Freeman Familie

4. Juli 2019

EPIC CASH

EPIC PRIVATES INTERNET GELD

Ein elektronisches Peer-to-Peer Zahlungssystem

WERTSPEICHER + TAUSCHMITTEL + RECHNUNGSEINHEIT

1,7 Milliarden Erwachsene haben keinen Zugang zum globalen Finanzsystem, während weitere 1,3 Milliarden Menschen unterversorgt sind. Epic Cash setzt menschliches Potenzial frei, indem es Individuen mit dem globalen Markt verbindet. Schnell, nahezu frei nutzbar und offen für alle.

Version 7.1b

Inhalt

I. Abstrakt

Epic Cash ist das Endprodukt auf dem Weg zum echten P2P-Internet-Cash, dem Eckpfeiler eines privaten Finanzsystems. Die Epic-Währung soll die weltweit effektivste Form von digitalem Geld mit Schutz der Privatsphäre werden. Um dieses Ziel zu erreichen, erfüllt es die drei Hauptfunktionen des Geldes:

1. **Wertspeicher** – kann gespeichert, abgerufen und jederzeit getauscht werden und ist zum Zeitpunkt des Erhalts von berechenbarem Wert;
2. **Tauschmittel** – alles was als ein Wertstandard akzeptiert und gegen Waren oder Dienstleistungen austauschbar ist;
3. **Rechnungseinheit** – die Einheit mit der der Wert einer Sache erfasst und verglichen wird.

	$ USD	BTC	EPIC
Wertspeicher	✗	✓	✓
Tauschmittel	✓	✗	✓
Rechnungseinheit	✓	✗	✓

Im Jahr 2009 tauchte Bitcoin als erste Blockchain-basierte digitale Währung auf und mit ihr drei definierende Merkmale, gegen die andere Kryptowährungen bewertet werden:

- ✓ **Vertrauenslosigkeit** – niemand ist verpflichtet einer zentralisierten Einheit oder Gegenpartei zu vertrauen, um die Funktion des Netzwerks zu gewährleisten;
- ✓ **Unveränderlichkeit** – Transaktionen können nicht rückgängig gemacht werden;
  a. Es sollte unwahrscheinlich oder schwierig sein, die Geschichte neu zu schreiben;
  b. Es sollte unmöglich sein, dass jemand außer dem Besitzer eines private key Gelder bewegt, die mit diesem private key verbunden sind
  c. Alle Transaktionen werden in der Blockchain aufgezeichnet.
- ✓ **Dezentralisierung** – "Blockchains sind politisch dezentralisiert (niemand kontrolliert sie) und architektonisch dezentralisiert (keine infrastrukturelle Problem-stelle).... "[1].

Bitcoin beschritt technologisch neue Wege und hielt sich bei der Struktur seiner Geldpolitik an bewährte Grundlagen. Bitcoins Erfolg hängt stark von seinem begrenzten Angebot ab, kombiniert mit einer vertrauenswürdigen, unveränderlichen und dezentralen Blockchain. Epic Cash emuliert Bitcoins Geldpolitik der sinkenden Inflation und des begrenzten Angebots und stellt damit sicher, dass die Epic-Währung als effektiver Wertspeicher dienen kann.

Trotz des Erfolgs von Bitcoin wurden seit seiner Gründung vor 10 Jahren einige Mängel aufgedeckt. Andere Projekte haben versucht diese Mängel zu überwinden und wir haben die besten von ihnen untersucht, die wir als Ausgangspunkt nehmen können. Wir haben uns für die Grin-Codebasis und die ausgezeichnete Arbeit mehrerer anderer Projekte entschieden, um die hart erkämpften Leistungen zu perfektionieren und Fehler der Epic Cash-Vorgänger zu entdecken. Epic Cash verfügt über die Schlüsselqualitäten, um eine ideale Währung zu sein:

- ✓ **Fungibilität** – Der Wert einer bestimmten Einheit von Epic muss immer gleich einer anderen Einheit von Epic sein, so wie ein Yen oder Yuan immer gleich und durch einen anderen Yen oder Yuan ersetzbar ist. Die Erreichung der Fungibilität hängt zu einem großen Teil von der Privatsphäre ab.
- ✓ **Privatsphäre** – Die Epic Cash Blockchain schützt die Anonymität von Epic-Inhabern und -Nutzern, indem sie die Details von Transaktionen vor Dritten schützt in dem sie nicht zurückverfolgbar und für die Überwachung unsichtbar konzipiert ist.
- ✓ **Skalierbarkeit** – Epic Cash verfügt über eine platzsparende Blockchain, auf der neue Knoten cohne ressourcenintensive Ausrüstung einfach eingerichtet werden können. Die Epic Cash Blockchain ist in der Lage, mindestens den doppelten Durchsatz von Bitcoin zu erreichen.
- ✓ **Geschwindigkeit** – Die Epic Cash Transaktionen sind reibungslos, kontinuierlich und werden viel schneller ausgeführt als in früheren Generationen der Blockchain-Technologie. Während Bitcoin sechs 10-Minuten-Blöcke benötigt, um eine vollständige Transaktionsbestätigung zu erhalten, erfolgen Epic-Transaktionen innerhalb einer einzigen Blockbestätigung, sobald ein 1-Minuten-Block gemined wurde.

[1] Buterin, Vitalik, *The Meaning of Decentralization*, 6 February, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. Privatsphäre

Der zeitgemäße Umgang mit Geld kann als kollektive Übertragung von Rechnungseinheiten zwischen Menschen und Institutionen verstanden werden. Die Landschaft des Geldes zu einem bestimmten Zeitpunkt kann durch Beantwortung der folgenden Fragen abgebildet werden:

1. Wer hat es und wie viel haben sie?

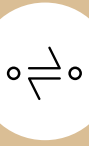
2. Wer handelt mit wem und für wie viel?

Für traditionelle Fiat-Währungen und auch für Bitcoin können wir diese Fragen beantworten. Auf diese Weise kann viel über das Leben der Menschen preisgegeben werden, wie z.B. Konsumverhalten, Eigentum und Transaktionspartner. Durch die Verfolgung von Werttransfers können recht genaue Rückschlüsse auf die Interessen und Absichten eines Einzelnen gezogen werden. Ohne Privatsphäre können Transaktionsdaten gefährliche Informationen in den Händen von räuberischen Dritten sein.

Die Verwendung von Kryptowährungen in den letzten zehn Jahren zeigt ein kontinuierliches Maß an " Privatsphäre " in verschiedenen Blockchain Implementierungen. Die Skala der Privatsphäre, wenn man sie betrachtet, reicht von offen und bekannt auf der einen Seite bis hin zu anonym auf der anderen Seite. Da die Privatsphäre schwindet, wird ein wesentlicher Eckpfeiler von Kryptowährungen, Vertrauenslosigkeit, verschlechtert. Wie der Erfolg der Bitcoin Blockchain-Analyse zeigt, ist Bitcoin eher auf das berüchtigte transparente Ende des Datenschutzspektrums ausgerichtet. Benutzer müssen zunehmend Maßnahmen ergreifen um sicherzustellen, dass sie nicht versehentlich mit beschmutztem Bitcoin handeln. Die Epic Cash-Lösung schwenkt die Nadel in Richtung Anonymität und stellt diese wesentliche Eigenschaft wieder her, indem sie sicherstellt, dass sowohl die Privatsphäre des Einzelnen als auch die Privatsphäre von Transaktionen auf einer grundlegenden Ebene in das System integriert werden.

Privatsphäre der Identität

Privatsphäre der Transaktion



Privatsphäre der Identität

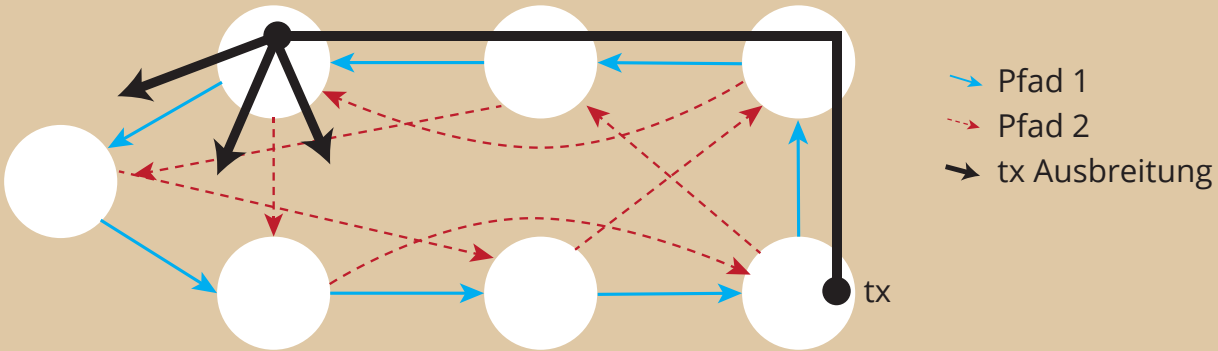
Die meisten Kryptowährungen wie Bitcoin werden in Wallets gespeichert, deren Adressen sich auf öffentliche Schlüssel beziehen, die von den privaten Schlüsseln eines Wallets abgeleitet werden. Diese Adressen können als Ortung des privaten Tresors in der digitalen Welt angesehen werden. Die Epic Cash Blockchain eliminiert Adressen vollständig und verwendet stattdessen eine große Multisignatur, aus der alle öffentlichen und privaten Schlüssel als Einmalschlüssel generiert werden

Da die Wallet-Adressen von Bitcoin der Tresor in der digitalen Welt sind, kann dieses Wallet auf die Internet Protocol (IP)-Adresse eines Besitzers zurückgeführt werden, die den Eigentümer an einem Computer an einem eindeutigen Ort zu einem bestimmten Zeitpunkt verankert. Einfach erklärt: Wenn eine Bitcoin-Transaktion stattfindet, wird die Transaktion von einem Kommunikationszentrum namens "Knoten" übertragen und dann an andere Knoten namens "Peers" weitergeleitet. Diese Informationen werden dann schnell an die Peers der einzelnen Knoten im gesamten Netzwerk weitergegeben. Dieser Prozess wird zu Recht als "Gossip Protocol" bezeichnet. Einfach ausgedrückt, hat jeder Bitcoin eine sichtbare Online-Position und einen physischen Standort, an dem er bzw. der Bitcoin-Besitzer gefunden werden kann. Wie die Journalistin Grace Caffyn feststellte, ist Bitcoin "nicht geheimer als eine Google-Suche über eine Internetverbindung zu Hause". [2]

Zusätzlich zur Eliminierung von Wallet-Adressen schützt die Epic Cash Blockchain die Privatsphäre der Identität, indem sichergestellt wird, dass IP-Adressen nicht verfolgt werden können. Dies geschieht durch die Integration des Dandelion++ Protokolls. Das Dandelion++ Protokoll, das sich an seinem Vorgänger, dem ursprünglichen Dandelion Protokoll anlehnt, ist das Ergebnis der kontinuierlichen Arbeit von sieben Forschern zur Bekämpfung von Deanonymisierungsangriffen auf der Blockchain. Durch Dandelion++ werden Transaktionen über zufällig verschachtelte Pfade oder "Kabel" geleitet und dann plötzlich an ein großes Netzwerk von Knoten verteilt, wie die Hülsen einer Löwenzahnblume, wenn sie von ihrem Stamm geblasen werden (Abbildung 1). Dies macht es nahezu unmöglich auf die Herkunft von Transaktionen und damit auf die von ihnen stammenden IP-Adressen zu schließen.

Abbildung 1: Anonymisierung von Transaktionen mit dem Dandelion++ Protokoll.

Dandelion++ leitet Nachrichten über einen von zwei ineinander verschachtelten Pfaden in einem 4-Norm-Graphen weiter und sendet dann mittels Diffusion. In der Abbildung propagiert sich die Transaktion über den blauen, festen Pfad[3]. Dieser Prozess macht es äußerst schwierig, Transaktionen bis zur Quelle zurückzuverfolgen und schützt somit die Privatsphäre.



[2] F2Caffyn, Grace, ***Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,*** 14 March, 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees', ***Proc. ACM Meas. Anal. Comput. Sys.***, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

Privatsphäre der Transaktion

Die Epic Cash Blockchain garantiert die Vertraulichkeit von Transaktionen, indem sie die Beträge und die Sender-Empfänger-Beziehung einer Transaktion verdeckt. Dies wird durch die Anwendung bekannter Ideen aus der Anwendung von ***Confidential Transactions (CT)***[4] ***und CoinJoin***[5], erreicht, Methoden, die größtenteils von Gregory Maxwell (Bitcoin Core Entwickler, Mitbegründer und CTO von Blockstream) entwickelt wurden.

CT, ursprünglich von Adam Back entwickelt und später von Maxwell verfeinert, funktioniert durch die Zerlegung von Transaktionen in kleinere Teile durch Homomorphe Verschlüsselung, eine Methode zur Durchführung von Berechnungen an verschlüsselten Informationen, ohne diese zuerst zu entschlüsseln, um die Privatsphäre zu schützen. Sobald sie aufgeteilt sind, können die Teilnehmer die tatsächlichen Beträge der Transaktionen aufgrund von Blindungsfaktoren , nicht mehr sehen, ein System, das Zufallszahlen in die Mischung der Transaktionsfragmente wirft, um die Werte dieser Fragmente zu verbergen. Letztendlich kennen nur Transaktionspartner den Wert eines Tausches, während die Transaktion vom Netz durch eine Bestätigung verifiziert wird, die besagt, dass die Summe der Ausgabewerte gleich der Summe der Eingabewerte ist und die Summe der Ausgabeverblindungsfaktoren gleich der Summe der Eingabeverblindungsfaktoren.

Um die Problematik der neugierigen Blicke weiter zu erschweren, werden alle Epic Cash-Transaktionen mit CT getarnt und dann miteinander vermischt, um die Verbindungen zwischen den Transaktionspartnern zu verbergen. Dies geschieht durch Maxwells zweites Konzept, ***CoinJoin***.

Um ***CoinJoin*** einfach zu veranschaulichen, stellen Sie sich vor, dass A, B und C Epic an X, Y und Z senden. Durch das ***CoinJoin*** Medium gesendet ist nur bekannt, dass A, B und C senden und X, Y und Z empfangen, während die Transaktionsbeträge unsichtbar bleiben. Das ***CoinJoin***-System ist von grundlegender Bedeutung für die Entwicklung von Epic Cash durch One-Way Aggregate Signatures (OWAS), die alle Transaktionen innerhalb eines Blocks zu einer einzigen Transaktion kombinieren.

Privatsphäre: Zusammenfassung

Die Epic Cash Blockchain schützt die Privatsphäre von Personen und deren Transaktionen durch:

- **Eliminierung von Wallet-Adressen – Es gibt keine Standortkennungen für digitale Tresore innerhalb der Blockchain. Transaktionen werden direkt von Mensch zu Mensch auf einer Wallet zu Wallet Basis erstellt;**
- ***Dandelion++* Protokoll - verdeckt den digitalen Weg einer Transaktion zu der IP-Adresse des Transaktionssenders;**
- ***Vertrauliche Transaktionen* - teilen Sie Transaktionen in mehrere Stücke und führen Sie Blindungsfaktoren in die Sammlung dieser Stücke ein, so dass die Werte der Stücke und andere Transaktionsparameter unbekannt bleiben;**
- ***CoinJoin* – kombiniert Transaktionen zu Paketen, um die Beziehungen zwischen den Transaktionspartnern zu maskieren.**

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 August, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

III. Fungibilität

Charlie Lee, der Schöpfer von Litecoin, erklärte die Fungibilität sei das einzige Eigentum an gesundem Geld, das Bitcoin und Litecoin fehle und bekannte, dass Privatsphäre und Fungibilität die nächsten Schlachtfelder für diese Coins seien[6]. Andreas Antonopoulos, einer der weltweit führenden Blockchain-Experten, behauptete, dass "...verunreinigte Coins destruktiv sind. Wenn du Fungibilität und Privatsphäre brichst, brichst du die Währung."[7]

Fungibilität ist das Eigentum einer Reihe von Waren oder Vermögenswerten, die sicherstellen, dass die einzelnen Einheiten dieser Gruppe gleichwertig und austauschbar sind. Es unterscheidet die frühesten Formen der Währung von ihren vorhergehenden Systemen des Tauschhandels. Ohne das Vertrauen in die Fungibilität des Geldes verliert dieses Geld schnell seinen Nutzen. Wie im Folgenden dargestellt, ist die Fungibilität der meisten Kryptowährungen ungewiss, während die Datenschutzarchitektur von Epic Cash sicherstellt, dass sie für dieselben Bedrohungen nicht anfällig ist.

Die meisten Kryptowährungen, die Bitcoin ähnlich sind, können aufgrund der Art der transparenten Blockchain, auf denen sie existieren, nachweislich über jedes Wallet, in dem sie aufbewahrt wurden, verfolgt werden. Private Dritte und Regierungen überwachen die Bitcoin Blockchain mit immer ausgefeilteren Mitteln, um Coins, die in früheren Aktivitäten verwendet wurden, schnell zu identifizieren. Dies führt natürlich zu der Befürchtung, dass verunreinigte Münzen eines Tages von den Transaktionen ausgeschlossen werden könnten, so dass ihre späteren gutgläubigen Besitzer auf der Strecke bleiben.

Am 19. März 2018 gab das U.S. Office of Foreign Asset Control (OFAC) bekannt, die Aufnahme von Adressen in digitaler Währung in die Liste der Specially Designated Nationals (SDNs) in Betracht zu ziehen, d.h. Unternehmen, mit denen US-Personen oder -Unternehmen keine Geschäfte tätigen dürfen. Noch beunruhigender ist, dass die OFAC die Aufnahme von Adressen, die derzeit verunreinigte Münzen enthalten, in die SDN-Liste nicht ausgeschlossen hat, was dazu führen würde, dass unschuldige Besitzer von verunreinigten Kryptowährungen aufgrund der Zugehörigkeit der verunreinigten Münzen auf eine kriminelle schwarze Liste gesetzt würden. Dies hat dazu geführt, dass der Rechtsprofessor der New York Universität, Andrew Hinkes, witzelte, "Küssen Sie die Fungibilität zum Abschied", und dass die Öffentlichkeit "eine Prämie auf frisch geprägte oder auf saubere Coins erwarten sollte...."[8].

Vor dem Hintergrund dieser Entwicklungen ist es nicht schwer, sich eine Umwälzung des Krypto-Marktes und das Leid oder sogar das Aussterben vieler etablierter Krypto-Währungen vorzustellen. Epic ist jedoch eine der wenigen Kryptowährungen, die dieses Problem aufgrund der starken Datenschutzfunktionen, die zuvor in diesem Beitrag beschrieben wurden, vollständig vermeidet. Durch die Aufhebung der Verbindung zwischen Identität und Eigentum sowie der Beziehung zwischen den Transaktionspartnern kann Epic niemals einer Person oder einer Aktivität zugeordnet werden. Damit bleibt der Wert von Epic unabhängig von seinen Nutzern und bietet ein hohes Maß an Privatsphäre und Sicherheit, das von böswilligen Akteuren in kriminellen, finanziellen oder politischen Bereichen nicht ohne weiteres manipuliert werden kann.

> **“...VERUNREINIGTE COINS SIND DESTRUKTIV. WENN DU FUNGIBILITÄT UND PRIVATSPHÄRE BRICHST, BRICHST DU DIE WÄHRUNG.”** **ANDREAS ANTONOPOULOS**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 January, 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 April, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 March, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. Skalierbarkeit

Epic Cash ist eine MimbleWimble Blockchain-Implementierung, die Fortschritte in der Skalierbarkeit durch ein platzsparendes Design ermöglicht, das redundante Transaktionsdaten speichert. Die dafür verantwortliche Cut-Through-Funktionalität stellt sicher, dass die Blockchain im Laufe der Zeit im Gegensatz zu den meisten Kryptowährungen, einschließlich Bitcoin, speichereffizienter wird und dass neue Knoten mit minimalen Investitionen in Speicher und Rechenleistung erstellt werden können. Durch die effiziente Platzausnutzung ermöglicht es ein weit verstreutes Netzwerk und fördert die Dezentralisierung. Während jeder Bitcoin-Knoten die gesamte Chain speichern muss, sind Epic Cash-Knoten in der Lage, auf der Grundlage einer kleinen Teilmenge von Blöcken zur Netzwerksicherheit beizutragen.

Die meisten Kryptowährungen erfordern eine unbestimmte Speicherung aller Transaktionsdaten auf ihren Blockchains. Die Bitcoin-Chain erhöht sich derzeit täglich um 0,1353 GB, während die Ethereum-Chain noch schneller um 0,2719 GB pro Tag wächst. Wenn die Bitcoin-Chain weiterhin mit ihrer aktuellen Geschwindigkeit wächst, wird sie schließlich eine Größe von etwa 6 TB erreichen, bis ihr letzter Reward-Block im Jahr 2140 gemined sein wird. Ethereum wird bis zu diesem Zeitpunkt 10 TB überschreiten[9]. In den meisten Blockchains ohne MimbleWimble müssen Transaktionen von Knoten auf der ganzen Welt verifiziert werden. Mit zunehmenden Datenmengen steigt auch die Belastung der einzelnen Knoten. Selbst bei nur 200 GB (der ungefähren Größe der aktuellen Bitcoin-Chain) erfordert die Synchronisation der Daten ein stabiles Netzwerk und eine schnelle Lese- und Schreibfähigkeit der Festplatte. Infolgedessen hat sich das Mining zunehmend auf große Pools konzentriert, die kostspielige Computerressourcen nutzen. **Wenn stattdessen die gesamte Blockchain-Historie von Bitcoin auf der Epic Cash Blockchain gespeichert würde, würde sie um fast 90% reduziert werden**. Kleiner ist schneller, da jede Transaktion weniger Zeit für die Übertragung und Sicherheit benötigt.

MimbleWimble löst dieses Speicherproblem mit einer innovativen Methode des Block- Prunings, die als "Cut-Through" bezeichnet wird. Um zu verstehen, wie Cut-Through funktioniert, ist es am besten zunächst zu untersuchen, wie Transaktionen und Blöcke innerhalb einer MimbleWimble-Blockchain zusammengesetzt sind.

Inputs:

Verweise auf alte Outputs;

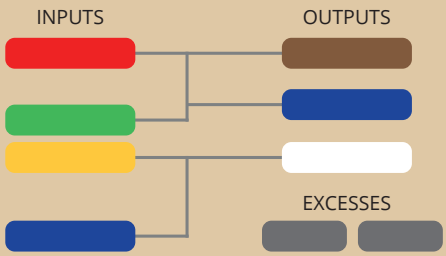
Outputs:

Confidential Transaction outputs und **Rangeproofs**;

Excess:

Der Unterschied zwischen Outputs und Inputs sowie **Signaturen** (zur Authentifizierung und zum Nachweis der Nicht-Inflation).

Abbildung 2:
MimbleWimble Transaktionsteile.



[9] Li, Crypto, ***Blockchain's Big Data Problem,*** 27 January, 2019, https://www.longhash.com/news/blockchains-big-data-problem

Alle Epic Cash Blöcke enthalten:

Merkle Trees von Transaktionsinputs;

Merkle Trees von Transaktionsergebnissen und Rangeproofs;

Eine Liste mit überschüssigen Werten und Signaturen.

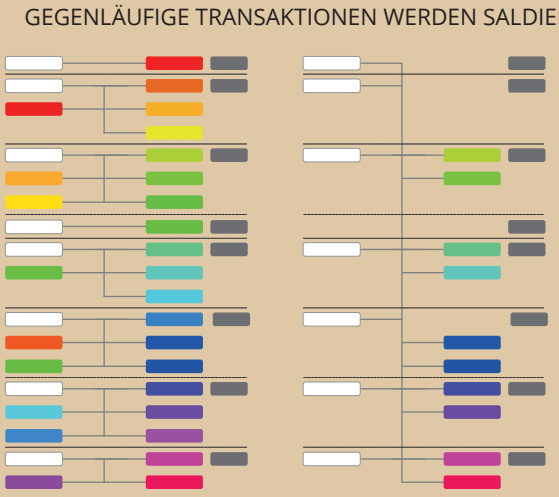
In den Abbildungen 2 und 3, die aus den Präsentationen von Andrew Poelstra[10] übernommen wurden, sehen wir das neu gewonnene Epic als weiße Input-Zellen dargestellt. Identisch gefärbte Zellen stellen Outputs mit entsprechenden verbrauchten Inputs dar. Mit dem Cut-Through-Prozess werden Inputs und passende verbrauchte Outputs entfernt, um Platz innerhalb des Blocks zu schaffen, was die Datenmenge reduziert, die auf der Blockchain gespeichert werden muss. Während die Transaktionen im Ledger weggelassen werden, dokumentieren die verbleibenden überschüssigen Kerne (nur 100 Bytes) dauerhaft, dass die Transaktionen stattgefunden haben.

Während Blöcke weiterhin erstellt werden, wendet MimbleWimble Cut-Through blockübergreifend an, damit auf lange Sicht nur noch die Blockheader (ca. 250 Byte), nicht verbrauchte Transaktionen und Transaktionskerne (ca. 100 Byte) übrig bleiben. Grin, die zweite MimbleWimble-Implementierung, die auf den Markt kam zeigte, dass eine MimbleWimble-Kette mit einer ähnlichen Anzahl von Transaktionen wie die Bitcoin-Kette fast 10% der Größe der Bitcoin-Kette[11] betragen würde. Darüber hinaus wird die Größe eines Knotens "in der Größenordnung von wenigen GB für eine Bitcoin-fähige Kette liegen und möglicherweise auf einige hundert Megabyte optimiert werden können"[12]

Dies steht im deutlichen Gegensatz zu Bitcoin, da hier die gesamte Blockchain von jedem Knoten gespeichert werden muss. Im Laufe der Zeit werden mit zunehmender Flächeneffizienz der Epic Cash Blockchain im Vergleich zur Bitcoin Blockchain auch die Kosteneffizienz im Vergleich zur Teilnahme von Knoten am Epic Cash Netzwerk steigen. Geringere Beteiligungsbarrieren tragen dazu bei, die entscheidende Widerstandsfähigkeit auf der Knotenebene des Netzwerkaufbaus zu gewährleisten.

Durch die Implementierung von MimbleWimble und die Anwendung von Chain Pruning mit dem Cut-Through-Prozess bietet die Epic Cash Blockchain Skalierbarkeit, wie sie von der Kryptowährungsgemeinschaft oft übersehen wird. Es handelt sich um ein Projekt, das die Essenz von Bitcoin und gleichgesinnten Projekten einfängt: Dezentralisierung. Ungeachtet dessen, wie viele Transaktionen pro Sekunde ein Coin verarbeiten kann, was nützt es, wenn es nicht von einem breiten und vielfältigen Netzwerk getragen werden kann? Wenn die Speicheranforderungen so sind, dass die Validierung letztendlich zu starken Mining-Konglomeraten führt, dann sind alle Bemühungen der Krypto-Währungsgemeinschaft, ein dezentrales Ökosystem zu schaffen, obsolet. Um einen zusätzlichen Durchsatz zu gewährleisten, ist eine Layer-2-Implementierung im Lightning-Stil als kurzfristiges Ziel in der Epic Cash Entwicklungs-Roadmap geplant.

Abbildung 3: MimbleWimble Transaktionen vor und nach dem Cut-Through.



[10] SF Bitcoin Developers, ***MimbleWimble with Andrew Poelstra,*** 24 November, 2016, https://www.youtube.com/watch?v=aHTRlbCaUyM&t=940s

[11] Grin Forum, ***Grin Blockchain Size,*** December, 2018, https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] GandalfThePink, ***Introduction to Mimblewimble and Grin,*** 28 March, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V. Geldpolitik

Die Geldpolitik von Epic Cash und Bitcoin ist sehr ähnlich. Das zirkulierende Angebot von Epic Cash wächst zunächst schnell und synchronisiert sich dann 2028 mit dem zirkulierenden Angebot von Bitcoin. Danach steigt sie mit abnehmender Geschwindigkeit an, bis sie 2140 ein maximales Angebot von 21 Millionen Epic erreicht. Epic Cash hat die Qualitäten, ein sicherer Speicher von langfristigem Wert zu werden, da das zirkulierende Angebot zu jedem Zeitpunkt entlang seines Emissionszyklus bekannt ist und in einem festen Maximalangebot gipfelt. Die Geldpolitik von Epic Cash ist durch die folgenden vier Merkmale gekennzeichnet:

- Schnelle Emission in den ersten neun Jahren seiner Lebensdauer, in denen 20.343.750 Epic (96,875% des gesamten Angebots) gemined werden sollen. Die genauen Emissionswerte sind im Abschnitt Emissionsplanung dieses Dokuments beschrieben;
- Ein maximales Angebot von 21 Millionen Epic wird im Jahr 2140 erreicht, etwa zur gleichen Zeit wie Bitcoin ein maximales Angebot von 21 Millionen Einheiten erreicht;
- Die Epic-Umlauf- und Emissionsrate synchronisiert sich mit der von Bitcoin auf der Epic Singularität um den 24. Mai 2028. Nach der Singularität nimmt die Emissionsrate mit zunehmender Geschwindigkeit ab, während das zirkulierende Angebot mit abnehmender Geschwindigkeit wächst;
- Epic hat eine 8 Dezimalteilbarkeitsstruktur, so dass: 1 Epic entspricht 100.000.000.000 Freeman (genau wie 1 Bitcoin 100.000.000 Satoshi entspricht).

Die Geldpolitik von Epic Cash ist aus den folgenden Gründen nach dem Vorbild von Bitcoin gestaltet:

- Vereinbarung mit den wirtschaftlichen Grundlagen von Bitcoin, nämlich dass Knappheit und Vorhersehbarkeit des zirkulierenden Angebots seinem starken Wertspeicher zugrunde liegen;
- Die Öffentlichkeit ist bereits mit dem Modell und der bewährten Erfolgsgeschichte von Bitcoin in den letzten zehn Jahren seit seiner Gründung vertraut. Durch die annähernde Synchronisation mit dem zirkulierenden Angebot von Bitcoin und durch die Spiegelung der maximalen Angebots- und Teilbarkeitsstruktur von Bitcoin geht Epic den Weg des geringsten Widerstandes in Richtung Massenadoption.

VI. Emissionsplanung

Epic Cash verfügt über insgesamt 33 Mining-Epochen, die jeweils durch einen Rückgang der Blockbelohnungen im Vergleich zu ihrer Vorgängerzeit definiert sind. Der Epic Genesis, das Datum an dem der Epic Block #1 gemined wird, findet am August 2019 statt. Es wird 1 Block pro Minute gemined. Die ersten fünf Ären produzieren fast 97% des maximalen Angebots von Epic, was 20 Jahren Bitcoin-Emissionen in etwa neun Jahren entspricht. Dies kann als eine Chance angesehen werden, die Uhr zurückzudrehen" für diejenigen, die den spektakulären Aufstieg von Bitcoin verpasst haben.

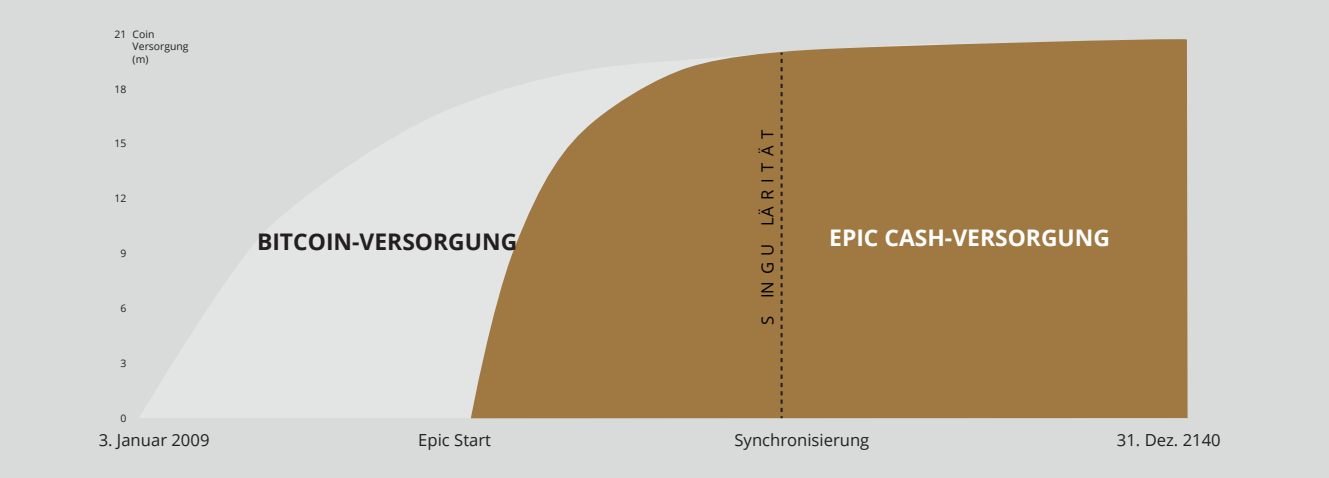
Der Emissionsplan in Tabelle 1 zeigt die Anfangs- und Enddaten der ersten sieben Mining Epochen, die entsprechenden Blockbelohnungen und die daraus resultierenden zirkulierenden Versorgungen für jede Zeit. Die Zeiträume 8 bis 33 sind aus Gründen der Kürze nicht in der Tabelle enthalten. Für diese Epochen sollte es ausreichen zu verstehen, dass jede nachfolgende Ära eine Blockprämie haben wird, die der Hälfte der Belohnung der vorangegangenen Ära entspricht, genau wie bei Bitcoin. Die Menge an Epic, die während jeder dieser Ären freigesetzt wird, ist die Summe der Blockbelohnungen innerhalb der 4-jährigen Ära (ca. 1460 Tage).

Bei der Epic Singularity (2028) schneidet das zirkulierende Epic-Angebot die Anzahl des zirkulierenden Angebots von Bitcoin, zu diesem Zeitpunkt übernimmt Epic Cash die Bitcoin-Blockbelohnung und das Halbierungsmuster, bei dem die Blockbelohnungen alle vier Jahre um die Hälfte sinken. Die einzige Ausnahme ist, dass Epic-Blöcke weiterhin mit einer Rate von einem Block pro Minute gemined werden, im Gegensatz zu Bitcoins Rate von einem Block alle zehn Minuten. Auf diese Weise behält das Epic-Zirkulationsangebot für den Rest seiner Existenz eine ungefähre Parität mit dem zirkulierenden Angebot von Bitcoin.

Tabelle 1: Emissionsplan für die ersten sieben Mining Epochen. Die Daten sind genaue Näherungswerte.

Epoche	1	2	3	4	5	SINGULÄRITÄT	6	7
Block Belohnung	16	8	4	2	1		0.15625	0.078125
Startdatum	Aug 1, 2019	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025		May 24, 2028	May 22, 2032
Enddatum	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025	May 24, 2028		May 22, 2032	May 20, 2036
Dauer (in Tagen)	334	470	601	800	1019		1460	1460
Start- Versorgung	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
End- Versorgung	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% der Maximalversorgung	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

Abbildung 4: Epic- und Bitcoin-Emissionspläne.



VII. Mining

Die Epic Cash Blockchain verfolgt die Dezentralisierung, indem sie eine Vielzahl von Computerhardware begrüßt. Epic Mining ist zunächst für CPUs, GPUs und ASICs verfügbar und verwendet drei entsprechende Hashing-Algorithmen: RandomX, ProgPow und CuckAToo31+. Algorithmen können trivial im laufenden Betrieb ausgetauscht werden, ohne die Integrität der Chainzu beeinträchtigen.

1 RandomX und CPUs

RandomX ist ein Proof-of-Work (PoW)-Algorithmus, der für Universal-CPUs optimiert ist. Es verwendet randomisierte Programmausführungen mit mehreren speicherfesten Techniken, um die folgenden Ziele zu erreichen:

- Verhinderung der Entwicklung von Single-Chip-ASICs;
- Minimierung des Effizienzvorteils spezialisierter Hardware gegenüber Universal-CPUs.

Das Mining von Epic mit CPUs erfordert eine kontinuierliche Zuweisung von 2 GB physischem RAM, 16 KB L1-Cache, 256 KB L2-Cache und 2 MB L3-Cache pro Mining-Thread[13]. Windows 10-Geräte benötigen 8 GB oder mehr RAM. Es ist nicht unvorstellbar, dass Mobiltelefone eines Tages in nicht allzu ferner Zukunft zu lebensfähigen Miningknoten werden könnten. Die frühe CPU-Integration in das Epic Cash Mining Netzwerk ist für viele mit nur bescheidenen Computermitteln eine ausgezeichnete Gelegenheit, Blockbelohnungen zu verdienen, indem sie zur Sicherung des Epic Cash Netzwerks beitragen.

2 ProgPow und GPUs

Programmatischer Proof-of-Work (ProgPow) ist ein Algorithmus, der von der Speicherbandbreite und der Kernberechnung randomisierter mathematischer Sequenzen abhängt, die viele der Rechenfunktionen eines Grafikprozessors nutzen und so die gesamten Energiekosten der Hardware effizient erfassen. Da ProgPow speziell darauf ausgelegt ist, die Vorteile von Standard-GPUs voll auszuschöpfen, ist es schwierig und teuer, durch spezialisierte Hardware deutlich höhere Wirkungsgrade zu erzielen. Somit mildert der ProgPow-Algorithmus Anreize für große ASIC-Pools, GPUs zu übertreffen, wie dies bei vielen anderen PoW-Algorithmen, wie beispielsweise dem SHA-256 von Bitcoin, häufig der Fall ist. GPUs sind zwar nicht so verbreitet wie CPUs aber immer noch allgemein verfügbar. Mit der technologischen Entwicklung, die von den Kraftwerken Nvidia und AMD vorangetrieben wird, sind GPUs in der Lage, viele Vielfache von Mining-Lösungen über CPUs pro Einheit parallel zu verarbeiten. Dank dieser Kombination aus Allgegenwärtigkeit und hoher Rechenleistung werden GPUs das Rückgrat für einen Großteil der Mining-Aktivitäten während der Anfangszeiträume bilden, wie in Tabelle 2 dargestellt.

3 CuckAToo+31 und ASICs

CuckAToo31+ ist eine ASIC-freundliche Permutation des Cuckoo Cycle Algorithmus, der vom niederländischen Informatiker John Tromp entwickelt wurde. Als Verwandter des ASIC-resistenten CuckARoo29 erzeugt CuckAToo31+ zufällige zweiteilige Graphen und stellt die Miner vor die Aufgabe, eine Schleife von gegebener Länge 'N' zu finden, die durch die Ecken dieses Graphen verläuft.

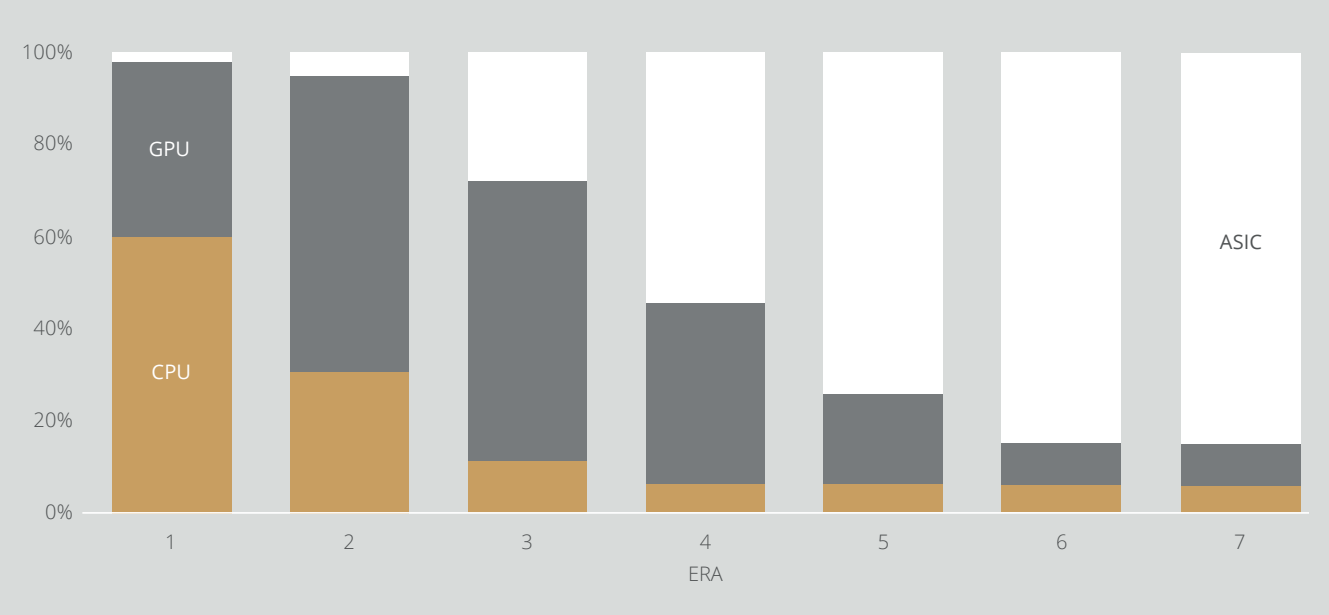
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

Dies ist eine speichergebundene Aufgabe, d.h. die Lösungszeit wird durch die Speicherbandbreite und nicht durch die Rohprozessor- oder GPU-Geschwindigkeit begrenzt. Infolgedessen produzieren die Cuckoo Cycle Algorithmen weniger Wärme und verbrauchen deutlich weniger Energie als herkömmliche PoW Algorithmen. Der ASIC-freundliche CuckATOo31+ ermöglicht Effizienzsteigerungen gegenüber GPUs, indem er Hunderte von MB SRAM verwendet und gleichzeitig durch den Speicher I/O[14] Engpässe verursacht. Letztendlich bieten ASICs die größten potenziellen Skaleneffekte der drei Mining Optionen. Obwohl ihnen jedoch im Interesse der Inklusivität frühzeitig ein kleiner Teil der Mining-Belohnungen im Verhältnis zu CPUs und GPUs zugewiesen wird, übernehmen schließlich ASICs eine Mehrheitsbeteiligung an die Block Belohnungen des geminten Blocks, unter der Annahme, dass es ein wettbewerbsfähiges Ökosystem von Geräteherstellern für CuckATOo31+ geben wird.

Tabelle 2: Mining Belohnungen Zuteilungen. Änderungen vorbehalten. Die Zuteilungen werden auf eine maximale Dezentralisierung ausgerichtet und stehen im Einklang mit den langfristigen Interessen des Netzwerks.

Epoche	1	2	3	4	5	6	7
Tage	334	470	601	800	1019	1460	1460
CPUs	60%	30%	10%	5%	5%	5%	5%
GPUs	38%	65%	62%	40%	20%	10%	10%
ASICs	2%	5%	28%	55%	75%	85%	85%

Abbildung 5: Mining Belohnungskontingente für jede Epoche gemäß Tabelle 2. Änderungen vorbehalten.



[14] Le Sceller, Quentin, ***An Introduction to Grin Proof-of-Work,*** 16 November, 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 Mining-Beiträge

Beginnend mit dem Epic Genesis (2019) und endend mit dem Epic Singularity (2028), gibt es während des Mining-Prozesses eine Zuordnung von Epic, die als Mining-Beiträge an die EPIC Blockchain Foundation weitergeleitet wird.

Die EPIC Blockchain Foundation widmet sich der technischen Entwicklung und der Förderung des Bekanntheitsgrades und Nutzens des Epic Cash-Projekts in den ersten Jahren seiner Gründung, indem sie Marketingaktivitäten durchführt und Partnerschaften innerhalb der Finanztechnologiebranche entwickelt.

Nach der Singularität wird die Rolle der EPIC-Stiftung von der EPIC Distributed Autonomous Corporation (EDAC) übernommen, die von der Stiftung vor der Übergabe entwickelt wird.

Die EPIC Blockchain Foundation wird durch einen Prozentsatz der Mining-Belohnungen finanziert, die von den Blockbelohnungen abgezogen werden, gemäß den folgenden Jahresraten:

Tabelle 3: Jährliche Raten für die Miningbeiträge der Foundation als Prozentsatz der Mining-Belohnungen.

Jahr	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
% der Mining-Belohnungen	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. Fazit

Epic strebt die Anerkennung als "dezentrales digitales Silber" an, ein Gegenstück zu Bitcoins anerkannter Position als dezentrales digitales Gold. Durch die Wiedereinführung der verlorenen Fungibilität auf einem viel energieeffizienteren und umweltfreundlicheren Hardware-Backbone kippt Epic Cash die Machtverhältnisse zugunsten der einzelnen Benutzer und steht damit im starken Gegensatz zu den jüngsten Zentralisierungstrends. Die Kombination von Bitcoin-Ökonomie, Spieltheorie und bewährter Proof-of-Work-Formel mit dem Besten der modernen Blockchain-Technologie führt zu einer vertrauenswürdigen, unveränderlichen und dezentralen Währung (Epic), die skalierbar und fungibel ist und die Privatsphäre ihrer Nutzer schützt. Die Epic Cash Blockchain ist offen, öffentlich, grenzenlos und zensurresistent. Sie bewahrt die Privatsphäre und den Reichtum ihrer Benutzer und belohnt diejenigen, die ihre Hardware zur Unterstützung des Netzwerks über Mining einsetzen. Jedes Epic wird durch den Nachweis der Arbeit erschaffen. Die Lieferung beginnt bei Null und das Netzwerk gilt als fair gestartet, wobei derzeit ein funktionales Testnetz läuft.

Epic Cash Schlüsselfakten :

- **Das Mining beginnt am August 2019.**

- **Die Epic Cash Blockchain basiert auf MimbleWimble.**

  Definierende Merkmale des Protokolls sind:

  1. **Cut-Through** - die Entfernung redundanter Informationen aus der Blockchain, um die Raumeffizienz zu fördern, eine breite Beteiligung an der Netzwerkbereinigung zu fördern und die Dezentralisierung zu unterstützen;
  2. **CoinJoin** - die Bündelung von Transaktionen innerhalb eines Blocks, um die Fungibilität der Epic Kryptowährung zu gewährleisten;
  3. **Dandelion++ Protokoll** - die Verbreitung von Transaktionen durch Kommunikation über verschachtelte Kanäle und Diffusion über ein breites Netzwerk von Knoten, wobei Verbindungen zwischen Transaktionen und ihrem Ursprung getrennt werden;
  4. **Keine Wallet-Adressen** - die Verwendung einer großen Multisignatur zur Generierung von privaten Einweg-Schlüsseln für Transaktionspartner, wodurch die Notwendigkeit von Wallet-Adressen vollständig entfällt.

- **Die Geldpolitik von Epic Cash** zielt darauf ab, das Epic-Umlaufangebot mit dem Bitcoin-Umlaufangebot in etwa neun Jahren zu synchronisieren und im Jahr 2140 das gleiche maximale Angebot von 21 Millionen Einheiten parallel zu Bitcoin zu erreichen. Diese immer weniger inflationäre Politik garantiert Transparenz, Vorhersehbarkeit des Angebots und Knappheit und fördert die Sicherheit der langfristigen Wertspeicherung.

- **Mining**, das CPUs, GPUs und ASICs über entsprechende RandomX-, ProgPow- und CuckAToo31+-Algorithmen integriert, um die Massenübernahme und Netzwerkeffizienz zu erleichtern.

IX. Technische Spezifikationen

Projektname: Epic Cash
Währungsname: Epic
Blockzeit: 60 Sekunden
Blockgröße: 1 MB
Start- Versorgung: 0
End- Versorgung: 21.000.000
Genesis Block: August 2019
Konsens : RandomX (CPUs), ProgPow (GPUs) und CuckATOO31+ (ASICs)

Links:

www.epic.tech

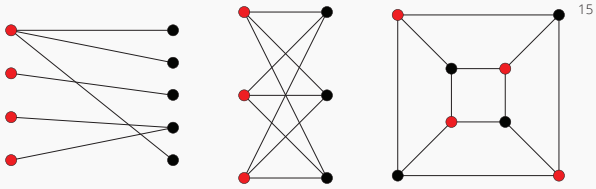
t.me/EpicCash – Telegram

t.me/EpicCashDeutsch

X. Glossar

ASIC Anwendungsspez. integr. Schaltungen; Chips, die für einen bestimmten Zweck entwickelt wurden.

Zweiteiliger Graphit einen Satz von Graph-Eckpunkten, die in zwei disjunkte Mengen zerlegt sind, so dass keine zwei Graph-Eckpunkte innerhalb desselben Satzes benachbart sind.



Blindungsfaktor ein zufälliges Element, das in eine digitale Nachricht eingeführt wird, um die Verschlüsselung zu erleichtern; ein gemeinsames Geheimnis zwischen beiden Parteien, das die Ein- und Ausgänge der jeweiligen Transaktion sowie die öffentlichen und privaten Schlüssel der Transaktionspartner verschlüsselt[16].

Block Belohnung das neue Epic, das vom Netzwerk als Belohnung für Berechnungen zur Überprüfung der Transaktionen innerhalb eines neuen Blocks verteilt wird.

Cache eine Hard- oder Softwarekomponente, die Daten so speichert, dass zukünftige Anforderungen dafür erfüllt werden. Daten können schneller bereitgestellt werden.

Zirkulierende Versorgung die Menge an Epic, die zu einem bestimmten Zeitpunkt existiert.

CPU Central Processing Unit: Computerkomponente, die für das Dolmetschen und Übersetzen verantwortlich ist. Ausführen der meisten Befehle von der anderen Hard- und Software des Computers.

Cut-Through einen MimbleWimble-Blockchain-Prozess, bei dem Eingaben und übereinstimmende ausgegebene Ausgaben entfernt werden, um Platz innerhalb des Blocks freizugeben und so die Menge der Daten zu reduzieren, die in der Blockchain gespeichert werden müssen.

Dezentralisierung den Stand der Streuung der Betriebsabläufe und der Governance eines Netzwerks.

Emission die Erschaffung neuer Epics, die von Minern in Blockbelohnungen verdient wurden. Epic wird alle 60 Sekunden erstellt, wenn Transaktionen in der Blockchain bestätigt werden.

Epic Singularität der Zeitpunkt, an dem die Versorgung von Epic mit der Versorgung von Bitcoin übereinstimmt (Mai 2028).

Überschuss (MimbleWimble) der Unterschied zwischen Outputs und Inputs sowie Signaturen (Authentifizierung)

Fungibilität die Eigenschaft eines Gutes oder einer Ware, wobei einzelne Einheiten im Wesentlichen austauschbar sind und jedes seiner Teile von einem anderen Teil nicht unterscheidbar ist.

Genesis (Event) das Mining des ersten Epic-Blocks und der offizielle Beginn der Blockchain.

GPU Graphikprozessor: Einheit, die einen programmierbaren Logikchip (Prozessor) enthält, der für Anzeigefunktionen spezialisiert ist. Consumer-GPUs eignen sich gut für das Kryptowährungs-Mining.

Halbierung (für Bitcoin) tritt alle 4 Jahre auf. Die Versorgungsrate sinkt nach jeder Halbierung um 50%.

Hash einen Wert, der aus einer Basis-Eingabezahl unter Verwendung einer Hashing-Funktion berechnet wird.

Hashing-Algorithmus (Funktion) mathematischer Algorithmus, der Daten beliebiger Größe auf einen Hash fester Größe abbildet, der zum Erzeugen und Verifizieren digitaler Signaturen, Message Authentication Codes (MACs) und anderer Formen der Authentifizierung verwendet wird.

Homomorphe Verschlüsselung ein Verfahren zum Durchführen von Berechnungen an verschlüsselten Informationen, ohne diese vorher zu entschlüsseln.

Unveränderlichkeit (in der Programmierung) der Zustand, in dem ein Objekt nach seiner Erstellung nicht mehr verändert werden kann.

Input (MimbleWimble) die Komponente einer MimbleWimble-Transaktion, die die sendende Partei der Transaktion repräsentiert; erstellt aus Ausgaben früherer Transaktionen.

I/O Input/Output; die Kommunikation zwischen einem Informationsverarbeitungssystem, wie beispielsweise einem Computer, und der Außenwelt, möglicherweise einem Menschen oder einem anderen Informationsverarbeitungssystem.

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, ***Grin Coin and MimbleWimble: An Introductory Guide***, 18 October, 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

Maximale Versorgung	die zu erreichende Menge an Epic, an der sich das Umlaufangebot danach nicht erhöht (21.000.000 Epic).
Speicherfest	die Verwendung von viel RAM, um gleichzeitige Verbindungen mit parallelen Versuchen auszuschließen. Speicherfeste Funktionen sind Algorithmen, deren Berechnungszeiten in erster Linie vom verfügbaren Speicher bestimmt werden, um Daten zu speichern. Auch bekannt als speichergebundene Funktionen.
Merkle Tree	eine Datenstruktur, die in computerwissenschaftlichen Anwendungen verwendet wird. In Blockchains ermöglichen Merkle-Trees eine effiziente und sichere Verifikation der Inhalte in großen Datenstrukturen.
MimbleWimble	ein Protokoll, das von einem pseudonymen Mitwirkenden, dem Spitznamen Tom Elvis Jedusor, in einem Bitcoin-Entwickler-Chatroom erstellt wurde.
Multisignatur	ein digitales Signaturschema, das einer Benutzergruppe ermöglicht, ein einzelnes Dokument zu signieren. Normalerweise erzeugt ein Multisignatur-Algorithmus eine gemeinsame Signatur, die kompakter ist als eine Sammlung von unterschiedlichen Signaturen aller Benutzer[17].
Knoten	Computer, der sich mit einem Blockchain-Netzwerk verbindet und zu anderen Knoten des Netzwerks verzweigt, um Informationen über Transaktionen und Blöcke in Peer-to-Peer-Manier zu verteilen.
Einweg-Aggregatsignatur (OWAS)	eine Transaktionssignatur, die aus vielen Signaturen besteht und so verschlüsselt ist, dass es sehr schwierig ist, die einzelnen Signaturen zu berechnen, die Teil des Aggregats sind.
Output (MimbleWimble)	die Komponente einer MimbleWimble-Transaktion, die den Empfang der Transaktion darstellt; wird als Input für nachfolgende Transaktionen verwendet.
Pedersen Engagement-Programm	ein kryptographisches Element, das es einem Spender erlaubt, sich an einen ausgewählten Wert zu binden, ohne Informationen darüber zu enthüllen und ohne dass der Spender in der Lage ist, die Bindung an diesen Wert rückgängig zu machen.
Private Key	ein Private Key ist ein winziges Stück Code, das mit einem Public Key gepaart ist, um Algorithmen zur Textver- und -entschlüsselung zu aktivieren. Es wird als Teil der Public-Key-Kryptographie bei der asymmetrischen Schlüsselverschlüsselung erstellt und dient zur Entschlüsselung und Transformation einer Nachricht in ein lesbares Format.
Proof of Work (PoW)	ein Datenstück, das schwer zu produzieren (kostspielig und zeitaufwendig), aber für andere leicht zu überprüfen ist und bestimmte Anforderungen erfüllt. Proof of Work wird häufig bei der Generierung von Blöcken für Kryptowährungen eingesetzt.
Public Key	ein Public Key wird in der Public-Key-Verschlüsselung erzeugt, die Algorithmen der asymmetrischen Schlüsselverschlüsselung anwendet. Public Keys werden verwendet, um eine Nachricht in ein unlesbares Format zu konvertieren.
RAM (Random Access Memory)	Datenspeicherchips für schnellen Zugriff auf Daten in einem Computergerät, in dem das Betriebssystem (OS), Anwendungsprogramme und aktuell verwendete Daten aufbewahrt werden, so dass sie vom Prozessor des Geräts schnell erreicht werden können.
Rangeproofs	eine Commitment-Validierung zur Überprüfung, ob die Summe der Transaktionseingaben größer ist als die Summe der Transaktionsausgaben und ob alle Transaktionswerte positiv sind. Rangeproofs stellen sicher, dass die Geldmenge nicht manipuliert wird.
(Digitale) Signatur	ein Standardteil eines Blockchain-Protokolls, das hauptsächlich zur Sicherung von Transaktionen und Transaktionsblöcken, zur Übertragung von Informationen, zur Vertragsverwaltung und in allen anderen Fällen, in denen die Erkennung und Verhinderung von externen Manipulationen wichtig ist, verwendet wird. Diese bieten drei Vorteile bei der Speicherung und Übertragung von Informationen auf der Blockchain: • Diese zeigen an, ob die gesendeten Daten manipuliert wurden; • Prüfung der Teilnahme einer bestimmten Partei an der Transaktion; • Kann rechtsverbindlich sein;
SRAM (Static Random Access Memory)	Random Access Memory (RAM) zur Aufbewahrung von Datenbits in seinem Speicher, solange Strom zugeführt wird.
Durchsatz	das Messen von Transaktionen pro Sekunde, die von einem gegebenen Kryptowährungsprotokoll durchgeführt werden können.
Vertrauenslosigkeit	die Qualität eines Kryptowährungsnetzwerks zur Einhaltung von Regeln eines Protokolls ohne Durchsetzung durch eine zentrale Partei.

[17] Bellare, Mihir, Neven, Gregory, 2007, ***Identity-based Multi-signatures from RSA***, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

EPIC PRIVATES INTERNET GELD