MOCHIMO

Post-Quantum-Währung

Abstract

Ein innovativer Ansatz für Kryptowährungen, der ein quantensicheres Transaktionsnetzwerk, echte Dezentralisierung, ultraschnelle Transaktionsverarbeitung, beispiellose Konvergenzzeit und Skalierbarkeit bietet - und das alles in einem vertrauenswürdigen Peer-to-Peer-Netzwerk, das auf Consumer-Hardware läuft.

Matt Zweil
mzweil@mochimo.org

INHALTSVERZEICHNIS

1. VORWORT & DANKSAGUNG 3

2. EXECUTIVE SUMMARY 4

3. DESIGNPRINZIPIEN DES MOCHIMO PROTOKOLLS 6

3.1 AUTONOME DEZENTRALISIERUNG 8

3.2 DAS SELBSTHEILENDE LEDGER 8

3.3 EGALITÄRE INKLUSION DER MINER 10

4. DAS MOCHIMO DESIGN LÖST VIELE PROBLEME 11

4.1 DIE BEDROHUNG DURCH QUANTENCOMPUTER 11

4.2 LANGFRISTIGE LÖSUNG ZUR NETZWERK-SKALIERBARKEIT 13

4.3 NEUERFINDUNG VON TRANSAKTIONSGEBÜHREN ZUR SICHERSTELLUNG DER ABWICKLUNG NACH F.I.F.O. 14

4.4 TRANSAKTIONSDURCHSATZ UND SICHERHEIT 15

5. TECHNISCHER ÜBERBLICK ÜBER DIE WICHTIGSTEN MERKMALE 16

5.1 VERBINDUNGSMANAGEMENT UNTER VERWENDUNG DES RANDOM NETWORK MODELLS 16

5.2 TRANSAKTIONSSPIEGELUNG 18

5.3 DREIWEGE-HANDSHAKE 19

5.4 SCHNELLE SERVER INITIALISIERUNG 21

5.5 DIE TECHNOLOGIE HINTER CHAINCRUNCH™ 23

5.6 DER KONSENSALGORITHMUS 25

5.7 DER KONFLIKTALGORITHMUS 27

6. WICHTIGSTE ECKDATEN DER WÄHRUNG 29

7. ENDNOTEN 30

1 VORWORT & DANKSAGUNG

ALS DAS MOCHIMO ENTWICKLUNGSTEAM IM SOMMER 2017 mit der Arbeit begann, haben wir vereinbart, kein Whitepaper zu veröffentlichen, bis das System ein funktionierendes Produkt zu bieten hat. Heute haben wir nicht nur eine Währung, $MCM, sondern eine lizenzierbare, robuste Gruppe von Algorithmen, die es jedem ermöglicht, eine Währung der nächsten Generation auf einem robusten Protokoll aufzubauen, das Langlebigkeit, Unveränderlichkeit und Dezentralisierung gewährleistet.

Was im folgenden präsentiert wird, ist eine Beschreibung der Mochimo Kryptowährung, **wie sie heute ist**. Dies sind keine Zukunftspläne, sondern eine konkrete Dokumentation, wie wir viele der entscheidenden Probleme, unter denen Kryptowährungen heutzutage leiden, bereits gelöst haben. Wir haben eine Reihe von innovativen Methoden, KI und disruptiven Algorithmen implementiert, die wir in Summe als **Mochimo-Protokoll** bezeichnen.

Das MCM-Projekt ist Dr. Andreas Hülsing und Daniel Bernstein für ihre bahnbrechende Arbeit auf dem Gebiet der Post-Quanten-Kryptographie sehr dankbar. Insbesondere gegenüber Hülsing sind wir zu Dank dafür verpflichtet, dass er unseren kryptographischen Code überprüft hat. Ein weiterer Dank und eine Anerkennung geht an Albert-Laszlo Barabasi für seine Beiträge über Random Networks. Seine Arbeit hat auch die zugrundeliegende Mechanik unseres Konfliktlösungs- und Verteilungsprozesses beeinflusst. Abschließend an Satoshi Nakamoto, den Vater von Bitcoin, wer immer und wo immer Sie sind: Wir danken Ihnen für Ihre Vision einer dezentralen Währung. Wir sind stolz darauf, Ihre Arbeit fortzusetzen, um eine Währung zu schaffen, die wirklich skalierbar und nachhaltig ist.

2 EXECUTIVE SUMMARY

MOCHIMO [$MCM] IST EIN KRYPTOWÄHRUNGS- UND TRANSAKTIONSNETZWERK DER DRITTEN GENERATION , das von Grund auf neu entwickelt wurde, um bekannte Probleme und Mängel in bestehenden Blockchain-Systemen zu verhindern. Mochimo wurde von Grund auf neu geschrieben, um erstklassige Funktionen in einem Krypto-Ökosystem zu kombinieren, das durch kryptographische Algorithmen auch trotz des bevorstehenden Quantum-Zeitalters zukunftssicher ist. Als Teil dieses Protokolls verwendet die Währung ein zufälliges Peer-to-Peer-Netzwerk, ein neues Konsensusverfahren und eine einzigartige Proof-of-Work-Mining-Technologie. Diese Teile arbeiten zusammen, um ein vertrauenswürdiges, verteiltes Ledger zu erstellen.

Am wichtigsten ist, dass die verschiedenen Algorithmen, die für die Mochimo-Währung entwickelt wurden, mehrere Innovationen und Funktionen beinhalten, die eine bereits funktionierende Lösung für einige der kritischsten Probleme bieten, die heute bestehende und neuere Blockchains plagen.

Hier ist eine kurze Liste einiger unserer Innovationen:

1. **ChainCrunch™ Technologie**
   Eine proprietäre Technologie, die die Gesamtgröße der Blockchain reduziert, um dadurch die Skalierbarkeit und Verarbeitung einer großen Anzahl von Transaktionen zu gewährleisten (Skalierung von aktuell 1.000 Transaktionen pro Sekunde(TPS) auf 20.000 TPS innerhalb von 6,75 Jahren); kurz- und langfristige Skalierung ist für Mochimo kein Problem.
2. **Trigg's Algorithmus**
   Eigener Proof-of-Work-Algorithmus, der die FIFO-Transaktionsverarbeitung mit einer festen Transaktionsgebühr gewährleistet. Das Mining wird dadurch für alle Zeit praktikabel bleiben, unabhängig von Menge oder Größe der Miner.
3. **Der Mochimo-Konsensmechanismus**
   Ein neues System, das auf dem Random Networks-Modell aufbaut, eine schnelle Konvergenzzeit und verwaiste Kettenbeschneidung bietet. Es verfügt zudem über einen mathematisch belegbaren Konsens, der dem Consensus-by-Rumor-Modell

2 EXECUTIVE SUMMARY

vieler Kryptowährungen überlegen ist.

4. **Quantenresistente Sicherheit**
   Durch den Einsatz von WOTS+, das von der durch die EU finanzierte PQCRYPTO-Forschungsorganisation geprüft wurde, um Mochimo-Adressen zu sichern, und durch die Verwendung des gesamten MCM-Protokolls auf quantensicheren Algorithmen hat das Mochimo-Entwicklungsteam ein entscheidendes Problem gelöst, welches letztendlich dazu führen wird, dass ECDSA-basierte Protokolle wie Bitcoin, Ethereum und alle ERC-20-Token funktional unsicher und inoperabel werden, sowohl als Transaktionsnetzwerk und als Wertspeicher.
5. **Modell der gerechten Verteilung**
   Ein minimaler Premine für das Entwicklungsteam, kein ICO, selbstregulierende und konstante Mining-Schwierigkeiten und die langsam abnehmenden Blockbelohnungen sind allesamt Garanten, um eine faire Verteilung von MCM zu gewährleisten und die Zugänglichkeit für “spätere” Anwender aufrecht zu erhalten.

Das Mochimo-Entwicklungsteam wird von dem Systemarchitekten Matt Zweil geleitet, einem erfahrenen Netzwerkarchitekten, der einige der ehrgeizigsten Projekte in den Bereichen Transaction Networking, Datacenter Design und Service Provider Networking in der Branche konzipiert und umgesetzt hat. Mochimos Hauptentwickler ist Trigg, ein meisterhafter C-Programmierer und ein KI-Forscher, der seit Ende der 70er Jahre innovative Systeme entwickelt. Gemeinsam haben sie das MCM-Protokoll und die ChainCrunch™ Technologie erstellt. Mit der Unterstützung des breiteren Mochimo-Entwicklungsteams haben Matt und Trigg ein Arbeitsprotokoll erschaffen, das die Basis für dieses Whitepaper bildet.

3 DESIGNPRINZIPIEN DES MOCHIMO PROTOKOLLS

NACH INVESTITIONEN IN KRYPTOWÄHRUNGEN und Beiträgen zu ihrer Entwicklung während der ersten und zweiten Krypto-Welle seit dem Jahr 2009 hat sich Anfang 2017 ein Team von Blockchain-Veteranen zusammengefunden, um gemeinsam das Mochimo Projekt zu starten.
Als Kryptowährungs-Puristen sahen sie es als eine ihrer ersten Aufgaben an, die Prinzipien festzuhalten, die das Design bestimmen sollten.

Die grundlegenden Ziele von MCM bestanden darin, eine zukunftssichere Kryptowährung, die wirklich dezentralisiert, nicht auf Vertrauen basierend („trustless"), unveränderlich und ohne Obergrenzen skalierbar wäre. Mit unserem Protokoll ist es uns gelungen, alle vier Grundsätze und noch weitaus mehr zu erreichen.

Zusammenfassend lässt sich sagen, dass das Mochimo Kryptowährungs-Netzwerk ein Peer-to-Peer, nicht auf Vertrauen basierendes, verteiltes Ledger mit schneller Konvergenz und starkem Schutz vor Doppelausgaben ist. Mochimo ist weder eine Fork, noch wäre es durch eine einfache Überarbeitung von bestehendem Code möglich gewesen, das zu erreichen, was sich hier umgesetzt findet. Stattdessen ist das Mochimo Krypto-Ökosystem eine komplette Neuimplementierung eines Blockchain Distributed Ledgers, das auf der ursprünglichen Vision von Satoshi Nakamoto basiert, aber vor dem Hintergrund jahrelanger Erfahrungs erweitert wurde.
Von den oben erwähnten Grundsätzen war die Dezentralisierung am wichtigsten.

Heute werden Kryptowährungen in zwei grundlegende Kategorien eingeteilt:

1. **Wirklich dezentral und damit nicht auf Vertrauen basierend („trustless")**
2. **Halb-zentralisiert**

Die halb-zentralen Währungen sollten ausnahmslos abgelehnt werden. Zentralisierung von allem - Börsen, Kreditinformationen, Währungen – lädt zu Angriffen ein. Anstelle eines unabhängigen Ledgers - der eigentlichen Essenz der Blockchain - erhalten wir eine zentralisierte Autorität, richtig oder falsch, die dem gesamten Netzwerk vorschreibt, wie der aktuelle Zustand des Ledgers ist.

3 DESIGNPRINZIPIEN DES MOCHIMO PROTOKOLLS

Natürlich könnten einige Leute diesen Mangel als ein Feature bezeichnen. Zentralisierte Systeme lenken Menschen oft von den inhärenten Mängeln in ihrer Architektur ab, indem sie außergewöhnliche Transaktionsdurchsatzwerte hervorheben. Sie erwähnen nicht, dass die hiermit verbundenen Kosten der Ausweidung des nicht auf Vertrauen basierenden Systems gleichkommen. Tatsächlich sind exorbitante Transaktionen pro Sekunde (“TPS”) oft der erste Hinweis darauf, dass die Entwickler eines Systems beabsichtigen, **die Kontrolle über die Vermögenswerte der Nutzer zu behalten.**

Wie übersetzt sich “schnelle Geschwindigkeit” in “Kontrolle”? Eine zentrale Autorität kann Hunderttausende (wenn nicht sogar Millionen) von TPS verarbeiten, nicht weil ihr Konsensmechanismus so effizient ist, sondern weil jeder Konsens umgangen wird. Um eine politische Analogie zu verwenden, sind Diktaturen effizient, aber die Regierung ist weder ein legitimer Vertreter des Volkes noch dient sie dem Volk. Das Hindernis für die Erreichung der Skalierbarkeit von Kryptowährungen besteht heute darin, dass die Geschwindigkeit der derzeitigen Konsensmechanismen einen Engpass darstellt.
Wie also können wir die Geschwindigkeit beibehalten oder erhöhen, ohne die Kontrolle an eine zentrale Autorität zu übergeben? Aus unserer Sicht sind dies die wichtigsten Herausforderungen in Bezug auf das Design:

- Sicherzustellen, dass die Größe der Blockchain nicht außer Kontrolle gerät.
- Die Bandbreitenanforderungen für die Kommunikation derart zu kontrollieren, dass sie für den Durchschnittsbürger zugänglich sind. Jeder sollte in der Lage sein, einfach und unkompliziert eine Node aufzusetzen und dem Netzwerk beizutreten, das Ledger vollständig zu synchronisieren und damit zu beginnen, Transaktionen zu verarbeiten und Blöcke zu minen.
- Eine schnelle Verbreitung von Transaktionen, Block-Updates und schnelle Konvergenz zu ermöglichen, realisiert durch einen effektiven und mathematisch belegbaren Modus der Schlichtung im Falle von Konflikten.

Um diese Probleme zu lösen, führt das Ökosystem von Mochimo mehrere Innovationen ein, darunter “ChainCrunch™”, das es jeder einzelnen Node im Netzwerk ermöglicht, einen vollständigen Überblick über das Ledger zu behalten, während alte Blöcke entsorgt werden.

3 DESIGNPRINZIPIEN DES MOCHIMO PROTOKOLLS

Mochimo zeichnet sich außerdem durch eine außergewöhnlich schnelle Konvergenz und die Reduzierung („pruning“) von verwaisten Abschnitten der Chain aus. Im Einklang mit der hier vorgestellten Vision verfügt Mochimo über einen der am besten dokumentierten Codes in der Krypto-Welt.

3.1 AUTONOME DEZENTRALISIERUNG

Unser erster Grundsatz ist, dass eine Kryptowährung, will sie wirklich dezentralisiert sein, keine Akteure vorsehen kann, weder die Miner noch die Entwickler, die in der Lage wären, nach der Veröffentlichung über das Regelwerk zu bestimmen. Daher wird der Code als alleiniges Gesetz fungieren, das das System regelt, und niemand sollte den Code kontrollieren.

Aus diesem Grund lehnt Mochimo alle Versuche jüngster Kryptowährungen ab, bedingungslos zu vertrauende Netzwerkknotenpunkte, Abstimmungsmechanismen, Proof-of-Stake-Algorithmen oder delegierte Proof-of-Stake-Algorithmen einzuführen. Darüber hinaus lehnen wir uneingeschränkt jede Konsolidierung der Mining Power ab, da sie es diesen Akteuren ermöglicht, das Regelwerk des Netzwerks mit roher Gewalt zu bestimmen. Jeder in Krypto eingeführte Mechanismus, der es einem bestimmten Teilnehmer ermöglicht, einen größeren Einfluss auszuüben als jeder andere Akteur, kann und wird es schließlich denjenigen in Machtpositionen ermöglichen, ihre Macht weiter und weiter zu bündeln. Dies wird letztendlich die Autonomie des Netzwerks beeinträchtigen. Diese Manipulation hat bereits in fast jeder bestehenden Kryptowährung stattgefunden und kann kollektiv als Tendenz zur Zentralisierung bezeichnet werden. Es wird langfristig zum Tod der betreffenden Ledger führen.

3.2 DAS SELBSTHEILENDE LEDGER

Das Mochimo-Team ist der Ansicht, dass jeder einzelne Netzwerkknoten in der Lage sein muss, den Zustand des Netzwerks, des Ledgers und einer bestimmten Transaktion zu bestimmen, ohne dass eine ranghöhere Quelle angefragt werden muss.
Das Vertrauen in eine einzige Autorität ist das schwache Glied eines jeden autonomen Systems.

Aus diesem Grund lehnt das Mochimo-Design das Konzept von “Master Nodes”, “Super Nodes”, “Trusted Nodes” und allen anderen Euphemismen ab, die einer zentralen Autorität

3 DESIGNPRINZIPIEN DES MOCHIMO PROTOKOLLS

die Möglichkeit geben sollen, das Verhalten des Netzwerks zu regeln. Kurz gesagt: Wenn das Netzwerk von den Parteien verlangt, dass sie in irgendeiner Weise Vertrauen zueinander gewinnen, um zu funktionieren, dann ist das betreffende Ledger veränderbar.

WENN DAS LEDGER IN IRGENDEINER WEISE VERÄNDERBAR IST, IST DIE WÄHRUNG WERTLOS.

Stattdessen bestimmen die MCM-Netzwerkknoten selbst mathematisch die „Master Chain“ und beschneiden autonom alle verwaisten Chains, wenn es innerhalb des Netzwerks zu Konflikten kommt. Ebenso werden Transaktionen und gelöste Blocks nicht über zentrale Knoten weitergeleitet, sondern über Multicast-Mechanismen an das gesamte Netzwerk weitergegeben.

Auf jeder Ebene lehnt das Mochimo-Protokoll die Zentralisierung von Verarbeitung, Transaktionsverteilung, Peer-Erkennung, Konfliktlösung, Abstimmung, sowie die Zentralisierung der Anwendung von Kollisionsregeln und Durchsetzung von Codeversionen ab. Alle diese Mechanismen sind Schwächen. Sie schaffen Möglichkeiten, das Ledger veränderbar zu machen, und jeder von ihnen kann von einer Gruppe missbraucht werden, um die Ergebnisse und den Zustand des Ledgers zu ändern und es veränderbar zu machen. Nur durch den Betrieb eines vertrauenswürdigen Systems, d.h. wo jeder Netzwerkknoten über alle Informationen verfügt, die er benötigt, um Entscheidungen zu treffen und einen Konsens zu erzielen, können die Endbenutzer der Währung dem Transaktionsnetzwerk wirklich vertrauen.

3.3 EGALITÄRE INKLUSION DER MINER

Die Skalierung ist das größte Problem, mit dem Kryptowährungen der ersten und zweiten Generation heute konfrontiert sind. Die meisten der heutigen Währungen in den Top-100 haben Computer-, Bandbreiten- und Speicheranforderungen, die mit einer höheren Rate wachsen, als es in Bezug auf die Hardware, die dem Durchschnittsbürger zur Verfügung steht, tragbar und zukunftsfähig wäre. Im Zuge der steigenden Schwierigkeit des Minings kann der Durchschnittsmensch nicht mehr am Miningprozess teilnehmen.

Sobald das Mining effektiv auf die größeren Unternehmen beschränkt ist, die über ausreichende Ressourcen verfügen, um leistungsstarke Computer- und Speicherressourcen bereitzustellen, beginnt die zentralisierte Kontrolle über einen Coin. Da das Mining zentralisiert ist, zentralisieren diese Miner auch die Netzwerkknoten. Dadurch beginnen sie, die Richtung der Entwicklung des Coins zu kontrollieren und verzögern oder verhindern jede Innovation, die ihrem Interesse als Miner schadet. Kurz darauf kommt es zu einer feindlichen Fork und anderem abträglichen Verhalten.

Ebenso will niemand in eine Situation eintreten, in der er immer machtlos sein wird. Wenn zudem die Entscheidungen immer gegen den betreffenden Akteur gerichtet sind, wird er schließlich die Währung zugunsten einer egalitären Situation verlassen.
Da es der zentralisierte Mehrheit nicht gelingt, die neueren und kleineren Spieler zu halten, entfernt sich die Währung von der Idee, einen nachhaltigen Wertspeicher zu schaffen, der täglich von der gesamten Bevölkerung genutzt werden kann. Sie entwickelt sich hin zu einer Währung, die nur die Interessen desjenigen widerspiegelt, der sie am meisten mined.

Alle Nutzer werden immer in der Lage sein, Mochimo zu minen, ohne von schlechten Akteuren an den Rand gedrängt zu werden.

4 DAS MOCHIMO DESIGN LÖST VIELE PROBLEME

MIT ZUNEHMENDER REIFE VON KRYPTOWÄHRUNGEN SIND VERSCHIEDENE, Probleme durch die stetig steigende Anwendung entstanden. Eine Vielzahl der Coins der zweiten Generation sind Versuche, eines oder mehrere dieser Probleme zu lösen. Im Gegensatz zu diesen stückweisen Protokollen hat das Mochimo-Team jedoch eine ganzheitliche und vorausschauende Lösung entwickelt, indem es eine Reihe von Innovationen im Bereich des Kryptowährungsdesigns integriert hat, die alle folgenden Probleme gelöst haben (die im Folgenden im Detail behandelt werden):

- Die Bedrohung durch Quantencomputer
- Eine langfristige Lösung für die Skalierbarkeit des Netzwerks
- Sicherstellung von FIFO-Transaktionen und Vermeidung von Transaktions-Warteschlangen (“queues”)
- Transaktionsdurchsatz und Sicherheit

4.1 DIE BEDROHUNG DURCH QUANTENCOMPUTER

Das erste und bemerkenswerteste Problem, das Mochimo löst, ist die Bedrohung des Kryptowährungsökosystems durch den sich schnell nähernden Aufstieg der Quantencomputer. Derzeit ist die Mehrheit der Blockchain-Systeme und Kryptowährungen durch quantenunsichere digitale Signaturalgorithmen geschützt. Am häufigsten wird ECDSA eingesetzt (verwendet von Bitcoin, Ethereum und allen ERC-20-Token), und er wird sich konfrontiert mit einem Quantencomputerangriff als hauchdünn herausstellen.

Das Brechen dieses elliptischen Kurvenalgorithmus mit herkömmlichen Computern ist rechenintensiv. Doch für Quantencomputer stellt es eines der ersten Entwicklungsziele dar. Vor diesem Hintergrund zeigen diese ECDSA-Kryptowährungen, obwohl eine bemerkenswerte Leistung, eine offen liegende Schwachstelle.[1] Sie können daher realistisch betrachtet nicht als langfristiger Wertspeicher angesehen werden. Es gibt auch keine Wunderheilung, die dem zugrunde liegenden Code dieser Kryptowährungen hinzugefügt werden kann, um sie quantenresistent zu machen.

Deshalb muss der Quantenwiderstand von Grund auf neu aufgebaut werden und darum haben wir unser Design nicht von einem bestehenden Protokoll geliehen oder darauf basiert.

4 DAS MOCHIMO DESIGN LÖST VIELE PROBLEME

Unternehmen und Einzelpersonen, die sich der Quantenmängel der ECDSA bewusst sind, haben damit begonnen, neue kryptografische Protokollstandards zu schreiben, die als “Post-Quantum“ sicher gelten. Die bemerkenswerteste dieser Organisationen ist die von der Europäischen Union finanzierte PQCRYPTO-Arbeitsgruppe. Ihr Dokument “ICT-645622” ist ein Referenzstandard für quantensichere Verschlüsselungsalgorithmen, die auf den aktuellen und zukünftigen Fähigkeiten von Quantencomputern basieren.

IM FEBRUAR 2018 BEAUFTRAGTE DAS MOCHIMO DEV TEAM HÜLSING mit der kompletten Überprüfung unseres kryptografischen Codes. Die Verwendung des WOTS+ Digital Signature Algorithmus durch das Mochimo-Projekt und unsere ANSI-C (1989) Implementierung dieses quantensicheren Algorithmus für unsere Adressen und das Protokoll wurde nun von Andreas Hülsing selbst, dem Entwickler des Algorithmus, gründlich überprüft. Unsere Implementierung erwies sich als frei von Fehlern und Hülsings abschließender Code Review wird auf der Mochimo-Website

Innerhalb dieses Standards haben sie eine Handvoll Digital Signature Algorithmen empfohlen, die unabhängig von den Verbesserungen der Quanteninformatik rechenintensiv bleiben.[2] Aus dieser Liste wählte das Mochimo-Entwicklungsteam das XMSS+ mit der WOTS+-Variante der Winternitz One-Time Signature aus, welche von Andreas Hülsing im September 2017 vorgeschlagen und bewiesen wurde. [3]

4 DAS MOCHIMO DESIGN LÖST VIELE PROBLEME

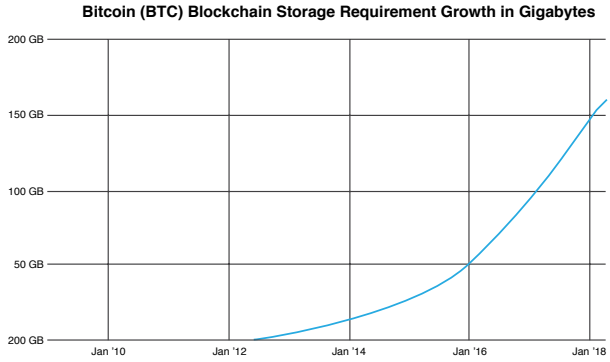
4.2 LANGFRISTIGE LÖSUNG ZUR NETZWERK-SKALIERBARKEIT

Mochimo ist ein Transaktionsnetzwerk; als solches steht die Skalierbarkeit im Vordergrund. Viele Protokolle haben es in unverantwortlicher Art und Weise zugelassen, dass ihre Blockchain auf unbestimmte Zeit wächst und regelmäßig Hunderte von Gigabyte und sogar Terabyte erreicht.

Im Falle von Bitcoin[4] können wir deutlich sehen, dass das Wachstum der Blockchain die Größe dieser etwa alle 12-16 Monate verdoppelt. Die Größe der Bitcoin-Blockchain, die eine vergleichsweise kleine Adressgröße und Signaturgröße aufweist, ist entlang einer Exponentialkurve gewachsen und liegt seit März 2018 bei über 180 GB Rohdaten. Ethereum, bekannt für seine häufigen Netzwerküberlastungen, hatte Stillstände, die durch ein viel aggressiveres Wachstum verursacht wurden, wobei die volle Blockchain-Größe (einschließlich der Traces) nun mehr als 1 TB an erforderlichem Speicherplatz beträgt.

Andere Währungen werden nicht besser abschneiden, wenn die Netzwerkanforderungen und die Größe der Blockchain zunehmen. Angesichts dieser Überlastung ist es leicht zu verstehen, warum es Widerstand gegen die Umsetzung von Quantensicherheitsmaßnahmen geben könnte. Die Größe der Adressen und Signaturen sind maßgeblich größer als die von Protokollen wie Bitcoin oder Ethereum.

Trotz der Überlastung behaupten diese Entwickler jedoch immer, dass Moores Vorhersagen über die Entwicklungsgeschwindigkeit der



MOCHIMOS RADIKALE CHAINCRUNCH™ LÖSUNG

zur Skalierung hört damit nicht auf. Es ermöglicht dem System auch, Speicherplatz zu sparen und die Geschwindigkeit der Datensuche radikal zu verbessern. Mit ChainCrunch™ können dem Netzwerk neue Knoten beitreten und innerhalb von Minuten statt Tagen oder Wochen vollständig synchronisiert werden. Diese Technologie ermöglicht eine beispiellose Skalierbarkeit, ohne dass große Mengen an Speicherplatz benötigt werden. Darüber hinaus ist die ChainCrunch™ Technologie nur eine Komponente einer Reihe von Innovationen im MCM-Protokoll, die eine nahezu sofortige Nachverfolgung von Adressbeständen und Transaktionsdaten ermöglichen.

4 DAS MOCHIMO DESIGN LÖST VIELE PROBLEME

Zukunftstechnologie schließlich zu ihrem außer Kontrolle geratenen Größenwachstum der Blockchain aufholen werden. Dieser Appell an “Moore’s Law” ist grundlegend fehlerhaft, da Kryptowährungskritiker empirisch ein Wachstum des Speicherverbrauchs über praktisch ALLE Blockchains hinweg beobachtet haben, das das vom Moore’s Law vorhergesagte technologische Wachstumsziel von 18 Monaten überschreitet.

Mochimo hat jedoch bereits das Problem des großen und unkontrollierbaren Blockchainwachstums mit einem innovativen Blockchain-Verarbeitungsalgorithmus namens ChainCrunch™ gelöst. ChainCrunch™ ist eine proprietäre Mochimo-Technologie, die es dem Nutzer ermöglicht, einen vollständigen Netzwerkknoten zu betreiben, aber nur einen kleinen Prozentsatz der historischen Blockchain-Daten zu pflegen. ChainCrunch™ ist durch HASH256 gesichert und quantensicher. Aufgrund dieser Innovation - die später in diesem Beitrag näher erläutert wird - wird die Größe der Mochimo-Blockkette nicht wachsen. Stattdessen bleibt es außerordentlich und dauerhaft klein, egal wie viele Jahre das Netzwerk arbeitet oder wie viele Transaktionen wir abwickeln.

4.3 NEUERFINDUNG VON TRANSAKTIONSGEBÜHREN ZUR SICHERSTELLUNG DER ABWICKLUNG NACH F.I.F.O.

Das Problem mit den bestehenden Transaktionsgebührensystemen besteht darin, dass sie ein egalitäres, dezentrales Netzwerk nehmen und es zerbrechen, indem sie Miner dazu anregen, Transaktionen in einer Reihenfolge durchzuführen, bei welcher die Bestbezahlte zuerst verarbeitet wird. Wenn Miner sich für die höchste Gebühr entscheiden können, lassen sie die

niedrigen oder gebührenfreien Transaktionen stundenlang im Speicher eines ausgelasteten Netzwerkes warten. Im Falle der Ethereum ICOs haben Teilnehmer absurde Beträge bezahlt, um “an der Schlange vorbeizuschreiten”. Dies ist kein Verhalten, das ein zuverlässiges, skalierbares System fördert. Nur die Änderung der Mining-Anreize kann diese Art von Verhalten stoppen.

WIE WERDEN ALSO DIE MINER JETZT MOTIVIERT? Die kleine, feste Transaktionsgebühr für Mochimo ermutigt die Miner, so viele Transaktionen wie möglich in ihren Kandidatenblock zu stapeln, um FIFO-Transaktionen sicherzustellen und Warteschlangen im Speicher zu vermeiden, wie sie in anderen

Das Mochimo-Entwicklungsteam ist der Ansicht, dass ein Anreiz für Miner, eine Transaktion der anderen vorzuziehen, kontraproduktiv für ein gesundes Netzwerk ist. Aus diesem Grund verfolgt das Mochimo-Protokoll einen neuartigen Ansatz zur Transaktionsabwicklung mit festen Gebühren. Die Kosten für den Versand einer Transaktion über das Mochimo-Netzwerk sind jetzt und werden immer 0.00000005 $MCM bleiben. Um Ihnen eine Vorstellung davon zu geben, wie gering diese Kosten sind: Wenn die Mochimo-Marktkapitalisierung wächst und die gesamte Altcoin-Marktkapitalisierung überholt und dadurch eine Mochimo-Münze 25.000 USD wert ist, wären die Transaktionskosten trotzdem weniger als 0,13 USD. Daher ist es ohne weiteres möglich, die Transaktionsgebühr für einige Jahre als trivial gering zu bezeichnen. Dies wird die tägliche Verwendung der Währung fördern.

4.4 TRANSAKTIONSDURCHSATZ UND SICHERHEIT

Das Mochimo-Protokoll verlangt, dass jede Transaktion die folgenden 6 Grundelemente aufweist: Quelladresse, Zieladresse, Änderungsadresse, gesendeter Betrag, Mining-Gebühr (fest) und Wechselgeldbetrag.

Es enthält auch die folgende wichtige Einschränkung: Die Quelladresse wird bei der Verwendung immer geleert und zerstört. Das System prüft, ob der gesendete Betrag plus der Wechselgeldbetrag plus die Mining-Gebühr dem Saldo der Quelladresse entspricht. Dadurch ist die Größe jeder Transaktion in Bytes festgelegt, die Ein- und Ausgänge sind trivial einfach und der Schutz vor einem Coin-Verlust ist simpel.

Darüber hinaus können Sie keine Transaktion senden, ohne eine vollständige Abrechnung des gesamten Währungsbestandes in der bestehenden Quelladresse durchzuführen. Sie können auch nicht mehrere Inputs und Outputs aggregieren. Die gesamte Wallet- und Saldenverwaltung für Adressen ist eine kundenseitige Funktion der Wallet-Software.

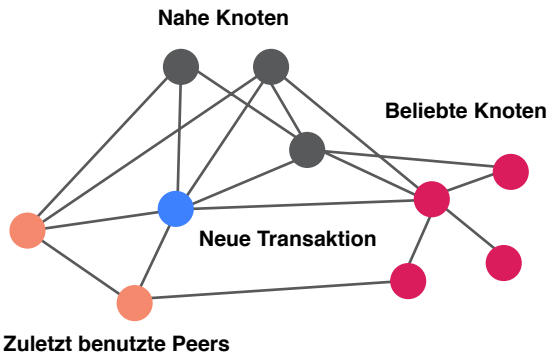
In Kombination mit der außergewöhnlichen Geschwindigkeitssteigerung, die durch die ChainCrunch™-Technologie von Mochimo ermöglicht wird, gehören die Lookup-, Validierungs- und Ausführungsgeschwindigkeiten von Transaktionen in unserem Netzwerk zu den schnellsten der Branche.

5 TECHNISCHER ÜBERBLICK ÜBER DIE WICHTIGSTEN MERKMALE

Noch wichtiger ist, dass bei ChainCrunch™ diese Geschwindigkeiten nicht langsamer werden oder stagnieren, wenn das Netzwerk an Größe oder Transaktionsdurchsatz zunimmt, sondern konstant schnell bleiben und mit zunehmender Verarbeitungshardware des durchschnittlichen Netzwerkknotens über die ursprüngliche Kapazität hinaus skaliert werden. Mochimo ist also schnell und wird mit der Zeit immer schneller.

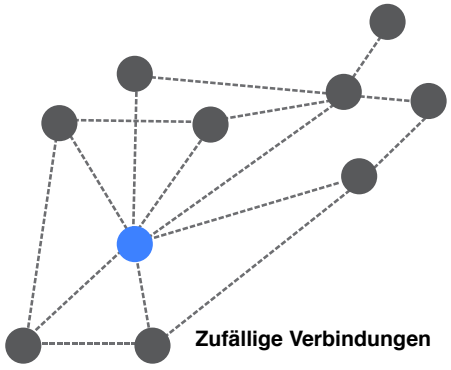
5.1 VERBINGUNDSMANAGEMENT UNTER VERWENDUNG DES RANDOM NETWORK MODELLS

Die durchschnittliche Blockchain
Nicht-zufällige Weitergabe von Informationen über das Blockchain-Netzwerk



Die durchschnittliche Blockchain wählt nur nahe, beliebte oder zuletzt verwendete Peers (Knoten). Wiederholtes Auslesen aus einer viel kleineren Gruppe ähnlicher Knoten ermöglicht verschiedenste Möglichkeiten das Netzwerk anzugreifen.

Mochimo Blockchain
Zufällige Weitergabe von Informationen über das Blockchain-Netzwerk



Jeder Knoten im Mochimo-Netzwerk öffnet und schließt zufällige Verbindungen über die gesamte Struktur des Netzwerks. Der Server füllt die 16-köpfige aktuelle Peer-Liste zufällig mit Verbindungen zweiten Grades und versucht, Verbindungen mit jeder einzelnen aufzubauen, wobei er immer fehlgeschlagene Verbindungen auflöst. Für jede fehlgeschlagene Verbindung gibt der Server einen GET_PEER an eine erfolgreiche Verbindung zweiten Grades aus, mischt die Antwort und füllt seine aktuelle Peerliste weiterhin mit eindeutigen Verbindungen dritten Grades.

ANSTATT SICH NUR MIT AKTUELLEN, BEKANNTEN ODER GEOGRAFISCH NAHEN PEERS ZU VERBINDEN, war das Designziel des MCM-Verbindungsmanagements, eine vertrauenswürdige Umgebung zu gewährleisten, in der jeder Knoten im Mochimo-Netzwerk zufällige Verbindungen über die gesamte Struktur des Netzwerks öffnet und schließt. Das Random Networks-Protokoll wurde entwickelt, um alle empfangenen Transaktionen schnell und asynchron an den Rest des Netzwerks zu verteilen. Dieses zufällige Netzwerkmodell wurde von Albert-Laszlo Barabasi in seiner Netzwerkwissenschafts-Publikation “Random Networks”5 formal analysiert.

Der Prozess: Die Serververteilung wird mit einer Auswahlliste bekannter Peers besetzt. Dies

sind nur die Standardknoten, die in der Verteilung enthalten sind. Diese Liste kann durch den Schalter -S über die Befehlszeile überschrieben werden, wobei der Benutzer entweder einen bestimmten Peer für die erste Verbindung oder eine Datei mit einer Liste von Peers für die Verbindung liefert. Obwohl das Mochimo Dev-Team diese bekannten Knoten eingerichtet hat, sind sie nicht anders als andere Knoten.

Bei der Initialisierung lädt der Server die bekannte Peer-Liste oder die vom Benutzer bereitgestellte Liste, mischt sie und wählt zufällig einen Peer aus, mit dem er sich verbinden kann. Bei der Verbindung gibt der Server den OP_CODE: GET_PEER aus, und falls erfolgreich, erhält er eine Kopie der aktuellen Peer-Liste von dieser Verbindung ersten Grades. Aus dieser Liste füllt der Server zufällig die 16 Mitglieder der aktuellen Peer-Liste mit Verbindungen zweiten Grades und versucht, Verbindungen mit jeder einzelnen aufzubauen, wobei er die fehlgeschlagenen Verbindungen abschneidet. Für jede fehlgeschlagene Verbindung gibt der Server einen GET_PEER an eine erfolgreiche Verbindung zweiten Grades aus, vermischt die Antwort und füllt im Weiteren seine aktuelle Peerliste mit eindeutigen Verbindungen dritten Grades.

EIN ROTIERENDES, ZUFÄLLIGES NETZWERK BEDEUTET, dass der Grad der Trennung zwischen zwei beliebigen Knoten im offenen Internet 16^D = N beträgt, wobei D die Anzahl der Grade der Trennung und N die Anzahl der Knoten im Netzwerk ist. Zum Beispiel, in einem Netzwerk mit genau 4096 Knoten, beträgt der durchschnittliche Grad der Trennung zwischen zwei beliebigen Knoten 16^3 = 4096, oder 3 Hops. Bei einem Netzwerk mit 65536 Knoten steigt der Durchschnitt auf 4 Hops.

Der Prozess des Füllens der Peer-Liste wiederholt sich, bis die aktuelle Peer-Liste 16 aktive Peers mit einer Trennung von mindestens zweitem oder drittem Grad vom ursprünglich bekannten Peer enthält. Wenn aktuelle Peers altern oder unerreichbar werden, werden Verbindungen vierten Grades in die aktuelle Peer-Liste auf die gleiche Weise rotiert, d.h. durch Extrahieren einer Peerliste aus dem zuletzt hinzugefügten Peer. Auf diese Weise rotiert jeder Mochimo-Server ständig durch neue und vielfältige Peers auf der ganzen Welt.

5 TECHNISCHER ÜBERBLICK ÜBER DIE WICHTIGSTEN MERKMALE

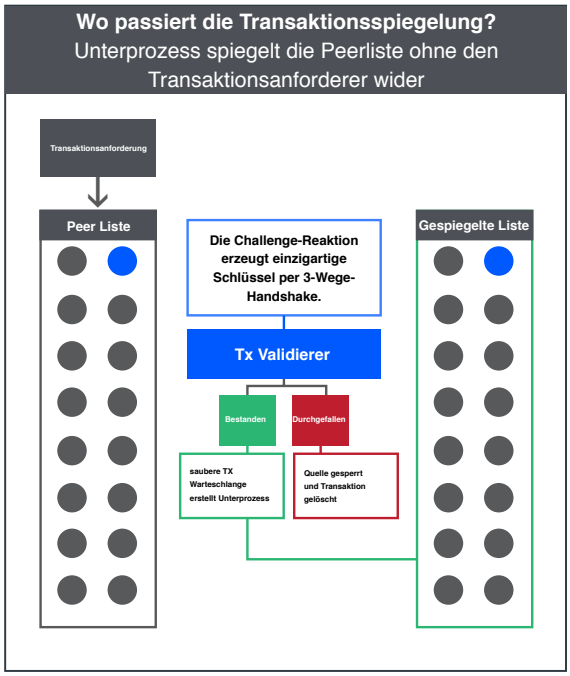
Dieses Zufallsnetzmodell kann unter anderem dazu verwendet werden, mathematisch die durchschnittliche Anzahl der Separationsgrade zwischen zwei beliebigen Knoten im Mochimo-Netzwerk zu bestimmen. Per Design durchsuchen wir das Netzwerk nach neuen Knoten, und jeder Mochimo-Server arbeitet dynamisch, um die schnelle Verbreitung von Transaktionsspiegelungen und Blockverteilungen sicherzustellen.

Wie skaliert es? Wenn bei diesem Netzwerktyp die Netzwerkgröße in Knoten N der aktuellen ungefähren Größe von Bitcoin entspricht, liegt die durchschnittliche Anzahl der Trenngrade zwischen zwei beliebigen Knoten im Mochimo-Netzwerk bei einer rotierenden, zufälligen Auswahl von k = 16 zwischen 3 und 4. Das bedeutet, dass Transaktionsverbreitung, Blockfindungsbenachrichtigung und netzwerkweite Konvergenz in maximal 3-4 Hops für die relevanten Daten erfolgen.[6]

5.2 TRANSAKTIONSSPIEGELUNG

Das Designziel der Transaktionsspiegelung ist die Nutzung des Random Network-Modells.

Um zu verstehen, wo die Spiegelung hineinpasst, muss zunächst bedacht werden, dass der primäre Serverprozess eine rotierende Liste aktueller Peers führt, Transaktionsanforderungen empfängt, sie in Warteschlangen stellt, ihre Signaturen validiert und dann Unterprozesse erzeugt, um die Transaktionsspiegelung durchzuführen.



Der Prozess: Der Server unterhält eine Socket-Tabelle mit Peer-Verbindungen zu den 16 neuesten Peers, alias der **Tabelle CURRENT_PEER**, und fragt jeweils nach eingegangenen Anfragen. Der Server führt einen Challenge-Response-Drei-Wege-Handshake durch, um für jede neue eingehende Anfrage eindeutige Kommunikationsschlüssel zu erstellen.

Eine Transaktion wird von einem Peer mit OP_CODE empfangen: OP_TX. Der Server

analysiert die Transaktion und übergibt sie an die Funktion Transaction Validator (TX_VAL).

Die Funktion **TX_VAL** überprüft eine Reihe von Parametern, darunter die folgenden: Werbt der Peer mit dem gleichen aktuellen Block wie das lokale System? Sind die Transaktionsparameter für das lokale Ledger gültig? Anschließend führt es die Erkennung von Duplikaten durch; wenn alle Transaktionsparameter korrekt sind, führt es eine Signaturvalidierung durch.

Wenn gültig, wird die Transaktion in den **CLEAN_TX_QUEUE** verschoben. Wenn die Transaktion schlecht ist, wird der Absender auf die schwarze Liste gesetzt und die Transaktion gelöscht. Bei sauberen Transaktionen erzeugt der Server asynchron einen Unterprozess, um den CLEAN_TX_QUEUE zu stützen. Der Unterprozess bedient die Warteschlange, indem er Transaktionen auf bis zu 16 Peers in der CURRENT_PEER_LIST spiegelt, exklusive des Peers, der die Transaktion verursacht hat, und dann beendet. In der Zwischenzeit setzt der Server seine normale Verarbeitungsschleife fort. Transaktionsspiegelung verwendet eine eingehende Source-Hash-Validierung, um sicherzustellen, dass Transaktionen nicht zu ihren Absendern zurückgespiegelt werden.

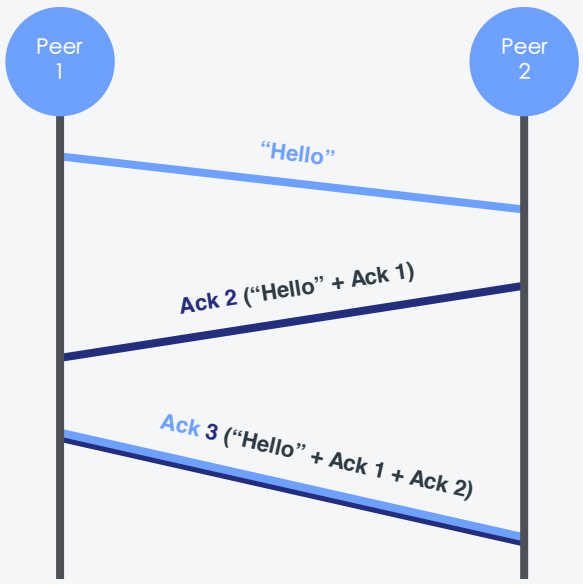
5.3 DREIWEGE-HANDSHAKE

In der gesamten Peer-to-Peer-Kommunikation setzt Mochimo ein Sicherheitsmerkmal ein, um Denial-of-Service-Angriffe, Spoofing und Man-in-the-Middle-Angriffe zu verhindern. Dieser Dreiwege-Handshake ist in vielen Netzwerkprotokollen zu finden; hier ist dargelegt, wie er in Mochimo funktioniert.

5 TECHNISCHER ÜBERBLICK ÜBER DIE WICHTIGSTEN MERKMALE

The process: Für jede neue ausgehende Verbindung generiert der Mochimo-Server einen zufälligen 16-Bit-Identifikator in einer Hello-Nachricht. Dieser Identifikator wird als ID1 bezeichnet. Der empfangende Peer antwortet mit einem Hello-Acknowledgement(ACK), der ID1 und seinen eigenen, einzigartigen, zufällig generierten Identifikator ID2 enthält. Der ursprüngliche Peer vervollständigt den Drei-Wege-Handshake mit einem ACK-ACK, das sowohl ID1 als auch ID2 enthält, und von diesem Zeitpunkt an gelten die Peers als "vollständig aneinander angrenzend". Sie können nun innerhalb dieser einen Sitzung senden und empfangen, indem sie den Datenverkehr entsprechend markieren.

Der Drei-Wege-Handshake



Alles ohne Ack 1+Ack 2 wird ignoriert.

Diese Identifikatoren sind einzigartig und gebunden an diese kurzlebige Sitzung und verhindern Denial-of-Service, der durch Node-Imaging und Man-in-the-Middle-Angriffe auftreten kann. Da ID1 & ID2 bei jeder neuen Transaktion neu verhandelt werden, bietet der Mochimo Drei-Wege-Handshake schnelle, einfache und verwertbare Sicherheit.

Alle Mitteilungen, die von Peers erhalten wurden, die:

1. Nicht Teil des Drei-Wege-Handshakes oder 2. Nicht mit den richtigen IDs signiert sind, werden einfach ignoriert.

5.4 SCHNELLE SERVER INITIALISIERUNG

Wenn der Mochimo-Server online geht, befindet er sich in einem von zwei Zuständen: Clean Boot oder Graceful Restart. Das System befindet sich nur dann im Modus Graceful Restart, wenn das System durch Eingreifen des Endbenutzers vom Monitor heruntergefahren wurde. In allen anderen Fällen, wenn das System ausfällt (z.B. um Konflikte zu lösen, eine

5 TECHNISCHER ÜBERBLICK ÜBER DIE WICHTIGSTEN MERKMALE

verwaiste Kette zu beschneiden oder aufgrund eines schwerwiegenden Fehlers), werden alle Zustandsinformationen für den Server bereinigt. Dazu gehören die Peer-Listen, das lokale Ledger, die vollständige Blockchain, alle Kandidatenblöcke auf der Festplatte usw.

Der Prozess: Das Mochimo-System behält die Stabilität, indem es in den Clean Boot-Zustand zurückkehrt und nutzt die schnelle Konvergenzfunktion von Mochimo, um seine Blockchain / sein lokales Ledger jederzeit wiederherzustellen, wenn Beschädigungen oder Konflikte bestätigt werden. Da Konflikte in der Mochimo-Implementierung äußerst selten sind, wird ein softwarebedingter Neustart nicht oft vorkommen.

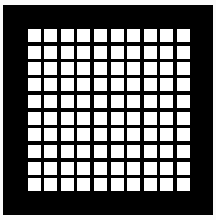
Beim Clean Boot initialisiert das System seine Kern-IP-Liste und erstellt eine Liste zufälliger Peers von mindestens dem zweiten und dritten Grad.

Der Server nutzt dann unsere MCM-eigene Quorum-Funktion, um die längste Blockchain unter den Peers zu identifizieren, die in seiner Peer-Liste vorhanden sind, alias die “Masterchain”. Die längste Blockkette ist die Kette mit der höchsten Arbeitsleistung. Um das zu identifizieren, pflegen Mochimo-Knoten eine historische Block-Trailerdatei mit Ketteninformationen, die auf Block 0, den ursprünglichen Genesis-Block, zurückgehen. In dieser Datei sind sowohl 100-Byte-Einträge für jeden jemals gelösten Block enthalten, die eine nachweislich verknüpfte Liste von Blockauflösungen,

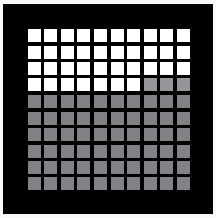
Clean Boot Prozess

Teil 1: Alles ist vollständig gelöscht und zwei Äonen an Blöcken werden aus der Trailer-Datei wiederhergestellt.

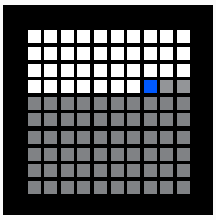
1. **Abrufen der ehemaligen Genesis Äon und Neuaufbau auf dem Knoten der geleert wurde.**



2. **Neuaufbau des aktuellen Äons bis zum aktuellen Block.**



3. **Warten auf die Formung eines neuen Blocks von einem Peer außerhalb des Quorums**



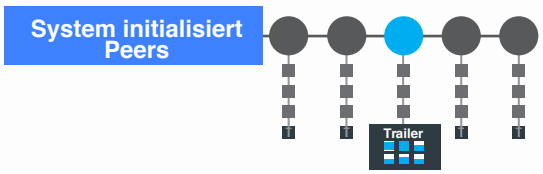
einschließlich Nonce und Hash, bilden, als auch die Zeitsignaturen, aus denen die Schwierigkeitsanforderung für jeden Block abgeleitet wird.

Die Datei wird von Anfang bis Ende durchlaufen; für jeden gelösten Block wird die Schwierigkeit, den Block zu lösen, zu einem Zähler zusammengefasst. Das Gewicht, das einem gelösten Block in der T-File-Kette gegeben wird, wird mit 2^(Schwierigkeit - 1) berechnet, was bedeutet, dass ein mit Schwierigkeit 35 gelöster Block das Doppelte des Gewichts von einem bei Schwierigkeit 34 gelösten Block hat. Da die T-File-Kette nachweislich verknüpft ist und gelöste Blöcke mit X-Schwierigkeiten enthält, können wir durch die Anforderung des T-File eines Peers den Gesamtaufwand berechnen, der an der Blockchain dieses Peers vom ursprünglichen Genesis-Block bis zum letzten Block geleistet wurde. Wenn das Gesamtgewicht dieser Chain das höchste im Netzwerk sichtbare Gewicht ist, befindet sich dieser Knoten in der Masterchain und kann vorläufig vertrauenswürdig sein.

Bestimmen der Masterchain

Teil 2: Das System vergleicht die Trailer-Dateien, um die Chain mit den Blöcken zu finden an denen am Meisten gearbeitet wurde

Knoten haben Trailer-Dateien mit historischen Daten



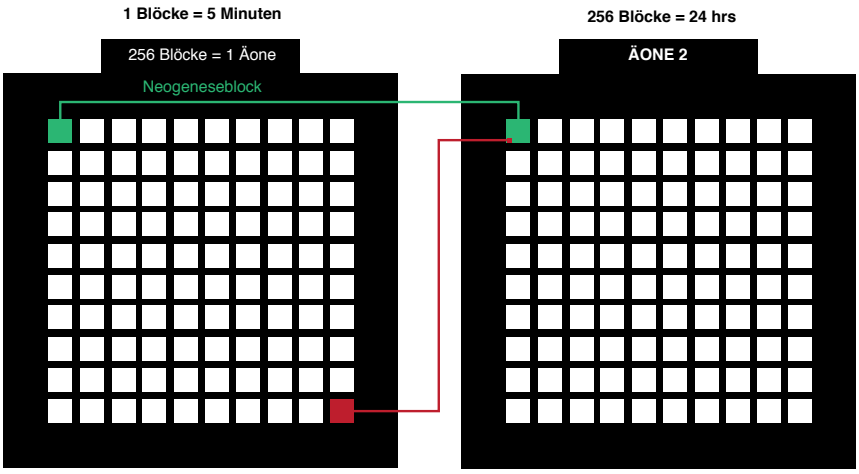
Der Server verwendet die MCM Quorum-Funktion, um die Trailer-Datei einzugeben, und damit die Schwierigkeit jedes Blocks zu “gewichten”. Die Kette mit den gewichtigsten Blöcken, die auf dem Weg

5 TECHNISCHER ÜBERBLICK ÜBER DIE WICHTIGSTEN MERKMALE

5.5 DIE TECHNOLOGIE HINTER CHAINCRUNCH™

Eine der wichtigsten proprietären Innovationen von Mochimo, ChainCrunch™, ermöglicht es dem Netzwerk, ein vollständiges Bild des Ledgers zu erhalten, Blöcke mit absoluter Gewissheit zu validieren und die lokale Datenbank eines neuen oder bestehenden Peers in wenigen Minuten statt Wochen neu aufzubauen. Darüber hinaus bietet ChainCrunch™ eine extrem schnelle Suche zur Transaktionsvalidierung unter Beibehaltung einer kleinen Blockkettengröße und eines Speicherbedarfs, der nur einen Bruchteil dessen ausmacht, was für alle anderen Kryptowährungsnetzwerke erforderlich ist.

Block & Äonen Details



Die Datenbank wird in den letzten Block geschrieben, gehasht und an eine

511 ist die maximale Anzahl an Blöcken, die zu jeder Zeitpunkt gehalten werden

Der Prozess: Ein Mochimo “Aeon” besteht aus 256 Blöcken, wobei die Blocklösungszeiten im Abstand von 337,5 Sekunden liegen, was zu einer durchschnittlichen Lebensdauer eines Aeons von 86.400 Sekunden beziehungsweise einem Tag führt. Der Mochimo-Server verfügt über eine lokale Datenbank auf der Festplatte, die eine sortierte, nach Adresse indizierte Liste jeder Adresse mit einem Guthaben im Netzwerk beinhaltet. Um dies in einen Kontext zu stellen, nimmt das System Ergänzungen und Deltas zu dieser Datenbank basierend auf den Blöcken 1 bis 255 vor, indem es gültige Transaktionen verarbeitet und die Änderungen bei jeder erfolgreichen Transaktion sortiert. Bei Block 255 angekommen, schreibt das System die Datenbank als Block 256 auf die Festplatte, hasht sie und hängt einen Trailer an. Dieser spezielle Block wird als “Neogeneseblock” bezeichnet. Vom Neogeneseblock aus fährt das System fort, indem es versucht, Block 257 zu lösen.

5 TECHNISCHER ÜBERBLICK ÜBER DIE WICHTIGSTEN MERKMALE

DER NEOGENESEBLOCK ERMÖGLICHT ES DEM SYSTEM, fast alle Blöcke in der Kette zu verwerfen, aber dennoch Transaktionen mit absoluter Gewissheit zu validieren. Mit ChainCrunch™ und dem Neogeneseblock muss das System nie mehr als 512 Blöcke auf der Festplatte speichern, da der Neustart eines neuen Systems einen Neuaufbau aus dem ersten vorherigen Neogeneseblock erfordert, d.h. nicht aus dem Neogeneseblock des aktuellen Aeons.

Wenn ein neues System online geht oder neu startet, weil eine Konkurrenzprüfung fehlgeschlagen ist, verwendet das System das zufällige Netzwerkmodell, um ein Quorum von Peers zu finden, die sich in der Masterkette befinden. Von diesem Zeitpunkt an stellt der Mochimo-Server einen Antrag an ein zufälliges Mitglied dieses Quorums und demontiert den ersten vorherigen Neogeneseblock.

DA ALLE 256 BLÖCKE EIN NEUER NEOGENESEBLOCK ERZEUGT WIRD, ist der angeforderte Block der aktuelle Block im Netzwerk minus (höchstens) 511 Blöcke. Somit bleibt die Anzahl der Blöcke, die für die vollständige Synchronisation eines Mochimo-Knotens erforderlich sind, immer zwischen 257 und 511. Wie im Diagramm auf Seite 16 ersichtlich, sind Sie, egal wo Sie sich im zweiten Äon befinden, immer weniger als 512 Blöcke von diesem ersten vorherigen Neogeneseblock entfernt.

Der nicht vertrauenswürdige Neogeneseblock, den der Server herunterlädt, enthält eine Roh-Datei des Ledgers, die die Salden jeder Adresse mit einem Saldo im Mochimo-Netzwerk auflistet. Der Mochimo-Server importiert dieses Ledger in einem nicht vertrauenswürdigen Zustand und verwendet es, um die folgenden 256 Blöcke in der Kette zu validieren, sie einzeln aus dem Quorum-Schwarm zu ziehen und sie gegen das Ledger zu validieren, sowie gegebenenfalls Anpassungen vorzunehmen und auf der lokalen Trailer-Datei aufzubauen.

Beim Erreichen des 256. Blocks erzeugt der Server einen eigenen Neogeneseblock, der in einem vorläufig vertrauenswürdigen Zustand existiert, und beginnt, alle vorhandenen Blöcke im aktuellen Aeon zu validieren, bis er zum gleichen aktuellen Block wie das Quorum gelangt und

den Blockhash gegen ihren validiert. Von diesem Zeitpunkt an wartet der Server darauf, dass ein neuer Block von einem Nicht-Quorum-Mitglied gelöst wird, und wenn dieser Block gegen den lokalen Zustand des Servers validiert werden kann, gilt der Server als “synchronisiert”, und lokalen Zustandsinformationen werden nun vertraut.

Der Server geht nun in den Zustand “Online” und sendet und empfängt wie gewohnt Transaktionen, versucht Blöcke zu lösen, etc. Dieser gesamte Prozess, von Anfang bis Ende, dauert in der Regel einige Minuten, je nachdem, wie lange es dauert, bis der nächste Block gelöst ist.

5.6 DER KONSENSALGORITHMUS

Ein Konsensverfahren beantwortet die Frage: “Woher weiß ein Knoten, ob er sich in der Masterchain oder in einer verwaisten Chain befindet?” Mochimo beantwortet dies, indem es die “BLOCK FOUND”-Meldungen entsprechend dem Arbeitsaufwand der Blockchain, auf der sich der werbende Peer befindet, validiert. Um diese Zahl zu erreichen, müssen wir zuerst die Idee der Trailer-Datei und des Chaingewichts vorstellen.

Der Prozess: Die Mochimo Trailer-Datei ist eine verknüpfte Liste aller Blocktrailer seit dem ursprünglichen Block 0 Genesis-Block, unabhängig davon, in welchem Aeon sich das System befindet oder wie viele Tausende oder Millionen von Blöcken vergangen sind. Jeder Trailer besteht aus 100 Bytes an Daten, so dass es, selbst wenn Mochimo Tausende von Jahre läuft, nicht unmöglich sein wird, diese Datenmenge zu speichern. Die Trailer-Datei ist unveränderlich, sie beinhaltet: die Start- und Lösungszeiten jedes Blocks, den Blockhash, die Nonce/Hash, die ihn gelöst hat, und die Schwierigkeitsstufe, die zum Zeitpunkt der Lösung vorhanden war. Diese verknüpfte Liste von Trailern wird verwendet, um die Gesamtarbeit der Kette zu berechnen, die behauptet, den Block gefunden zu haben. Dieser Wert wird als **“Gewicht” der Chain bezeichnet.**

> **DIE TRAILER-DATEI** ist Teil der zugrundeliegenden Mechanik von ChainCrunch™, die es uns ermöglicht, gewisse Blockdaten zu verwerfen, aber eine verkettete Liste von Blocklösungen vom ersten Block bis zum heutigen Tag zu behalten.

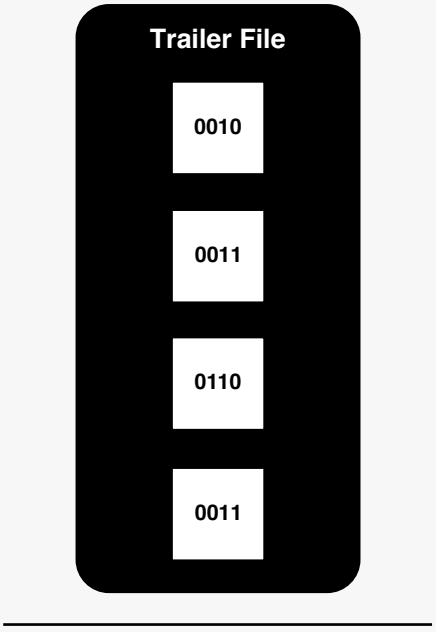
Um die geleistete Arbeit zu bestimmen, addieren wir einfach die Schwierigkeitswerte jedes Blocks in binärer Form. Ein Block, der beispielsweise mit einer Schwierigkeit von 34 gelöst wurde, benötigt einen Hash-Output mit 34 anführenden Nullen. Wenn wir das Gewicht berechnen, addieren wir 2^34 zum Gesamtgewicht der Chain, auf der dieser Block gelöst ist. Wenn der nächste Block mit einer Schwierigkeit von 35 gelöst wird, ist das Gewicht dieses Blocks doppelt so hoch wie das vorherige.

5 TECHNISCHER ÜBERBLICK ÜBER DIE WICHTIGSTEN MERKMALE

Mit zunehmender Größe und Anzahl der Miner nimmt die Schwierigkeit zu, so dass jeder gelöste Block im Laufe der Zeit schwerer wird als frühere Blöcke. Wichtig ist, dass wir bei der Validierung einer Trailer-Datei jeden Hash und Nonce, die Start- und Lösungszeiten, die Schwierigkeit (die aus Block 0 berechnet wird) und dann an das Gewicht für die kandidierende Kette anhängen.

Was ist Blockgewicht und was bewirkt es? **Das Gesamtgewicht des Blocks bestimmt, welche Chain zur Masterchain wird.**

Wir berechnen den Arbeitsaufwand für jeden Block im Binärformat und addieren ihn.



Erhalten des Gesamtgewichtes

Die Verwendung von Chaingewicht im Gegensatz zur Blockchainlänge in Bezug auf die Blocknummern ermöglicht es uns, schnell und deterministisch nachzuweisen, dass eine Chain mit mehr Gesamtarbeit erstellt wurde als eine andere. Es verhindert auch, dass böswillige Akteure versuchen, falsche Chains oder falsche Blöcke/Ledger in das Netzwerk einzubringen, da sie, um einen Block zu fälschen, die Summe aller Arbeiten, die das Netzwerk jemals ausgeführt hat, ausführen müssten. Wenn ein Peer einen Anspruch auf “BLOCK FOUND” stellt, sind diesem Anspruch vier Elemente beigefügt: der Hash des Blocks, der Hash des vorherigen Blocks, der Nonce und die Schwierigkeit.

Beim ersten Durchlauf überprüft der empfangende Peer, ob der durch die BLOCK FOUND-Nachricht angezeigte vorherige Blockhash mit dem aktuellen Block übereinstimmt. Wenn er die Nachricht findet, führt der Peer eine Überprüfung der angekündigten Schwierigkeit durch und bestätigt, dass sie mit der erwarteten Schwierigkeit übereinstimmt. Wenn diese Prüfung fehlschlägt, wird der werbende Peer auf die schwarze Liste gesetzt. Nachdem er bestätigt hat, dass sich der Peer sowohl in der richtigen Chain befindet als auch dass die Schwierigkeit übereinstimmt, fordert der lokale Peer den Block von diesem Peer an.

Nach dem Empfangen des Blocks ruft der Peer den ***Block Validator*** auf, der jede im Block enthaltene Transaktion validiert, einen Kandidatenblock konstruiert und diesen und den gelieferten Nonce durch den Mining-Algorithmus leitet.

Wenn der Block gültig ist, stoppt der lokale Peer das Mining, leert seine Transaktionswarteschlangen und ruft den ***Block Updater*** auf. Der Block Updater führt alle relevanten globalen Variablen-Deltas aus, aktualisiert die lokale Ledger-Datenbank und ruft, wenn wir uns an einer Äonengrenze befinden, die Neogenese-Routine auf. Wenn der Block-Updater die Ausführung beendet hat, kehrt der Zustand des Systems zu “In Sync” zurück, und wir haben “Konsens” mit dem Netzwerk gefunden.

5.7 KONFLIKTALGORITHMUS

Ein Konflikt tritt nur auf, wenn zwei oder mehr Knoten im Netzwerk einen Block ungefähr gleichzeitig lösen. Aufgrund des Random Networks-Modells und der Einstellung der durchschnittlichen Lösungszeit auf 337,5 Sekunden ist dies in Mochimo relativ selten, aber wenn es auftritt, konvergiert der Konsensalgorithmus das Netzwerk sehr schnell auf die folgende Weise.

Der Prozess: Nachdem ein Knoten eine “BLOCK FOUND”-Meldung erhalten hat, fährt er mit der Aktualisierung fort, wie im Abschnitt “Konsensalgorithmus” beschrieben. Wenn das Netzwerk in Konflikt gerät, was bedeutet, dass es mehr als eine Chain in dem Netzwerk mit der gleichen maximalen Länge gibt, können wir erwarten, dass der Knoten eine weitere Nachricht mit der Angabe “BLOCK FOUND” erhält, aber für den Block ist der Knoten bereits eingeschaltet. Diese Nachricht hat auch einen anderen Hash, der dem Knoten signalisiert, dass ein Konflikt vorliegt. Der Knoten ignoriert den BLOCK FOUND, da die angegebene Satznummer nicht höher ist als der aktuelle Block des Knotens und das angegebene Gewicht gleich ist.

In diesem Fall kann man mit Fug und Recht sagen, dass es im Netzwerk zwei Chains mit jeweils gleichem Gewicht gibt. Da die Blockpropagierung das Netzwerk in weniger als .5 Sekunden überspannen kann, wird erwartet, dass wir eine zweite Chain im Netzwerk in N * (337.5/.5) Blöcken sehen werden, wobei N die Anzahl der Knoten im Netzwerk ist. Das Ausmaß der Ausbreitung der zweiten Chain wird jedoch in den meisten Fällen stark eingeschränkt sein.

Die Art und Weise, wie dies gelöst wird, ist ziemlich einfach: Wenn der nächste Block abgebaut wird, unabhängig davon, wie viele gleichzeitige Ketten abgebaut wurden, erhalten alle Knoten eine BLOCK FOUND Meldung für eine höhere Blocknummer mit einem höheren Gewicht. Mit dieser Botschaft wird deutlich, dass der werbende Peer nicht in der gleichen Kette steht, da jeder beworbene BLOCK FOUND auch den Hash des vorherigen Blocks anzeigt. Da der Hash des vorherigen Blocks nicht mit unserem übereinstimmen wird, wissen wir, dass eine andere Chain als unsere behauptet, die Masterchain zu sein.

5 TECHNISCHER ÜBERBLICK ÜBER DIE WICHTIGSTEN MERKMALE

An dieser Stelle fragt der lokale Knoten den werbenden Peer nach seiner aktuellen Hashliste, um den Konflikt zu lösen. Der Peer antwortet, indem er den Hash jedes Blocks vom Neogeneseblock bis zum aktuellen Block bereitstellt. Der lokale Peer vergleicht diese Liste mit seiner eigenen Hashliste und sucht rückwärts nach einer Übereinstimmung. Wenn eine Übereinstimmung gefunden wird, befindet sich der Knoten in einer verwaisten Chain. Einige zusätzliche Validierungsprüfungen werden durchgeführt, um sicherzustellen, dass der Block nicht gefälscht wird, und nach der Validierung leert der empfangende Knoten alle Zustände und startet neu.

Man sollte beachten, dass die ultraschnelle Konvergenz des Netzwerks es uns ermöglicht, Konflikte zu lösen, indem Knoten, die sich in verwaisten Chains befinden, das Netzwerk verlassen und sich erneut synchronisieren lassen. Darüber hinaus ist es möglich, dass sich die Chain nicht nur einmal, sondern ein zweites Mal teilt. Die Wahrscheinlichkeit, dass dies geschieht, ist jedoch 1 in (N * (337.5/. 5)^2 Blöcke.

Es ist sehr wichtig zu verstehen, dass die Anzahl der aktiven Chains im Netzwerk nie größer als zwei ist, und eine BLOCK FOUND-Meldung nach einem Konflikt erhöht nicht die Anzahl der Chains im Netzwerk, sondern erhöht stattdessen die Anzahl der Knoten, die ihren Status zurücksetzen und den Neustart durchführen.

6 WICHTIGSTE ECKDATEN DER WÄHRUNG

Im Folgenden sind einige der wichtigsten Merkmale von Mochimo aufgeführt:

Maximale Versorgung: 76.533.882
Abbaubare Münzen: 71.776.816 (93,8%)
Mining-Algorithmus: Trigg's Algorithmus - PoW
Schwierigkeitsjustierung: Jeder Block
Zielblockzeit: 337,5 Sekunden
Genesis Block: 25. Juni 2018
Netzübertragungsentgelt: 0,000000005 MCM (fest)
Startbelohnung: 5,0 MCM / Block
Belohnungsschritt pro Block (einschließlich Block 373.760 4 Jahre: 0,00015 MCM)
Maximale Belohnung (Block 373.760): 59,17 MCM
Pro Block Belohnungssenkung (einschließlich Block 2.097.152 22 Jahre): 0,000028488 MCM
Letzte Belohnung (Block 2.097.152): 5 MCM
Gesamtdauer des Mining: ~22 Jahre

Details zum Premine:

Gesamter Premine: 6,34% (4,76 MIO. MCM)
Premine zur Vergütung des Entwicklungsteam: 4,18% (3,2 MIO. MCM)
Restlicher Premine (verwaltet von der Mochimo Foundation): 2,16% (1,56 Mio. MCM)
Genesis Block: 25. Juni 2018 23:40 UTC

7 Endnoten

1. Bernstein, et al., https://eprint.iacr.org/2017/314.pdf
2. PQCRYPTO, https://pqcrypto.eu.org/docs/initial-recommendations.pdf
3. Hülsing, https://eprint.iacr.org/2017/965.pdf
4. https://blockchain.info/charts/blocks-size?timespan=all
5. Barabasi, Albert-Laszlo, http://barabasi.com/f/624.pdf
6. BITNODES, https://bitnodes.earn.com/