

WATT NETWORK

Zentrale Speichernetzwerke der nächsten Generation

(Version1.0.0)

Katalog

Vorwort.....	1
Zitat: Warum ist verteilte Speicherung so wichtig?.....	1
I .Was ist verteilter Speicher basierend auf Blockchain?.....	1
II .Status der Branche für verteilte Speicherung in Blockketten.....	2
III .Problem: Verteilter Speicher ist nicht in der Lage, die Öffentlichkeit zu erreichen, und ein großer Teil des Benutzerspeicherplatzes wird nicht genutzt.....	3
IV .Lösung: WATT-Auslagerung und verteilte Speicherung auf mobilen Endgeräten.....	4
V .Einführung in das Protokoll des Konsenses von Sternen.....	5
VI.WATT-Wiederholung des SCP.....	6
VII. Einführung in den Konsensalgorithmus für WATT Mobile Distributed Storage.....	8
VIII. WATT-Wirtschaftsmodell: Gleichgewicht zwischen Knappheit und Zugänglichkeit..	11
IX. Von Governance-Crowd erstellte und öffentlich verwendete Kryptowährung.....	14
X . Roadmap / Bereitstellungsplan.....	15

Vorwort

Da die Welt immer digitaler wird, wird die dezentrale Speicherung (IPFS) zu einem natürlichen Trend in der Entwicklung der digitalen Wirtschaft. WATT wird das erste dezentrale Speichernetzwerk sein, das von allen im täglichen Leben genutzt wird. Dies ist ein großer Fortschritt bei der Einführung von Blockchain und verteiltem Speicher in der Welt.

Unsere Mission: Aufbau einer intelligenten Vertragsplattform für verteilten Speicher, die normale Menschen nutzen können und die sicher und einfach zu bedienen ist.

Unsere Vision: Unter dem Einfluss von WATT (dem weltweit am häufigsten genutzten dezentralen Speichernetzwerk) den umfassendsten dezentralen Speichermarkt der Welt zu etablieren.

Zitat: Warum ist verteilte Speicherung so wichtig?

Die Welt wird digitalisiert. Seit der Geburt der menschlichen Zivilisation haben die Menschen verschiedene Datenspeicherungs- und Übertragungstechnologien erfunden, und die menschliche Zivilisation kann in Form von Daten vererbt und bewahrt werden. Von den frühesten Orakeln bis zu modernen Computern hat die Geschwindigkeit und Dichte des Wissensaustauschs zusammen mit der Weiterentwicklung der menschlichen Technologie stetig zugenommen. Daten werden schnell produziert, übertragen, verwendet und gespeichert. Insbesondere mit der allmählichen Reife und Anwendung des Internet der Dinge in den letzten Jahren wird die Erzeugung und Übertragung von Daten ein beispielloses Ausmaß und eine beispiellose Geschwindigkeit erreichen. Das Datenanalyseunternehmen Statista hat Statistiken und Prognosen zu Angebot und Nachfrage von Internet-Datenspeicherung und Datenfluss erstellt. Aus globaler Sicht Das Speicherangebot entspricht nicht der Nachfrage nach Datenspeicherung. Darüber hinaus wird die Kommunikationstechnologie der fünften Generation (5G) kommerzialisiert, was das Layout des Internet der Dinge erheblich fördern wird. Die Kosten für die Speicherung und Übertragung von Daten werden unweigerlich zu einem Engpass, der die Entwicklung der Technologie einschränkt. Das Speichern und Übertragen von Daten zu geringeren Kosten ist zu einem dringenden Problem geworden, das gelöst werden muss. Verteilter Speicher basierend auf Blockchain bietet uns eine neue technische Lösung, mit der die Kosten für Datenspeicherung und -übertragung erheblich gesenkt und gleichzeitig die Sicherheit der Datenspeicherung verbessert werden können.

I .Was ist verteilter Speicher basierend auf Blockchain?

Ein verteiltes Datenspeichersystem ist ein Computernetzwerk, in dem Informationen normalerweise repliziert auf mehreren Knoten gespeichert werden. Wird normalerweise speziell verwendet, um auf eine verteilte Datenbank zu verweisen, in der Benutzer Informationen auf mehreren Knoten speichern, oder auf ein Computernetzwerk, in dem Benutzer Informationen auf mehreren Peer-to-Peer-Netzwerkknoten speichern. Verteilter Speicher ist relativ zu zentralem Speicher. Kurz gesagt bedeutet dies, Daten auf

mehreren Knoten zu speichern. Die Kombination von Blockchain und verteiltem Speicher ist ein "Blockchain-basiertes verteiltes Speichersystem". Dieses System kann als Kategorie der Sharing Economy angesehen werden. Die Anbieter und Nachfrager von Speicher- und Verkehr handeln mit Daten und Verkehr durch die Blockchain. Das Netzwerk erreicht allmählich das Gleichgewicht von Angebot und Nachfrage unter dem Gleichgewicht der Blockchain. Zu den Teilnehmern am System gehören: Speicher- und Verkehrsanbieter (die ihre eigenen Speichergeräte über das Netzwerk mit dem System verbinden, um Datenspeicherungs- und Verkehrsdienste bereitzustellen) sowie Speicher- und Verkehrsnachfrager (die für Speicherplatz und Zugriff auf das System bezahlen) Nutzung des Verkehrs) .

II .Status der Branche für verteilte Speicherung in

Blockketten

Die Forschung und Entwicklung von verteilten Speicherprojekten auf Basis von Blockchain begann von 2014 bis 2015. Bis heute sind es ungefähr 5 Jahre. Das repräsentativste ist das IPFS + Filecoin-Projekt, das derzeit entwickelt wird. Das System besteht aus zwei Protokollen: dem IPFS-Protokoll und dem Filecoin-Protokoll. IPFS-Protokoll: Der vollständige Name lautet InterPlanetary File System und ist definiert als: Ein Punkt-zu-Punkt-Hypermedia-Übertragungsprotokoll, ähnlich dem HTTP-Protokoll. Filecoin-Protokoll: Ein verteiltes Speicherprojekt, das auf Blockchain basiert.

Betrachten wir zunächst die Probleme, die durch diese beiden Protokolle gelöst werden, und ihre funktionale Positionierung. IPFS: Datenverteilung und Positionierung (Datenübertragungsprotokoll, ähnlich dem HTTP-Protokoll). Übertragung: Daten werden zwischen Knoten übertragen. Speicherort: Datenadressierung, suchen Sie den Speicherort der Daten. Filecoin: Datenspeicher (ähnlich einem Cloud-Speicher). Speicherplatztransaktion: Speicherung zwischen Benutzern und Bergleuten. Bei Weltraumtransaktionen "hängen" Bergleute ihren Speicherplatz zum Verkauf an das System, und Benutzer kaufen Speicherplatz, um ihre Daten zu speichern. Bandbreitentransaktion: Datenverkehrstransaktionen zwischen Benutzern und Bergleuten, Bergleute sehen ihre gespeicherten Daten zum Verkauf und Benutzer zahlen für Downloads. Blockchain-Netzwerkverwaltung: Bergleute pflegen das Netzwerk durch Beiträge, Erhalten Sie zusätzliche Vorteile. Speicherplatzhandel und Bandbreitenhandel werden zusammen als Wertbörsenmarkt bezeichnet. Filecoin löst den Wertaustausch von Datenspeicherung und Datendownload über die Blockchain. Die Gesamtzahl der Datei-Token beträgt 2 Milliarden. Ähnlich wie beim Bitcoin-System erfolgt die Verteilung der ersten Token durch "Bergbau" durch Bergleute. Die Token-Ausgabe von Filecoin erfolgt linear.

Eine der Herausforderungen bei der Verwaltung verteilter Transaktionsaufzeichnungen ist die Sicherheit - insbesondere, wie ein offenes und bearbeitbares Hauptbuch erstellt und gleichzeitig betrügerische Aktivitäten verhindert

werden können. Um dieser Herausforderung zu begegnen, führte filecoin einen neuartigen Prozess namens Mining ein (unter Verwendung eines Konsensalgorithmus "Proof of Work"), um festzustellen, wer "vertrauenswürdig" ist, und aktualisiert so die gemeinsame Aufzeichnung von Transaktionen. Sie können sich Mining als ein wirtschaftliches Spiel vorstellen, das "Validatoren" dazu zwingt, ihren Wert zu beweisen, wenn sie versuchen, Transaktionen zum Datensatz hinzuzufügen. Zur Überprüfung muss der Prüfer eine Reihe komplexer Rechenprobleme lösen. Der Mitwirkende, der dieses Rätsel zuerst löst, wird dafür belohnt, dass der neueste Transaktionsblock freigegeben wurde. Durch die Veröffentlichung des neuesten Transaktionsblocks können Validatoren einen Belohnungsblock "abbauen". Dieser Prozess ist sehr sicher, erfordert jedoch eine enorme Rechenleistung und einen enormen Energieverbrauch, da Benutzer tatsächlich "Geld verbrennen", um Computerprobleme zu lösen, wodurch mehr FileCoin verdient wird. Das Verhältnis von verbranntem Geld zu Belohnung ist so strafend, damit es immer im Eigeninteresse des Validators liegt, ehrliche Transaktionen in FileCoin-Datensätzen zu veröffentlichen

III. Problem: Verteilter Speicher ist nicht in der Lage, die Öffentlichkeit zu erreichen, und ein großer Teil des Benutzerspeicherplatzes wird nicht genutzt.

In den frühen Tagen von FileCoin überprüften nur wenige Personen Transaktionen und bauten den ersten Block ab. Jeder konnte FTL verdienen, indem er die FileCoin-Bergbausoftware auf einem PC ausführte. Als FileCoin populär wurde, erkannten intelligente Bergleute, dass sie mehr verdienen könnten, wenn sie mehr als einen Computer hätten.

Da der Wert von FileCoin weiter wächst, beginnen viele Unternehmen mit dem Bau von Minen. Diese Unternehmen haben spezialisierte Chips ("ASIC") entwickelt und diese ASIC-Chips verwendet, um eine riesige Serverfarm für die Gewinnung von FileCoin aufzubauen. Das Aufkommen dieser riesigen Bergbauunternehmen hat den FileCoin-Goldrausch gefördert und es für normale Menschen schwierig gemacht, zum Netzwerk beizutragen und Belohnungen zu erhalten. Ihre Bemühungen haben auch begonnen, immer mehr Rechenenergie zu verbrauchen, was zu zunehmend ernst globalen Umweltproblemen führt.

Die Bequemlichkeit des Mining von FileCoin und der anschließende Aufstieg von FileCoin-Minen trugen schnell zur großen Konzentration der Produktivität und des Wohlstands des FileCoin-Netzwerks bei. Um einige Hintergrundinformationen bereitzustellen, befinden sich 87% von FileCoin im Besitz von 1% des FileCoin-Netzwerks, von denen viele in den Anfangszeiten fast kostenlos abgebaut wurden. Ein weiteres Beispiel ist Bitmain, einer der größten Mining-Vorgänge von FileCoin. Hat Milliarden von Dollar an Umsatz und Gewinn verdient.

Die Machtkonzentration im FileCoin-Netzwerk ist für normale Menschen sehr schwierig und teuer. Wenn Sie FileCoin erhalten möchten, ist Ihre einfachste Option:

1. Grabe alleine. Solange Sie spezielle Hardware haben (wenn Sie interessiert sind, finden Sie hier eine Plattform bei Amazon!) Und dann einkaufen gehen. Wissen Sie nur, dass der Energieverbrauch der Energie des gesamten Schweizer Landes entspricht und Sie nicht zu viele Ressourcen abbauen können, da Sie mit großen Serverfarmen aus der ganzen Welt konkurrieren.

2. Kaufen Sie FileCoin an der Börse. Heute, zum Zeitpunkt des Schreibens, können Sie FileCoin zu einem Stückpreis von 3.500 USD pro Münze kaufen (Hinweis: Sie können einen Teilbetrag von FileCoin kaufen!). Da der Preis für FileCoin ziemlich instabil ist, ist dies natürlich auch erforderlich enorme Risiken.

FileCoin demonstrierte zum ersten Mal, wie Kryptowährung das aktuelle Finanzmodell brechen kann, sodass Menschen ohne Behinderung eines Dritten handeln können. Die Zunahme von Freiheit, Flexibilität und Datenschutz führt weiterhin dazu, dass die digitale Währung unweigerlich zu einer neuen Norm wird. Obwohl FileCoin viele Vorteile hat, aber seine (vielleicht unbeabsichtigte) Konzentration von Geldern und Macht hat große Hindernisse für Mainstream-Anwendungen gebracht. Das Kernteam von WATT führte eine Studie durch, um zu verstehen, warum Menschen nicht bereit sind, in das Feld Kryptowährung einzutreten. Die Menschen haben immer geglaubt, dass das Risiko von Investitionen / Bergbau ein wesentliches Hindernis für den Markteintritt darstellt.

FileCoin basiert auf Festplatten mit großer Kapazität für das Mining, die zu zentralisiert und für die breite Öffentlichkeit monetarisiert sind. Mit der Entwicklung der Mobiltechnologie verfügen die Endgeräte der Benutzer über einen großen freien Speicherplatz, und die Kapazität, die nicht genutzt ist, ist eine enorme Speicherverteilung. Auf dem Markt für mobile Speicher bietet WATT eine innovative verteilte Speicherung mobiler Wörter basierend auf dem freien Speicherplatz des mobilen Terminals.

IV. Lösung: WATT-Auslagerung und verteilte Speicherung auf mobilen Endgeräten

Nachdem das WATT-Kernteam diese Haupthindernisse für die Einführung identifiziert hatte, begann es, einen Weg für normale Menschen zu finden, um Minen abzubauen (oder Kryptowährungsbelohnungen durch Überprüfung von Transaktionen in verteilten Transaktionsdatensätzen zu erhalten). Als Vormund besteht eine der größten Herausforderungen bei der Pflege verteilter Transaktionsaufzeichnungen darin, sicherzustellen, dass Aktualisierungen dieser öffentlichen Aufzeichnungen nicht betrügerisch sind. Obwohl sich der Prozess der Aktualisierung von Datensätzen bei Bitcoin bewährt hat (Energie / Geld verbrennen, um die Glaubwürdigkeit zu beweisen), ist er nicht sehr benutzerfreundlich (oder umweltfreundlich!). Für WATT haben wir eine zusätzliche Entwurfsanforderung eingeführt, dh SPC verwendet einen Konsensalgorithmus, der sehr benutzerfreundlich ist und unter idealen Umständen auf PCs und Mobiltelefonen abgebaut werden kann.

Beim Vergleich vorhandener Konsensalgorithmen (der Prozess der Aufzeichnung von Transaktionen in einem verteilten Hauptbuch) ist das Stellar-Konsensprotokoll zum Hauptkandidaten für die Unterstützung des benutzerfreundlichen Mobile-First-Mining

geworden. Das Stellar Consensus Protocol (SCP) wurde von Davidmazi, Professor für Informatik an der Stanford University, entworfen, der auch Chefwissenschaftler der Stellar Development Foundation ist. Scp verwendet einen neuen Mechanismus namens föderierte byzantinische Vereinbarung (föderierte byzantinische Vereinbarung), um sicherzustellen, dass die Aktualisierung des verteilten Hauptbuchs korrekt und glaubwürdig ist. Scp wird auch in der Praxis über die Stellar-Blockchain bereitgestellt, die seit 2015 ausgeführt wird.

V. Einführung in das Protokoll des Konsenses von Sternen

WATT verwendet andere Arten von Konsensalgorithmen und basiert auf dem Stellar Consensus Protocol (SCP) und einem Algorithmus namens Federated Byzantine Agreement (FBA). Dieser Algorithmus hat keine Energieverschwendung, aber sie müssen viele Netzwerknachrichten austauschen, damit Knoten einen "Konsens" darüber erzielen können, was der nächste Block sein soll. Jeder Knoten kann unabhängig bestimmen, ob eine Transaktion gültig ist. Beispielsweise wird die Berechtigung zum Durchführen des Konvertierungs- und Wiederholungsaufwands basierend auf der verschlüsselten Signatur und dem Transaktionsverlauf bestimmt. Damit sich ein Computernetzwerk jedoch darauf einigen kann, welche Transaktionen in einem Block aufgezeichnet werden sollen und in welcher Reihenfolge diese Transaktionen und Blöcke angeordnet sind, müssen sie sich gegenseitig Nachrichten senden und mehrere Abstimmungsrunden durchführen, um einen Konsens zu erzielen. Intuitiv, Die Informationen von verschiedenen Computern im Netzwerk darüber, welcher Block der nächste Block ist, sehen folgendermaßen aus: "Ich schlage vor, dass wir alle dafür stimmen, dass Block a der nächste Block ist"; "Ich stimme dafür, dass Block a der nächste Block ist"; "Ich bestätige, dass die meisten Knoten, denen ich vertraue, auch für Block a stimmen." "Aus diesem Konsensalgorithmus kann der Knoten schließen: "a ist der nächste Block; Mit Ausnahme von a ist kein anderer Block der nächste Block"; obwohl die obigen Abstimmungsschritte viele zu sein scheinen, ist das Internet schnell genug und die Informationen sind leichtgewichtig, so dass dieser Konsensalgorithmus nicht nur ein Beweis für die Arbeit ist. Hauptvertreter dieses Algorithmus werden als Byzantine Generals Problem-Algorithmus bezeichnet. Einige der heutigen Top-Blockchains basieren auf BFT-Varianten wie NEO und Ripple.

Eine der Hauptkritikpunkte von BFT ist, dass es einen zentralen Punkt hat: Da es sich um eine Abstimmung handelt, wird die Menge der Knoten, die an der Abstimmung für das "Quorum" teilnehmen, zu Beginn zentral vom Ersteller des Systems bestimmt. Der Beitrag von Fba besteht darin, dass jeder Knoten anstelle eines von einer Zentralregierung festgelegten Quorums eine eigene "Quorumgruppe" eingerichtet hat. Diese Quorumgruppen werden wieder ein anderes Quartal bilden. Neue Knoten können dezentral dem Netzwerk beitreten: Sie deklarieren die Knoten, denen sie vertrauen, und überzeugen andere Knoten, ihnen zu vertrauen, müssen jedoch keine zentrale Behörde überzeugen.

SCP ist eine Instanz von FBA. Im Gegensatz zu FileCoin und dem herkömmlichen Proof-of-Work-Konsensalgorithmus für digitale Währungen, der Energie verbraucht, schützen SCP-Knoten gemeinsam genutzte Datensätze, indem sie sicherstellen, dass

andere Knoten im Netzwerk vertrauenswürdig sind. Jeder Knoten im Netzwerk erstellt eine Quorumslice, und eine Quorumslice besteht aus anderen Knoten im Netzwerk, die sie für vertrauenswürdig halten. Der Bereich richtet sich nach der Quorumgruppe seiner Mitglieder, und nur wenn und nur wenn ein Teil der Knoten im Quantum auch die Transaktion akzeptiert, akzeptiert der Validator die neue Transaktion. Da die Validatoren des gesamten Netzwerks ihre Kriterien erstellen, helfen diese Kriterien den Knoten, einen Konsens über Transaktionen unter der Voraussetzung der Gewährleistung der Sicherheit zu erzielen. Sie können mehr über das Stellar Consensus Protocol erfahren, indem Sie sich dieses kurze 7-minütige Erklärungsvideo oder die technische Zusammenfassung von SCP ansehen.

VI. WATT-Wiederholung des SCP

Der Konsensalgorithmus von WATT basiert auf SCP. Scp wurde offiziell bewiesen [Mazieres2015] und wird derzeit im Stellar-Netzwerk implementiert. Im Gegensatz zu StellarNetwork, das sich hauptsächlich aus Unternehmen und Institutionen (wie IBM) zusammensetzt, beabsichtigt WATT, persönlichen Geräten zu ermöglichen, auf Protokollebene Beiträge zu leisten und Belohnungen zu erhalten, einschließlich Mobiltelefonen, Laptops und Computern. Im Folgenden wird beschrieben, wie WATT SCP auf Personal Mining anwendet.

Der Benutzer kann zwei Rollen spielen, nämlich:

- **Minenarbeiter.** Benutzer der mobilen WATT-App bestätigen einfach, dass sie nicht jeden Tag "Roboter" sind. Dieser Benutzer überprüft seine Existenz jedes Mal, wenn er sich bei der Anwendung anmeldet. Sie können die App auch öffnen, um eine Transaktion anzufordern (z. B. WATT verwenden, um eine Zahlung an ein anderes führendes Unternehmen zu leisten).

- **Knoten.** Ein Pionier, der mobile WATT-Anwendungen verwendet, ein Mitarbeiter und WATT-Knotensoftware auf seinem Desktop oder Laptop ausführt. Die WATT-Knotensoftware ist die Software, die den Kern-SCP-Algorithmus ausführt. Diese Software bezieht sich auf die von den Mitwirkenden bereitgestellten Vertrauensdiagramminformationen.

Benutzer können mehrere oben erwähnte Rollen spielen. Alle Rollen sind erforderlich, daher erhalten alle Rollen täglich neue WATT-Münzen, sofern sie an diesem Tag teilnehmen und einen Beitrag leisten. In der losen Definition von "Bergmann (Bergmann)" bezieht sich "Bergmann" auf Benutzer, die neue Münzen als Beitragsbelohnung erhalten, und alle Rollen gelten als WATT-Bergarbeiter. Unsere Definition von "Mining" ist weiter gefasst als der traditionelle "Implementierungsnachweis-Konsens-Algorithmus", wie in Bitcoin oder Ethereum.

1. Knoten

Zur Vereinfachung des Lesens definieren wir den richtigen Verbindungsknoten, der im SCP-Artikel erwähnt wird, als vollständigen Knoten. Aus Gründen der Lesbarkeit definieren wir das Haupt-WATT-Netzwerk als Sammlung aller vollständigen Knoten im WATT-Netzwerk. Die Hauptaufgabe jedes Knotens besteht darin, ihn so zu konfigurieren,

dass eine ordnungsgemäße Verbindung zum Haupt-WATT-Netzwerk hergestellt wird. Intuitiv, Ein Knoten, der falsch mit dem Hauptnetzwerk verbunden ist, ähnelt einem Blockchain-Knoten, der nicht mit dem Haupt-Bitcoin-Netzwerk verbunden ist.

2. Benutzer der mobilen App

Wenn Pioneer bestätigen muss, dass eine bestimmte Transaktion ausgeführt wurde (z. B. π erhalten hat), wird die mobile App geöffnet. Zu diesem Zeitpunkt stellt die mobile Anwendung eine Verbindung zu einem oder mehreren Knoten her, um abzufragen, ob die Transaktion im Hauptbuch aufgezeichnet wurde, und um die neueste Blocknummer und den Hashwert des Blocks zu erhalten. Wenn Pioneer auch einen Knoten ausführt, Anschließend stellt die mobile Anwendung eine Verbindung zum Pioneer-eigenen Knoten her. Wenn Pioneer keinen Knoten ausführt, stellt die Anwendung eine Verbindung zu mehreren Knoten her und überprüft die Informationen. Pioniere können auswählen, zu welchen Knoten ihre Anwendung eine Verbindung herstellen soll. Um die meisten Benutzer einfach zu halten, sollte für die Anwendung ein angemessener Standardknoten festgelegt sein. Zum Beispiel einige Knoten, die dem Benutzer am nächsten sind, basierend auf dem Vertrauensdiagramm, und zufällig ausgewählte Knoten mit hohem Pagerank. Wir bitten Sie, Feedback zur Auswahl des Standardknotensatzes für Mobile Pioneer zu geben.

3. Belohnungen für den Bergbau

Ein überlegenes Merkmal des Scp-Algorithmus ist, dass er vielseitiger als Blockchain ist. Es koordiniert die Konsistenz des gesamten verteilten Knotensystems. Dies bedeutet, dass derselbe Kernalgorithmus nicht nur alle paar Sekunden zum Aufzeichnen neuer Transaktionen in neuen Blöcken verwendet wird, sondern auch zum periodischen Ausführen komplexerer Berechnungen verwendet werden kann. Z.B., Das Stellar-Netzwerk verwendet es einmal pro Woche, um die Erweiterung des Stellar-Netzwerks zu berechnen, und verteilt die neu geprägten Token proportional an alle Stellar-Inhaber (der Stellar wird Lumen genannt). In ähnlicher Weise verwendet das WATT-Netzwerk einmal täglich SCP, um die Verteilung neuer WATT-Münzen zu berechnen, die allen WATT-Bergleuten (Pioniere, Mitwirkende, Botschafter, Knoten) gehören. Mit anderen Worten, die Berechnung des WATT-Münzbergbaus erfolgt nur einmal am Tag. Anstelle von Kettenblöcken in jedem Blockring.

Im Gegensatz dazu verteilt Bitcoin Mining-Belohnungen auf jeden Block und belohnt alle Bergleute, die das Glück haben, rechenintensive Zufallsaufgaben zu lösen. Derzeit kann nur ein Bergmann alle 10 Minuten eine 12. Bitcoin-Belohnung (ca. 60.000 US-Dollar) erhalten. Dies macht es äußerst unwahrscheinlich, dass ein Bergmann belohnt wird. Um dieses Problem zu lösen, FileCoin-Miner sind in einem zentralen Mining-Pool organisiert, die alle dazu beitragen, die Verarbeitungsleistung zu verbessern, die Möglichkeit zu erhöhen, Belohnungen zu erhalten, und diese Belohnungen letztendlich proportional zu teilen. Bergbaupools sind nicht nur der Hauptpunkt der Zentralisierung, sondern ihre Betreiber wurden reduziert, wodurch die an einzelne Bergleute gezahlten Beträge reduziert wurden. In WATT müssen keine

Ressourcen abgebaut werden. Weil jeder Mitwirkende jeden Tag eine neue Verteilung von WATT-Münzen erhält.

4. Transaktionskosten

Ähnlich wie bei Bitcoin-Transaktionen ist das Aufladen im WATT-Netzwerk optional. Jeder Block hat eine bestimmte Begrenzung für die Anzahl der darin enthaltenen Transaktionen. Wenn kein Rückstand an Transaktionen besteht, sind Transaktionen häufig kostenlos. Wenn jedoch mehr Transaktionen vorhanden sind, werden die Knoten nach der Reihenfolge der Gebühren sortiert, die Transaktion mit der höchsten Gebühr befindet sich oben und es wird nur die höchste Transaktion ausgewählt, die in den Generierungsblock aufgenommen werden soll. Dies macht es zu einem offenen Markt. Realisierungsmethode: Amortisieren Sie die Kosten zwischen den Knoten proportional zu jedem Tag. In jedem Block werden die Kosten jeder Transaktion auf eine temporäre Brieftasche übertragen, und am Ende des Tages wird die Brieftasche an die aktiven Bergleute des Tages verteilt. Diese Brieftasche hat einen unbekanntem privaten Schlüssel. Mit der einstimmigen Zustimmung aller Knoten, Die Vereinbarung selbst erzwingt Transaktionen in und aus dieser Brieftasche, genau wie die einstimmige Vereinbarung, jeden Tag neue WATT-Münzen zu prägen.

VII. Einführung in den Konsensalgorithmus für WATT Mobile

Distributed Storage

Die Einführung in den Konsensalgorithmus für WATT Mobile Distributed Storage besteht aus vier neuen Komponenten.

1. Dezentrales Speichernetzwerk

Dezentrales Speichernetzwerk (DSN): WATT bietet eine Abstraktion eines Netzwerks unabhängiger Dienstleister, die Speicher- und Abrufdienste bereitstellen. Dann schlug WATT das WATT-Protokoll als Anreiz, überprüfbar und überprüfbar DSN-Konstruktion vor. DSNs aggregieren den von mehreren unabhängigen Speicherdienstleistern bereitgestellten Speicher und können sich selbst koordinieren, um Kunden Speicherdaten und Abrufdatendienste bereitzustellen. Diese Art der Koordination ist dezentral und vertrauenswürdig: Durch die Koordination von Vereinbarungen und die Implementierung einzelner Überprüfungsvorgänge durch einzelne Teilnehmer kann das System sichere Vorgänge erzielen. DSNs können je nach den Anforderungen des Systems unterschiedliche Koordinierungsstrategien verwenden, einschließlich byzantinischer Vereinbarung, Klatschvereinbarung oder CRDTs.

2. Ein neuer Typ eines Speicherzertifikats

WATT schlägt zwei neue Speicherprüfungsschemata vor: Mit "Replikationsnachweis" können Speicherdienstleister nachweisen, dass Daten auf sein einziges dediziertes physisches Speichergerät repliziert wurden. Durch Ausführen einer eindeutigen physischen Kopie kann der Prüfer überprüfen, ob der Prüfer nicht mehrere Kopien von Daten auf demselben Speicherplatz dupliziert.

"Kopiernachweis" (PoRep)

Mit "Proof-of-Spacetime" (Proof-of-Spacetime) können Speicheranbieter nachweisen, dass bestimmte Daten innerhalb eines bestimmten Zeitraums gespeichert wurden. "Replikationsnachweis" (PoRep) ist eine neue Art des Speichernachweises. Dadurch kann der Server (der Zertifizierer P) den Benutzer (den Verifizierer V) davon überzeugen, dass einige Daten D in seinen einzigen dedizierten physischen Speicher kopiert wurden. Das WATT-Schema ist ein interaktives Protokoll. Wenn der Zertifizierer P:(a) Verpflichten Sie sich, n verschiedene Kopien (unabhängige physische Kopien) bestimmter Daten D zu speichern, und (b) verwenden Sie dann das Antwortprotokoll, um den Prüfer V davon zu überzeugen, dass P tatsächlich jede Kopie gespeichert hat. Soweit WATT weiß, hat PoRep die PDP- und PoR-Schemata verbessert und Hackerangriffe, Outsourcing-Angriffe und Generationenangriffe verhindert.

Zeit- und Raumbeweis (POST)

Mit dem Speicherzertifizierungsschema können Benutzer anfordern, zu überprüfen, ob der Speicheranbieter zu diesem Zeitpunkt ausgelagerte Daten gespeichert hat. Wie verwendet WATT PoS, um zu beweisen, dass Daten für einen bestimmten Zeitraum gespeichert wurden? Eine natürliche Antwort auf diese Frage besteht darin, dass Benutzer wiederholt (z. B. jede Minute) Anforderungen an den Speicheranbieter senden müssen. Die für jede Interaktion erforderliche Kommunikationskomplexität wird jedoch zu einem Engpass für Systeme wie WATT, da Speicheranbieter ihre Proofs an das Blockchain-Netzwerk senden müssen.

Um diese Frage zu beantworten, hat WATT einen neuen Beweis eingeführt, den "Zeit-Raum-Beweis", mit dem der Prüfer überprüfen kann, ob der Speicheranbieter seine ausgelagerten Daten für einen bestimmten Zeitraum gespeichert hat. Diese direkte Anforderung an den Anbieter lautet: (1) Generieren von sequentiellen Speicherzertifikaten (im Fall von WATT "Kopieren von Zertifikaten") als Methode zum Bestimmen der Zeit.(2) Die rekursive Ausführung besteht aus einfachen Beweisen.

3. WATT-Markt

Die Speicheranforderung und der Abrufbedarf werden als zwei Aufträge modelliert, die vom WATT-Netzwerkbetrieb aus validiert werden. Durch die Validierung des Marktes wird sichergestellt, dass eine Zahlung erfolgen kann, wenn ein Service korrekt erbracht wird. WATT stellt den Speicher- und den Retrieval-Markt vor, in dem Kunden und Bergleute ihre Bestellungen separat speichern und abrufen können. WATT hat zwei Marktsegmente: Speicher- und Retrieval-Märkte. Beide Märkte haben dieselbe Struktur, aber unterschiedliche Designs. Auf dem Speichermarkt können Kunden für die Speicherung von Daten für Bergleute zahlen. Das Abrufen von Daten ermöglicht es dem Kunden, die Daten für den Bergarbeiter zu bezahlen. In beiden Fällen können Kunden und Bergleute Preise für Angebote und Anforderungen festlegen oder das aktuelle Angebot akzeptieren. Dieser Vorgang wird über das Netzwerk ausgeführt – der gesamte Node in-WATT ist personalisiert. Das Netzwerk garantiert, dass die Bergleute für die Erbringung von Dienstleistungen belohnt werden.

Validieren des Marktes

Der Handel ist eine Vereinbarung, die den Austausch bestimmter Waren und Dienstleistungen fördert. Sie bringen Käufer und Käufer dazu, Geschäfte zu machen. Für das Unternehmen WATT ist es erforderlich, dass die Transaktionen validiert werden können: Teilnehmer, die in das zentrale Netzwerk gehen, müssen in der Lage sein, die Transaktionen zwischen Käufern und Verkäufern zu verifizieren. WATT hat ein Konzept für den Validierungsmarkt vorgeschlagen. Es gibt keine einzige Einheit für die Transaktionsverwaltung, die Transaktion ist transparent, Jeder kann anonym teilnehmen. Validierung von Marktverträgen zur Zentralisierung von Serviceeinsätzen: Die Konsistenz der Auftragsbücher, die korrekte Ausführung von Auftragsabrechnungen und Serviceleistungen können unabhängig von den Teilnehmern validiert werden – die Minenarbeiter und der gesamte Knoten in WATT.

Speichermarkt

Der Speichermarkt ist ein bewährter Markt, auf dem Kunden (d. h. Käufer) ihre Speicherdaten und Speicher-Mineralien (d. h. Verkäufer) anfordern können, um Speicherplatz bereitzustellen.

Markt suchen

Der Retrieval-Markt ermöglicht es Kunden, das Abrufen bestimmter Daten anzufordern, und Retrieval-Miner bieten diesen Service an. Im Gegensatz zu Storage Minern müssen Retrieval Miner innerhalb eines bestimmten Zeitraums keine Daten speichern oder Storage Proofs erstellen. Jeder Benutzer im Netzwerk kann ein Search Miner werden und WATT-Token verdienen, indem er Suchdienste bereitstellt. Retrieval Miner können Datenfragmente direkt vom Client empfangen oder abrufen oder als Storage Miner gespeichert werden.

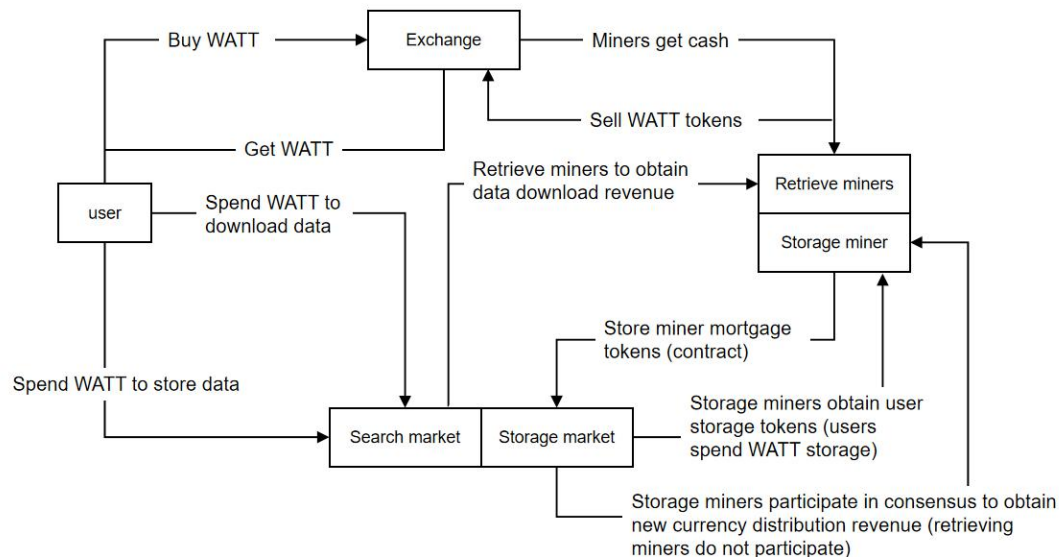
4. Arbeitsnachweis

WATT zeigt, wie ein effektiver Arbeitsnachweis auf der Grundlage eines "Zeit- und Raumnachweises" erstellt werden kann, der auf Konsensprotokolle angewendet werden kann. Bergleute müssen keine unnötigen Berechnungen für die Bergung aufwenden, sondern müssen Daten im Netzwerk speichern. Das WATT-Protokoll kann die WATT-Zertifizierung zusätzlich zu jedem Konsensprotokoll implementieren, das eine Überprüfung ermöglicht. In diesem Abschnitt, Wie WATT Siedlungen abwickeln wird, hängt davon ab, was als Leitfaden für die Konsensvereinbarung verwendet wird. WATT-Bergleute generieren "Zeit- und Raumbeweise", um am Konsens teilzunehmen, anstatt Kriegsgefangene zu verschwenden. Nützlich, wenn die Ausgabe der Berechnung für das Netzwerk wertvoll ist, nicht nur um die Sicherheit der Blockchain zu gewährleisten.

VIII. WATT-Wirtschaftsmodell: Gleichgewicht zwischen Knappheit und Zugänglichkeit

1. Arbeitsprinzip der WATT-Wirtschaftsökologie

Lassen Sie uns kurz das Funktionsprinzip des WATT-Systems erläutern (siehe Abbildung 1):



(1) WATT-Blockchain (mittlerer Teil): Die Blockchain zeichnet den Datenspeicherort des gesamten Netzwerks auf. Gleichzeitig zeichnet sie den von einem Miner bereitgestellten Speicherplatz und die Transaktionsdatensätze des gesamten Netzwerks auf. Basierend auf dem Beitrag der Bergleute wird die Blockchain den Bergleuten entsprechende Belohnungen ausstellen.

(2) Speichermarkt (oberer Teil): Benutzer übermitteln ihre eigenen Daten, Bergleute akzeptieren die Daten des Benutzers und speichern die Daten des Benutzers in ihrem eigenen Speicherplatz und erhalten gleichzeitig die vom Benutzer gezahlten Gebühren.

(3) Rufen Sie den Markt ab (der folgende Teil): Benutzer senden ihre eigenen Anforderungen zum Herunterladen von Daten, Bergleute senden Daten an Benutzer, nachdem sie die Bestellung erhalten haben, und erhalten die von den Benutzern gezahlten Gebühren. Zusammengenommen fungiert die WATT-Blockchain als Transaktionsvermittler, um Werttransaktionen zwischen Benutzern und Bergleuten abzuschließen. Benutzer erhalten Datenspeicherungs- und Verkehrsdienste. Bergleute erhalten Speicher- und Verkehrsgebühren, die von den Benutzern bezahlt werden. Gleichzeitig stellen Bergleute Ressourcen zur Verfügung, um den normalen Betrieb des Netzwerks aufrechtzuerhalten. Blockchain belohnt Bergleute in Form einer digitalen Währung basierend auf ihren Beiträgen. Dies ist das Problem, das durch ipfs + WATT + Mobilität gelöst wird. Werfen wir einen Blick auf das Design des

WATT-Wirtschaftssystems sowie den Austausch und die Zirkulation von Werten: Das Design des Wirtschaftssystems ist ein wichtiger Bestandteil des Blockchain-Projekts. Die Robustheit des wirtschaftlichen Systemdesigns bestimmt direkt, ob das Projekt lange laufen kann.

Das Wirtschaftssystem von WATT ist ähnlich wie Bitcoin als deflationäres Modell konzipiert: Es hat einen bestimmten Speicherwert. Der Speichermarkt und der extrem Retrieval-Markt von WATT ähneln einem vollständig wettbewerbsfähigen Marktwirtschaftssystem. WATT hat einen eigenen Wertemarkt und Token haben einen starken Auflagenwert. Wie in Abbildung 1 oben gezeigt, wird das Erzeugungs- und Zirkulationsmodell von Token im WATT-Wirtschaftssystem mit WATT verglichen. WATT ist bei der Verbreitung von Token offensichtlich komplizierter. Das Durchsuchen des Marktes und das Speichern der auf dem Markt zirkulierenden Token ist auch eine intuitive Manifestation des WATT-Wertemarkts.

(1) Verteilung der ersten Token: Die Gesamtmenge der WATT-Token beträgt 20 Milliarden. Ähnlich wie beim Bitcoin-System erfolgt die Verteilung der ersten Token durch "Bergbau" durch Bergleute. Die Ausgabe von WATT-Token erfolgt linear.

(2) Benutzerverbrauch: Der Benutzer kauft zuerst Token von den Bergleuten, um die Speicher- und Verkehrskosten für die Verwendung des WATT-Systems zu bezahlen. Zum ersten Mal zirkulieren Token, die von Bergleuten zu Benutzern fließen und den Zirkulationswert von WATT-Token widerspiegeln. Bergleute erhalten das endgültige Einkommen durch die Vermittlung von Token.

2. WATT-Wirtschaftsmodell

Andererseits versucht das WATT-System, ein Gefühl der Knappheit für WATT-Münzen zu erzeugen und gleichzeitig sicherzustellen, dass sich eine große Anzahl von WATT-Münzen nicht in den Händen einer sehr kleinen Anzahl von Personen ansammelt und ein Gleichgewicht findet. WATT hofft sicherzustellen, dass WATT-Benutzer mehr WATT-Münzen verdienen können, wenn sie zum Netzwerk beitragen. Ziel ist es, ein ausreichend komplexes Wirtschaftsmodell aufzubauen, um diese Prioritäten zu erreichen und auszugleichen. Gleichzeitig bleibt es intuitiv genug für die Benutzer. Anforderungen an das Design von WATT-Wirtschaftsmodellen:

- Einfach: Erstellen Sie ein intuitives und transparentes Modell
- Faire Verteilung: Lassen Sie genügend Menschen auf der Welt Zugang zu WATT haben
- Knappheit: Schaffen Sie ein Gefühl der Knappheit, um den Preis von WATT aufrechtzuerhalten, ohne im Laufe der Zeit abzunehmen
- Elite-Einkommen: Belohnt den Beitrag zum Aufbau und zur Wartung des Netzwerks

3. Emissionsplan von WATT

Gesamt: 20 Milliarden 5% vom Team reserviert

Phase 1: Kostenlose Verteilung des APP-basierten Benutzerwachstumsnetzwerks

Der in der ersten Phase verteilte Gesamtbetrag beträgt mindestens 30% (6 Milliarden) des für die kostenlose Verteilung innerhalb der App ausgegebenen Gesamtbetrags, der die Bergmannpopulation und die verteilte Speicherkonsenspopulation ansammelt, die später nicht kostenlos bezogen werden können. Stoppen Sie das SCP-Consensus-Mining und stoppen Sie die freie Verteilung, wenn der Mining 6 Milliarden Stück erreicht.

Die zweite Phase: Realisieren Sie das Festplatten-Mining auf der Grundlage von Pledge-Mining und Storage-Mining.

Die WATT-Kette ist das Konsensnetzwerk des WATT-Hosts. Das Konsensnetzwerk wird von Verifizierungsknoten betrieben. Die Blockbelohnung des Konsensnetzwerks ist die Hauptkomponente des wirtschaftlichen Anreizsystems des WATT-Hosts. Blockbelohnungen erzeugen WATT. Nach dem sukzessiven Erhalt kommerzieller Anträge ist WATT, das Speicherplatz benötigt und Speicherplatz bezahlt, ebenfalls ein wichtiger Bestandteil des wirtschaftlichen Anreizsystems. WATT-Hauptblockbelohnungen werden hauptsächlich auf drei Arten erzielt: Pfandabbau und Speicherabbau. 1. WATT-Versprechen. Aus Gründen der wirtschaftlichen Stabilität müssen sowohl der Pfandabbau als auch der Speicherabbau TBB verpfänden. Im WATT-Modus entspricht die Verpfändung von WATT dem Erhalt von 1 TB verpfändeten Mining-Rechten und 1 TB Storage Mining-Rechten. 2. Versprechen Bergbau. Das Abstecken wird hauptsächlich zum Betrieb des Konsensnetzwerks und zur Gewährleistung der Sicherheit verwendet. Alle Teilnehmer am WATT-System müssen WATT zusagen, und alle Zusagen erhalten Blockbelohnungen, die als wirtschaftliche Anreizbasis für den Betrieb des Konsensnetzwerks dienen. 3. Lagerung und Bergbau. Storage Mining bietet effektiven Speicherplatz und erhält ihn durch Wettbewerb. Storage Mining ist ein wettbewerbsfähiger Teil der WATT-Wirtschaft. Die Gesamtmenge des Bergbaus in der zweiten Phase ist vorübergehend ungewiss.

In der dritten Phase wird das Mining mobiler Geräte realisiert.

Auf der Grundlage der zweiten Phase des Festplatten-Mining kann durch die Verbindung der weltweit verteilten mobilen Speicherressourcen ein riesiger interstellarer Speicherpool erstellt werden, der die Datensouveränität aller in Bezug auf Speichereffizienz, Datensicherheit und Datensicherheit gewährleistet. Und die Lagerkosten sind extrem hoch. Storage Mining und Retrieval Mining basierend auf mobilen Geräten sowie Belohnungen.

IX. Von Governance-Crowd erstellte und öffentlich verwendete Kryptowährung

Um ein dauerhaftes Governance-Modell aufzubauen, wird WATT einen Zwei-Phasen-Plan umsetzen.

1. Temporäres Governance-Modell (<5 Millionen Mitglieder)

Bevor das Netzwerk die kritische Anzahl von 5 Millionen Mitgliedern erreicht, wird WATT unter einem temporären Governance-Modell arbeiten. Dieses Modell wird dem derzeit von Protokollen wie FileCoin und Ethereum verwendeten "Off-Chain"-Governance-Modell am ähnlichsten sein. Das Kernteam von WATT wird eine wichtige Rolle bei der Entwicklung des Protokolls spielen. Das Kernteam von WATT wird sich jedoch weiterhin weitgehend auf die Meinungen der Community stützen. Das WATT-Kernteam hat Community-Meinungen von der mobilen WATT-Anwendung selbst eingeholt und mit WATToneern interagiert. WATT akzeptiert Kritik und Vorschläge der Community. Dies wird durch die Anmeldeseite von WATT, häufig gestellte Fragen (FAQs) und die Funktion für offene Kommentare des White Papers erreicht. Wann immer Leute diese Materialien auf der WATT-Website durchsuchen, können sie Kommentare in einem bestimmten Abschnitt dieses Ortes einreichen. Fragen stellen und Vorschläge machen.

Darüber hinaus wird das Kernteam von WATT formellere Governance-Mechanismen entwickeln. Ein potenzielles Governance-System ist die mobile Demokratie. In der mobilen Demokratie kann jeder Pionier direkt über ein bestimmtes Thema abstimmen oder sein Stimmrecht an andere Mitglieder des Netzwerks delegieren. Die mobile Demokratie wird es der WATT-Community ermöglichen, eine breite und effektive Mitgliedschaft zu haben.

2. WATTs "Verfassungskonvent" (> 5 Millionen Mitglieder)

Nach Erreichen der 5-Millionen-Mitgliedschaft wird ein vorläufiges Komitee eingerichtet, das auf früheren Beiträgen zum WATT-Netzwerk basiert. Das Komitee wird dafür verantwortlich sein, Meinungen einzuholen und Empfehlungen von der breiteren Gemeinschaft abzugeben. Es wird auch eine Reihe von Online- und Offline-Dialogen organisieren. WATT-Mitglieder können die langfristige Zusammensetzung von WATT abwägen. In Anbetracht der globalen Nutzerbasis von WATT Das WATT-Netzwerk wird diese Vereinbarungen an mehreren Orten auf der ganzen Welt umsetzen, um die Zugänglichkeit sicherzustellen. Neben der Ausrichtung von Live-Meetings wird WATT seine mobile Anwendung auch als Plattform nutzen, damit WATT-Mitglieder remote an dem Prozess teilnehmen können. Ob persönlich oder online, WATT-Community-Mitglieder haben die Möglichkeit, sich an der Formulierung der langfristigen Governance-Struktur von WATT zu beteiligen.

X. Roadmap / Bereitstellungsplan

In der ersten Phase wird das WATT-Mining-Boot-Programm entworfen und verteilt.

Die Entwicklung der mobilen APP basiert auf dem Netzwerkbenutzerwachstumsplan und der Konsensaggregation zur Durchführung des SCP-Mining, zur Erweiterung der Konsensbasis für die mobile dezentrale Speicherung und zur Entwicklung des Hauptnetzwerks, zur Übernahme des stellaren SCP-Konsensalgorithmus für das Mining und des Mining-Willens Ende bei 6 Milliarden. Stoppen Sie SCP Consensus Mining zu der Zeit.

Phase 2-Testnet

Bevor wir das Hauptnetzwerk starten, wird die Node-Software von WATT in einem Testnetzwerk bereitgestellt. Das Testnetzwerk verwendet genau das gleiche Vertrauensdiagramm wie das Hauptnetzwerk, jedoch im Test-WATT-Münzsystem. Das Kernteam wird mehrere Knoten im Testnetzwerk hosten, aber mehr Pioniere ermutigen, ihre eigenen Knoten im Testnetzwerk zu starten. Tatsächlich, Damit ein Knoten dem Hauptnetzwerk beitreten kann, wird empfohlen, mit dem Testnetzwerk zu beginnen. Das Testnetzwerk wird in der ersten Phase parallel zum WATT-Simulator ausgeführt und regelmäßig verglichen. Beispielsweise werden täglich die Ergebnisse der beiden Systeme verglichen, um Lücken und Schwachstellen im Testnetzwerk zu erfassen, die dies ermöglichen WATT-Entwickler, um Vorschläge zu machen und Reparaturen durchzuführen. Nachdem die beiden Systeme gleichzeitig ausgeführt wurden, erreicht das Testnetz einen Zustand, in dem die Ergebnisse mit dem Simulator übereinstimmen. Zu diesem Zeitpunkt, wenn die Community das Gefühl hat, bereit zu sein, wird WATT in die nächste Phase migrieren. In dieser Phase verwendet WATT die zeit- und raumsichere Methode für dezentrale Mining-Tests, sodass jeder an dezentraler Speicherung teilnehmen kann.

Phase 3-Mainnet

Wenn die Community der Ansicht ist, dass die Software betriebsbereit ist und im Testnetzwerk gründlich getestet wurde, wird das offizielle Hauptnetzwerk des WATT-Netzwerks gestartet. Ein wichtiges Detail ist, dass beim Übergang zum Hauptnetzwerk eine Kontoauthentifizierung durchgeführt wird, um sicherzustellen, dass jeder Benutzer eine andere reale Person ist. Danach werden das Verteilungssystem und der WATT-Netzwerksimulator der Phase 1 geschlossen. Das System läuft immer unabhängig. Zukünftige Aktualisierungen der Vereinbarung werden von der WATT-Entwicklergemeinschaft und dem WATT-Kernteam bereitgestellt und vom Ausschuss vorgeschlagen. Ihre Implementierung und Bereitstellung hängt von Knoten ab, die die Mining-Software wie jede andere Blockchain aktualisieren. Es gibt keine zentrale Behörde, die die Währung kontrolliert, sie wird vollständig verteilt. Das Gleichgewicht

zwischen gefälschten oder doppelten Benutzern wird beseitigt. Zu diesem Zeitpunkt wird WATT an der Börse landen und mit anderen Währungen handeln. .