalerweise in Gebieten mit niedrigen Stromkosten. Dies führt zu einer weiteren geographischen Zentralisierung auf einige wenige Orte. In Abschnitt 3.2 stellen wir Ansätze vor, die der Zentralisierung entgegenwirken sollen.

2.3. Skalierbarkeit

Bitcoin sammelt Transaktionen in Blöcken. Der Konsensus-Algorithmus sieht eine maximale Blockgröße von einem Megabyte vor, wodurch die Anzahl der Transaktionen pro Block beschränkt ist. Zudem strebt der Konsensus-Algorithmus eine durchschnittliche Blockerstellungszeit von 10 Minuten an. Dies führt dazu, dass Bitcoin nur wenige Transaktionen pro Sekunde durchführen kann. Abbildung 2 zeigt den zeitlichen Verlauf der bestätigten Transaktionen pro Sekunde.

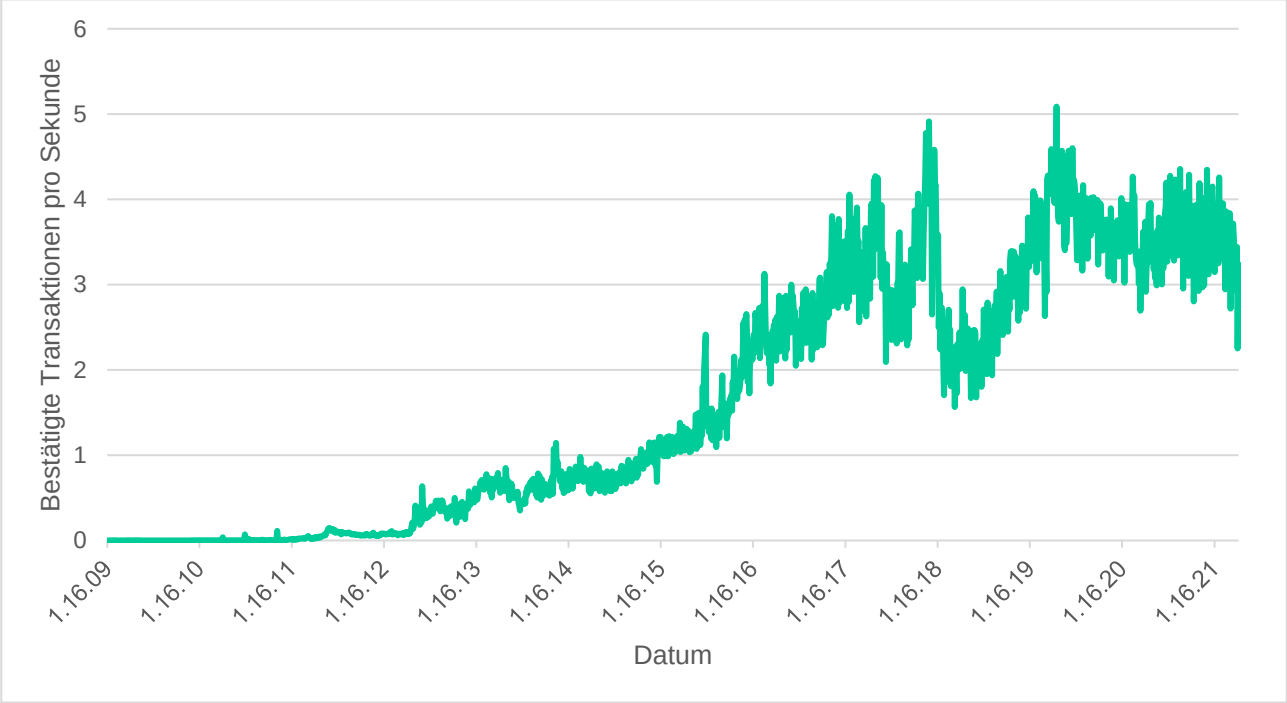

Abbildung 2: Bestätigte Transaktion pro Sekunde im Bitcoin-Netzwerk.

Im Vergleich dazu kann der Zahlungsdienstleister VISA bis zu 65000 Transaktionen pro Sekunden bearbeiten. Durchschnittlich bearbeitet VISA ca. 1800 Transaktionen pro Sekunde [2]. In Abschnitt 3.3 stellen wir Ansätze vor, die einen höheren Transaktionsdurchsatz ermöglichen.

2.4. Privatsphäre

Zu den Grundprinzipen von Bitcoin gehört, dass jeder Knoten teilnehmen darf und alles überprüfen kann. Aus diesem Grund ist jede Transaktion und jeder Block öffentlich einsehbar. Es sind auch die

Sendeadressen, die Empfängeradressen und auch die Beträge öffentlich einsehbar. Es kann zwar jede Benutzerin bzw. jeder Benutzer beliebig viele Adressen generieren und dies auch komplett anonym und offline, trotzdem bietet Bitcoin nur Pseudo-Anonymität. Die Adressen bieten zwar einen gewissen Grad an Privatsphäre, jedoch können die Transaktionen beispielsweise mittels Heuristiken verkettet und ausgewertet werden. Wenn dann eine Transaktion deanonymisiert wird, kann auch die Privatsphäre von vorhergegangenen und nachfolgenden Transaktionen verringert werden. Ansätze die die Privatsphäre besser schützen werden in Abschnitt 3.4 vorgestellt.

2.5. Speicherplatz

Das Bitcoin Protokoll sieht vor, dass jeweils die aktuelle beste Kette verlängert wird. Dadurch wächst die Blockchain laufend und wird nie kürzer. Jeder Knoten sollte für maximale Sicherheit alle Blöcke und Transaktionen selbstständig verifizieren. Dafür müssen einerseits bereits synchronisierte Knoten die gesamte Blockchain speichern, um die Blöcke bei Bedarf an neue Knoten ausliefern zu können und andererseits müssen neue Knoten die gesamte Blockchain herunterladen und verifizieren. Bereits heute benötigt die Blockchain mehr als 330 GB an Speicherplatz. Viele Geräte, wie beispielsweise Smartphones, Netbooks, Laptops oder IOT Geräte verfügen nur über eingeschränkte Ressourcen, wodurch sie die Bitcoin Blockchain nicht oder nur eingeschränkt nutzen können. Abbildung 3 zeigt das Wachstum der Bitcoin Blockchain seit dem Start. Da die Blockchain stetig wächst wird es zunehmend schwerer für Geräte mit beschränkten Ressourcen die komplette Blockchain zu verifizieren und zu speichern. In Abschnitt 3.5 stellen wir Ansätze vor, die diesem Problem entgegenwirken sollen.

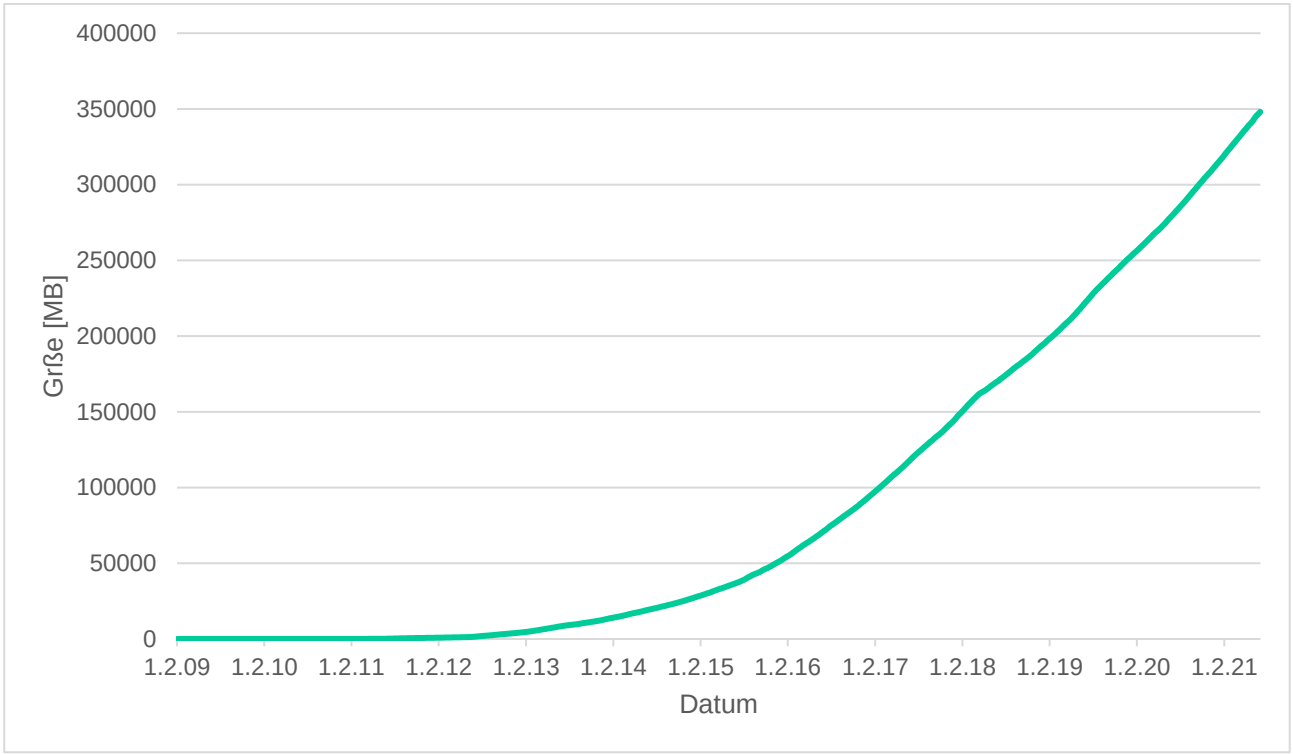

Abbildung 3: Größe der Bitcoin Blockchain (Quelle: [3]).

2.6. Unveränderbarkeit

Da es sich bei Bitcoin um eine öffentliche Blockchain handelt kann jeder teilnehmen und Transaktionen oder Blöcke erstellen. Das Protokoll prüft nur ob die Daten an sich gültig sind, kann fehlerhafte oder (rechtlich) illegale Daten aber nicht verhindern. Das Problem ist, dass sobald diese Daten einmal in die Blockchain aufgenommen wurden, sie nicht mehr entfernt werden können. Um die Daten zu entfernen müsste der betroffene Block sowie alle darauffolgenden Blöcke neu erstellt werden. Forscher haben unter anderem geheime Dokumente oder Links zu illegalen

pornografischen Inhalten in der Bitcoin Blockchain gefunden [4]. Die Unveränderbarkeit der Blockchain verhindert, dass diese Daten entfernt werden können. Auch das europäische Recht „vergessen zu werden“ kann von Bitcoin nicht umgesetzt werden. Potentielle Lösungen werden in Abschnitt 3.6 vorgestellt.

3. Potentielle Lösungen

In diesem Abschnitt stellen wir verschiedene Ansätze und Lösungen für die zuvor genannten Probleme vor. Teilweise sind diese Lösungen bereits fertig implementiert und können produktiv genutzt werden. Teilweise handelt es sich aber auch um Ansätze, welche noch erforscht und verbessert werden.

3.1. Energieverbrauch

Im Bereich Energieverbrauch gibt es mindestens zwei Arten von Lösungsansätzen die unterschieden werden müssen. Einerseits wird an Proof-of-Work Algorithmen geforscht, bei denen die Ergebnisse auch außerhalb der Kryptowährung Bedeutung haben, wodurch der Energieverbrauch zwar nicht verringert wird, dafür aber „sinnvoller“ eingesetzt wird. Andererseits werden auch alternativen zu Proof-of-Work erforscht. Beispiele für Alternativen sind „Proof-of-Stake“, „Proof-of-Authority“, “Proof-of-Burn” und “Proof-of-Capacity”. Diese Alternativen, sowie PrimeCoin, eine Kryptowährung mit speziellem Proof-of-Work Algorithmus werden in den nächsten Abschnitten kurz vorgestellt.

3.1.1. PrimeCoin

Bei PrimeCoin handelt es sich um eine Kryptowährung, welche den von Bitcoin verwendeten Proof-of-Work Algorithmus gegen einen sogenannten prime Proof-of-Work Algorithmus ersetzt hat. Miner die einen Block erstellen, erzeugen als Nebenprodukt spezielle Primzahlketten. Diese Primzahlketten sind unter den Namen „Cunningham Chains“ und „bi-twin Chains“ bekannt und noch relativ wenig erforscht und daher von wissenschaftlichem Interesse.

3.1.2. Proof-of-Stake

Im Gegensatz zu Proof-of-Work Algorithmen, bei denen alle Miner um die Wette rechnen und nur der Erste gewinnt, wird bei Proof-of-Stake Algorithmen der nächste Miner durch einen deterministischen Prozess ausgewählt. Dieser Auswahlprozess bezieht den Einsatz der einzelnen Kandidaten in die Berechnung ein. Ethereum plant den Proof-of-Stake Algorithmus *Casper* zu verwenden [5]. Bei *Casper* werden Miner die sich nicht an die Regeln halten bestraft und können ihren Einsatz verlieren. Dies soll zu einem stabilen Netzwerk führen. Durch den notwendigen Einsatz von Guthaben bei Proof-of-Stake Algorithmen, sind beispielsweise 51% Angriffe deutlich riskanter als bei Proof-of-Work Algorithmen [3]. Ein weiterer Vorteil von Proof-of-Stake Algorithmen ist der deutlich geringere Energieaufwand im Vergleich zu Proof-of-Work Algorithmen. Dies führt auch dazu, dass weniger Münzen ausgeschüttet werden können und trotzdem ein Anreiz zum minen vorhanden ist.

3.1.3. Proof-of-Authority

Bei Proof-of-Authority Algorithmen werden Miner an sich nicht mehr benötigt, stattdessen können autorisierte Signatoren jederzeit nach eigenem Ermessen neue Blöcke erstellen [6]. Dadurch ergeben sich neue Herausforderungen, wie die Kontrolle der Blockerstellungsfrequenz, welche Signatoren wann autorisiert sind und wie die Liste der in Frage kommenden Signatoren dynamisch angepasst werden kann. Ethereum hat sich für das Clique-Protokoll entschieden. Clique wird derzeit im Testnetzwerk verwendet. Beim Testnetzwerk handelt es sich um eine alternative zum Hauptnetzwerk, in dem ohne den Einsatz von echten Ether herumexperimentiert werden kann. Die im Testnetzwerk generierten Ether sind de facto wertlos. Das Clique-Protokoll sieht vor, das ein Signator maximal einen von x Blöcken signieren darf, dadurch kann ein bösartiger Signator keinen

verheerenden Schaden im Netzwerk anrichten. Des Weiteren sieht das Protokoll vor, das der Miner der an der Reihe ist exakt zum optimalen Zeitpunkt, entsprechend der gewünschten Blockfrequenz, einen Block erstellt und alle anderen Signatoren, die berechtigt, aber nicht an der Reihe sind eine gewisse Zeit warten. Dadurch hat der Signator der an der Reihe ist einen kleinen Vorteil gegenüber anderen Signatoren und es wird zusätzlich die Netzwerklast reduziert. Um neue Signatoren aufzunehmen bzw. bestehende aus der List zu entfernen ist ein Voting-Prozess vorgesehen. Jeder Signator auf der Liste hat pro Block ein Stimmrecht um neue Signatoren aufzunehmen oder bestehende auszuschließen.

3.1.4. Proof-of-Burn

Bei Proof-of-Burn Algorithmen wird im Gegensatz zur Proof-of-Work Algorithmen nicht Elektrizität „verbrannt“ sondern digitale Währungseinheiten [7]. Die Münzen werden „verbrannt“ indem sie auf zufällige Adressen überwiesen werden. Die Wahrscheinlichkeit, dass jemand den dazugehörigen privaten Schlüssel hat oder findet ist extrem gering. Durch das vernichten der Münzen erhält man das Recht an der Mining-Lotterie teilzunehmen. Je mehr Münzen man vernichtet desto höher ist die Wahrscheinlichkeit, dass man zum minen ausgewählt wird. Dies kann mit einem Proof-of-Stake Einsatz verglichen werden, den man niemals zurückbekommt.

3.1.5. Proof-of-Capacity

Proof-of-Capacity Algorithmen sind eine Implementierung der Idee „Megabytes als Ressource“ [7]. Bei diesem Ansatz werden große Mengen Speicherplatz benötigt, wodurch dieser Ansatz als relativ sicher gegen Botnetzangriffe zu sehen ist. Des Weiteren ist der Energieverbrauch deutlich geringer als bei Proof-of-Work Ansätzen. Bei diesem Ansatz werden Daten nach einem bestimmten Algorithmus erstellt, beispielsweise dem wiederholten hashen des öffentlichen Schlüssels. Die Wahrscheinlichkeit einen Block erstellen zu dürfen steigt mit der Größe des verwendeten Speicherplatzes. Kritiker sehen Probleme bei diesem Ansatz, da der Miner nichts zu verlieren hat, wenn er oder sie sich unehrlich verhält.

3.2. Zentralisierung

Ein Teil der Kryptowährungen verwenden spezielle Proof-of-Work Algorithmen um der Zentralisierung entgegen zu wirken. Die Algorithmen werden dabei so entworfen, dass sie auf herkömmlichen Prozessoren effizient implementiert werden können, gleichzeitig aber die Herstellung von spezialisierter Hardware, sogenannter ASICs unprofitabel ist. ASIC steht für „application-specific integrated circuit“, oder übersetzt „anwendungsspezifische integrierte Schaltung“. Die Idee ist, dass alle PC-Benutzer und Benutzerinnen ohne zusätzliche Anschaffungskosten minen kann. Im Vergleich dazu hat selbst ein schneller PC keine Chance gegen einen ASIC wenn es um das minen von Bitcoin geht. Ein Beispiel für eine Kryptowährung mit einem für CPUs optimierten Proof-of-Work Algorithmus ist Monero [6]. Aber auch diese speziellen Proof-of-Work Algorithmen lösen das Zentralisierungsproblem nicht komplett, da sich Miner trotzdem meist größeren Pools anschließen und auch der Strompreis einen großen Einfluss auf den Gewinn hat.

3.3. Skalierbarkeit

Es gibt mehrere relativ leicht umzusetzende Änderungen, die die Anzahl der Transaktionen pro Sekunde erhöhen. Es gibt Beispielsweise Kryptowährungen welche das durchschnittliche Blockerstellungsintervall von 10 Minuten auf 2,5 (z.B.: Litecoin) oder 1 Minute (z.B.: Primecoin) verringert haben. Ändere Kryptowährungen haben die Blockgröße erhöht. Während Bitcoin nur 1 Megabyte große Blöcke erlaubt, erhöhte Bitcoin Cash das Limit zuerst auf 8MB und im Jahr 2018 nochmals auf 32MB. Bitcoin hingegen hat sich für einen Ansatz namens „SegWit“ entschieden. SegWit [6] steht für Segregated Witness. Bei SegWit werden die Zeugendaten aus der Transaktion entfernt und in einer eigenen Datenstruktur gespeichert. Die Größe der Zeugendaten wird nur zu 25% berücksichtigt, wodurch bei rechnerisch gleicher Blockgröße mehr Transaktionen in einen ein Megabyte großen Block Platz haben. Dadurch kann die Anzahl der Transaktionen pro Sekunde erhöht werden.

3.4. Privatsphäre

Bei Bitcoin sind alle Transaktionen und Blöcke öffentlich einsehbar. Dadurch kann leicht nachvollzogen werden wann und wie viele Währungseinheiten transferiert wurden. Ein Teil der neueren Kryptowährungen verwendet Kryptografie um einen Teil oder alle Informationen zu schützen. Die Kryptowährung Monero [6] verwendet beispielsweise „Stealth Addresses“, Ringsignaturen und „Pedersen Commitments“. Die Stealth Addresses verhindern, dass Geldein- und Ausgänge öffentlich einsehbar sind. Die Ringsignaturen verhindern bzw. erschweren das Verfolgen von Geldströmen. Geldbeträge selbst werden mittels Pedersen Commitments verschlüsselt. Neben Monero gibt es auch andere Kryptowährungen die einen besseren Datenschutz bzw. Privatsphäre versprechen. Beispiele dafür sind Zcash und DASH.

3.5. Speicherplatz

Es gibt mehrere Ansätze die den Speicherplatzbedarf reduzieren sollen. In diesem Bericht stellen wir zwei bereits in der Praxis verwendete Ansätze, sowie einen noch nicht umgesetzten Ansatz einer komprimierbaren Blockchain vor.

3.5.1. Lightweight Node

Lightweight Nodes laden nicht die komplette Blockchain herunter und benötigen daher weniger Speicherplatz und Bandbreite. Stattdessen laden Lightweight Nodes nur die Blockheader herunter. Dadurch können sie überprüfen, ob die Kette prinzipiell gültig ist, d.h. ob die Verlinkung und der Schwierigkeitsgrad passen. Zur Transaktionsvalidierung wird ein Ansatz namens „Simplified Payment Verification“ oder kurz SPV verwendet. Mittels SPV kann ein Lightweight Node sicherstellen, dass eine Transaktion in einem Block aufgenommen wurde. Dafür muss der Lightweight Node einen Full Node kontaktieren, welcher eine Bestätigung schickt. Weiteres benachrichtigt der Full Node den Lightweight Node über Transaktionen, die ihn betreffen. Lightweight Nodes müssen dem Full Node vertrauen, dass dieser Transaktionen und Blöcke entsprechend der Regeln verifiziert und auch, dass sie über alle relevanten Transaktionen informiert werden. Zusätzlich hat die Verwendung eines Lightweight Nodes Auswirkungen auf die Privatsphäre, da zu beobachtende Adressen bekannt gegeben werden müssen. Daher sollten Lightweight Nodes nur mit eigenen oder vertrauenswürdigen Full Nodes verbunden werden.

3.5.2. The Mini-Blockchain Scheme

Bruce hat die Kryptowährung Cryptonite entworfen [8]. Cryptonite benötigt nicht alle alten Transaktionen, stattdessen verwendet die Kryptowährung eine eigene Datenstruktur um die „Guthaben“ aller aktiven Adressen explizit zu speichern. Dadurch können ältere Blöcke und Transaktionen verworfen werden. Aus Sicherheitsgründen werden aber die Blockheader der alten Blöcke aufgehoben. Mit Hilfe dieser kann die Verlinkung und der Schwierigkeitsgrad überprüft werden. Des Weiteren führt Cryptonite eine Account-Wartungsgebühr ein. Dadurch kann verhindert werden, dass Accounts mit geringen Guthaben unnötig Platz verbrauchen. Durch die Gebühr verlieren diese Accounts nach einer gewissen Zeit ihr Guthaben und können entfernt werden.

3.5.3. Komprimierbare Blockchain

Im Gegensatz zu Cryptonite sieht der Ansatz einer komprimierbaren Blockchain [9] vor, dass die gesamte Historie erhalten bleibt. Um trotzdem Platz zu sparen wird jedoch eine zweite verlinkte Kette parallel gebaut, deren Blöcke alle wesentlichen Daten enthalten. Die beiden Ketten können unterschiedliche Blockerstellungszeiten haben. Beispielsweise könnte alle 1000 Blöcke ein Block in der zweiten Kette erstellt werden. Dieser Block enthält nur die noch nicht ausgegebenen Transaktionsoutputs. Dadurch benötigt er nur ca. 3 GB. Im Vergleich dazu benötigt die Bitcoin Blockchain bereits über 330 GB an Speicherplatz. Dadurch kann viel Datenverkehr und Speicherplatz während des Synchronisierungsprozesses eingespart werden.

3.6. Unveränderbarkeit

Forscher haben mehrere Ansätze vorgestellt, die es erlauben, Daten in einer Blockchain nachträglich zu korrigieren bzw. zu löschen. In diesem Bericht werden wir zwei dieser Arbeiten vorstellen. Abschnitt 3.6.1 stellt einen Ansatz für private Blockchains vor. Dieser Ansatz basiert auf einer speziellen Hashfunktion. Abschnitt 3.6.2 stellt einen Ansatz für öffentliche Blockchains vor.

3.6.1. Private Blockchain

Ateniese u. a. [2] beschreiben in ihrer Publikation „*Redactable Blockchain – or – Rewriting History in Bitcoin and Friends*“ einen Ansatz, der die nachträgliche Modifikation der Blockchain durch die Verwendung von Chameleon-Hashfunktionen erlaubt. Chameleon-Hashfunktionen sind spezielle Hashfunktionen, die das Finden einer Hash-Kollision (zwei unterschiedliche Datensätze bzw. Blöcke, die auf denselben Hash-Wert abgebildet werden) effizient ermöglichen, sofern das dafür benötigte Geheimnis bekannt ist. Wenn das Geheimnis unbekannt ist, ist es wie bei herkömmlichen kryptografischen Hashfunktionen sehr schwer bis praktisch unmöglich, eine Kollision zu finden.

Bei diesem Ansatz kann man sich die Blockchain als eine Sequenz von Blöcken vorstellen, die über eine Kette mittels eines Schlosses verbunden sind. Das Schloss symbolisiert dabei das benötigte Geheimnis um eine Hash-Kollision zu finden. Die Kette hingeben symbolisiert die Referenz zum Vorgängerblock. Abbildung 4 zeigt für einen Ausschnitt einer Blockchain die nötigen Schritte, um einen Block auszutauschen.

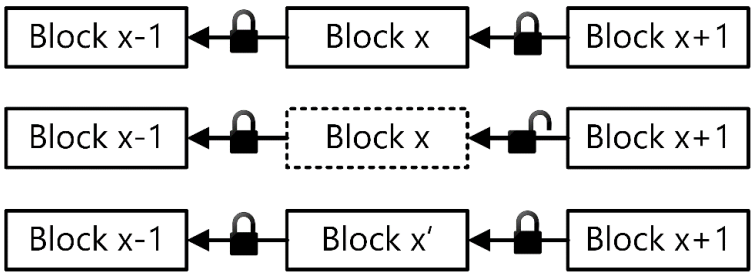

Abbildung 4: Austausch eines Blocks in der Blockchain.

Will man Block *x* verändern, öffnet man zuerst das Schloss, welches Block *x* und Block *x+1* verbindet. Dadurch kann Block *x* durch Block *x'* ausgetauscht werden. Das Schloss zwischen Block x und Block x-1 muss nicht geöffnet werden, da sich der Vorgängerblock bzw. dessen Hashwert nicht ändert. Anschließend wird das Schloss wieder verschlossen, um eine durchgehende Kette zu erhalten. Technisch gesehen wird Block *x'* unter zu Hilfenahme des Geheimnisses so erstellt, dass dessen Hashwert dem ursprünglichen Hashwert von Block *x* gleicht. Dadurch können Blöcke ausgetauscht werden, ohne die Kette zu zerstören.

3.6.2. Öffentliche Blockchain

Deuber u. a. [11] haben einen Ansatz für öffentliche Blockchains vorgestellt. Der Absatz sieht vor, dass zuerst ein Ersatzblock vorgeschlagen wird. Danach wird abgestimmt ob der Ersatzblock den ursprünglichen Block ersetzen soll. Während eines definierten Abstimmungszeitraumes können Miner dafür oder dagegen stimmen. Stimmen genügend Miner für die Korrektur wird der alte Block gelöscht und durch den Ersatzblock ersetzt. Bei einer normalen Blockchain würde dieser Vorgang die Verlinkung zerstören. Um dies zu verhindern fügen die Forscher ein weiteres Feld in die Header der Blöcke ein, welches den alten Merkle-Root-Wert[1] speichert. Des Weiteren ist eine Erweiterung des Blockchain-Verifikationsalgorithmus notwendig. Wenn ein gebrochener Link gefunden wird, wird zusätzlich überprüft ob der Link mit dem alten Merkle-Root-Wert gültig ist. Falls ja, wird überprüft ob

[1] Der Merkle Root ist ein Hashwert, der über alle in einem Block enthaltenen Transaktionen gebildet wird. Für Details wird auf das Bitcoin Whitepaper verwiesen.

genügend Miner für diese Korrektur gestimmt haben. Trifft auch dies zu wird der Link bzw. Block akzeptiert.

4. Conclusio

Bei der Blockchain handelt es sich um eine relativ neue Technologie, die noch ein paar Herausforderungen mit sich bringt. Je nach Anwendungsfalls kann die stetig wachsende Größe, die relativ geringe Anzahl der Transaktionen pro Sekunde oder auch der hohe Energieverbrauch zu einem Problem werden. Auch die limitierte Privatsphäre oder die Unveränderbarkeit der Blockchain schränkt die potentiellen Anwendungsfälle ein. Seit der Veröffentlichung von Bitcoin wurden einige Alternativen entworfen, die diese Nachteile eliminieren sollen. Für die meisten Probleme gibt es bereits produktiv eingesetzte Lösungen. Derzeit gibt es jedoch noch keine Lösung die alle Probleme beseitigt. Da jedoch viele Forscher und Firmen an weiteren Lösungen arbeiten ist davon auszugehen, dass sich die Situation weiter verbessert.

Referenzen

[1] S. Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System," [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Zugriff am 2020].

[2] Visa, „Visa fact Sheet," [Online]. Available: https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf. [Zugriff am 18 06 2021].

[3] Blockchain.com, „Blockchain Size," [Online]. Available: https://www.blockchain.com/charts/blocks-size. [Zugriff am 18 09 2020].

[4] S. Gibbs, „Child abuse imagery found within bitcoin's blockchain," 20 03 2018. [Online]. Available: https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content. [Zugriff am 26 05 2021].

[5] Ethereum, „Proof of Stake FAQ," [Online]. Available: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ. [Zugriff am 04 07 2017].

[6] Ethereum, „Clique PoA protocol & Rinkeby PoA testnet," [Online]. Available: https://github.com/ethereum/EIPs/issues/225. [Zugriff am 05 07 2017].

[7] R. Patterson, „Alternatives for Proof of Work, Part 2: Proof of Activity, Proof of Burn, Proof of Capacity, and Byzantine Generals," 26 08 2015. [Online]. Available: https://bytecoin.org/blog/proof-of-activity-proof-of-burn-proof-of-capacity/. [Zugriff am 05 07 2017].

[8] The Monero Project, „Monero," 2014. [Online]. Available: https://www.getmonero.org/. [Zugriff am 17 06 2021].

[9] E. Lombrozo, J. Lau und P. Wuille, „Segregated Witness (Consensus layer)," 21 12 2015. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki. [Zugriff am 18 06 2021].

[10] J. Bruce, „The Mini-Blockchain Scheme," 2014. [Online]. Available: https://cryptonite.info/files/mbc-scheme-rev3.pdf. [Zugriff am 11 05 2021].

[11] A. Marsalek, „Komprimierbare Blockchain," 12 2020. [Online]. Available: https://technology.a-sit.at/downloads/4118. [Zugriff am 12 2020].

[12] G. Ateniese, B. Magri, D. Venturi und E. Andrade, „Redactable Blockchain – or – Rewriting History in Bitcoin and Friends," 11 05 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7961975/. [Zugriff am 06 06 2018].

[13] D. Deuber, B. Magri und S. A. K. Thyagarajan, „Redactable Blockchain in the Permissionless Setting," 2019. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8835372. [Zugriff am 17 06 2021].

[14] Bitcoin Core, „Bitcoin Core," [Online]. Available: https://github.com/bitcoin/bitcoin. [Zugriff am 18 03 2020].

[15] Bitcoin, „Bitcoin Core version 0.11.0,“ 2015. [Online]. Available: https://github.com/bitcoin/bitcoin/blob/v0.11.0/doc/release-notes.md. [Zugriff am 16 09 2020].

[16] Bitcoin Project, „Running A Full Node,“ [Online]. Available: https://btcinformation.org/en/full-node#blocks-only-mode. [Zugriff am 16 09 2020].

[17] gmaxwell, „Blocksonly mode BW savings, the limits of efficient block xfer, and better relay,“ 26 02 2016. [Online]. Available: https://bitcointalk.org/index.php?topic=1377345.0. [Zugriff am 16 09 2020].

[18] statoshi.info, „Size of Serialized UTXO Set,“ [Online]. Available: https://statoshi.info/dashboard/db/unspent-transaction-output-set. [Zugriff am 18 09 2020].

[19] A. Marsalek, T. Zefferer, E. Fasllija und D. Ziegler, „Tackling data inefficiency: Compressing the bitcoin blockchain,“ in *18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Rotorua, 2019.