



Universal Credit System

Eine Kryptowährung der nächsten Generation

Willkommen!

In diesem Dokument finden Sie alles Wissenswerte zur neuen und innovativen Kryptowährung der nächsten Generation – dem **Universal Credit System**. Es enthält alle Informationen, die Sie benötigen um das Universal Credit System zu verstehen und ihm zu vertrauen.

Dieses Dokument dient als eine Art Whitepaper, welches eine genaue Spezifikation der Kryptowährung enthält. Des Weiteren sollen in diesem Dokument die logischen Abläufe für jedermann verständlich dargestellt werden.

Der Universal Credit Standard

Der **Universal Credit Standard** ist ein unabhängiger digitaler Kryptowährungs-Standard. Er soll allen Benutzern die Teilnahme am Handel und den Aufbau von Wohlstand ermöglichen. Das **Universal Credit System** ist die zugrunde liegende Software zur Verwaltung der Währung (Wallet) und die in dieser Software ausgezahlte Währung wird **Universal Credit Coins (UCC)** genannt.

Der *Universal Credit Standard* und die dahinter liegenden Prinzipien unterscheiden sich jedoch grundlegend von anderen Kryptowährungen. Denn anstatt wie bisher neue Blöcke in einer wie auch immer gearteten Form zu *minen* und dafür eine *reward* zu kassieren, wird allen Teilnehmern jeden Tag eine festgelegte Anzahl von Universal Credit Coins einfach *gutgeschrieben*.

Diese Universal Credit Coins werden nicht von einer zentralen Instanz gutgeschrieben oder gewährt, sondern die Teilnehmer verwalten sich selbst auf Basis eines Algorithmus. Die gewährten Universal Credit Coins sind unbegrenzt gültig und können vom Empfänger frei verwendet werden.

Die Auszahlung folgt einer einfachen Regel:

1.000000000 UCC pro Benutzer pro Tag

Mit Hilfe dieser einfachen Regel lässt sich der Wert einer Sache, aber auch der Wert eines Coins zu jeder Zeit einfach nachvollziehen. Hat etwas einen Preis von z.B. 200 UCC, so handelt es sich um die Coins von rund 200 Tagen. Und es ist egal ob heute, in 3 Jahren oder in 10 Jahren. Die Anzahl von 200 Coins entspricht der Auszahlung von 200 Tagen.

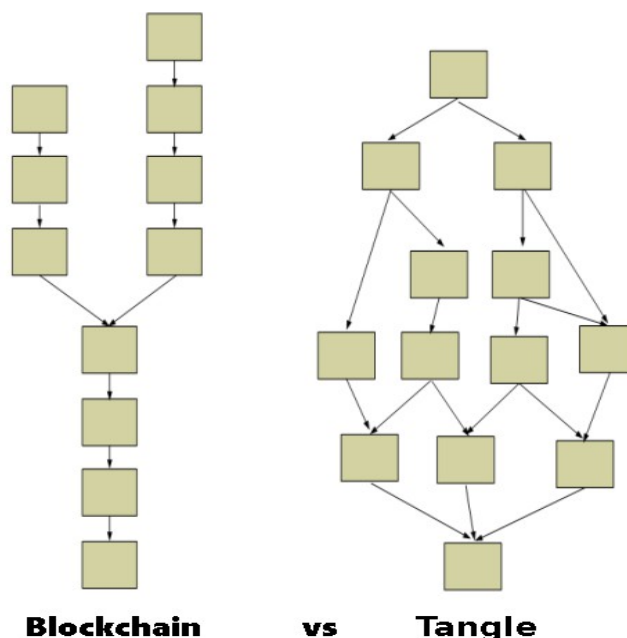
Weil die Belohnung / Auszahlung an die vergangene Zeit gebunden ist und immer gleichbleibend ist, entsprechen die Universal Credit Coins der Definition eines „stable coins“.

Der proof-of-Trust Algorithmus [poT]

Während die meisten Kryptowährungen entweder *proof-of-work*- oder *proof-of-stake*-/*delegated-proof-of-stake*-Algorithmen verwenden um einen Konsens zu erzielen ist die im Universal Credit System angewandte Technik grundlegend anders. Der im UCS verwendete Algorithmus lautet **proof-of-Trust-Algorithmus** („Vertrauensnachweis-Algorithmus“) und wurde komplett neu entwickelt.

Anstatt wie bei Bitcoin den Konsens aus einem monolithischen und zentralen Ledger (Blockchain) heraus bilden, verwendet das Universal Credit System eine Architektur basierend auf einem **gerichteten azyklischen Graphen** (englisch *DAG, directed acyclic graph*) bei der jeder Benutzer seine eigene Blockchain im Sinne einer Blockgitter-Struktur verwaltet (ein sogenannter „true distributed ledger“). Jeder Block eines Benutzers entspricht dabei einer Transaktion und die Blöcke sind untereinander **nicht** verkettet.

Die Struktur ähnelt dabei dem sogenannten „*tangle*“ (zu deutsch: „Gewirr“) der Kryptowährung IOTA. Im Unterschied zu IOTA wird der Konsens innerhalb des Netzwerks jedoch auf eine andere Art und Weise gebildet. Mit der verwendeten Architektur eines gerichteten, azyklischen Graphen unterscheidet sich die Kryptowährung bereits grundlegend von anderen, blockchain-basierten Architekturen:



Zwar erbringen Benutzer auch im UCS in gewissem Sinne einen Arbeitsnachweis (*pow*) indem sie ihre eigenen Transaktionen signieren und die Transaktionen anderer überprüfen, jedoch wird der Konsens über einen Kontostand nur zu einem Teil über diesen Arbeitsnachweis ermittelt. Den weitaus größeren Einfluss auf einen Kontostand haben die täglich ausbezahlten Coins, welche durch das beglaubigte Erstellungsdatum ermittelt werden. Das beglaubigte Erstellungsdatum sowie die vom Benutzer signierten als auch die an ihn gerichteten Transaktionen bilden zusammen mit den Bestätigungen von anderen Benutzern den *proof-of-Trust*.

Da die Teilnehmer sich selbst verwalten ist keine dauerhafte Online-Verbindung erforderlich. Jeder Benutzer verwaltet seine eigene Version des Blockgitters. Die Benutzer liefern sich bei jeder Aktion gegenseitig Vertrauensnachweise, welche die Gültigkeit ihres Kontostands gegenüber anderen Teilnehmern mathematisch beweisen.

Benutzer und die Beglaubigung des Erstellungsdatums von der TSA (Time Stamping Authority)

Jede Entität, von nun an als neutraler „Benutzer“ bezeichnet (ein Benutzer kann alles sein), darf ein Paar von 4096bit RSA-Schlüsseln erstellen. Der Benutzer muss den öffentlichen Schlüssel sofort einer RFC-3161 konformen Time Stamping Authority (TSA) mitteilen, die als unabhängiger Notar fungiert und das Erstellungsdatum des Profils **innerhalb von 120 Sekunden** beglaubigt. Die TSA bescheinigt dem Benutzer das Vorhandensein seines Keys zum Erstellungszeitpunkt. Dieser beglaubigte Erstellungszeitpunkt dient als Basis zur Berechnung der täglichen Auszahlung.

Die Beglaubigung eines neuen Benutzers bei der Erstellung ist der einzige Zeitpunkt an dem eine Internet-Verbindung zwingend erforderlich ist. Für alle weiteren Aktionen ist eine Internet-Verbindung nicht erforderlich.

Transaktionen

Ein Benutzer kann eine Transaktion erstellen, die seine Adresse als Absender, den Betrag, den Empfänger und den aktuellen Zeitstempel enthält und signiert dann diese Transaktion mit seinem privaten Schlüssel. Der Benutzer erstellt dann die Transaktionsdatei, die er dem Zahlungsempfänger auf einem Weg seiner Wahl zukommen lassen kann. Er muss dazu nicht mit dem Internet verbunden sein sondern kann ein beliebiges Medium seiner Wahl zum Austausch der Transaktionsdatei verwenden. Der Empfänger kann dann mit Hilfe des öffentlichen Schlüssels die Authentizität der Transaktion überprüfen und mit Hilfe des *proof-of-Trust* die Transaktion und damit verbundene Guthaben verifizieren.

Die Transaktionsdatei ist genau genommen ein Archiv, welches zur Abwicklung der Transaktion den öffentlichen Schlüssel des Senders, die Beglaubigung der TSA, sowie alle vom Sender zuvor gesendeten und empfangenen Transaktionen enthält. Des Weiteren enthält sie alle bisher gesammelten Schlüssel, deren TSA-Beglaubigungen und Transaktionen die im Besitz des Senders zu diesem Zeitpunkt waren. Dies dient dem Aufbau eines gemeinsamen Transaktionswissens.

Dieses gemeinsame Transaktionswissen wird dazu verwendet Abhängigkeiten von Transaktionen zu ermitteln und die damit verbundenen Guthaben überprüfen zu können. Dies ist besonders in Hinblick auf die Ermittlung von Guthaben wichtig, da ein Benutzer unter Umständen abhängig war von einer an ihn gesendeten Transaktion. Hier ein Beispiel zu einer Transaktion, die von anderen Transaktionen abhängig ist:

<u>Benutzer A Kontostand</u>	<u>Transaktion</u>
0	
100	+100 gewährt von System
200	+100 empfangen von Benutzer B
50	-150 gesendet an Benutzer C

Wie man sieht, hat *Benutzer A* die Transaktion von 150 Credit Coins nur senden können, weil er vorher selbst 100 Credit Coins von *Benutzer B* empfangen hat. Diese letzte Transaktion (150 Credit Coins) ist abhängig von einer zuvor eingegangenen Transaktion. Solche Abhängigkeiten lassen sich durch die gesammelten *proof-of-Trusts* der anderen Benutzer ermitteln und überprüfen.

Transaktionen und Bestätigungen

Eine Transaktion ist, sofern sie plausibel ist, immer sofort gültig für den Sender. Das bedeutet, dass wenn eine Transaktion erfolgreich erstellt wurde sich sofort der Kontostand des Senders verringert. Im Gegenzug erhöht sich der Kontostand des Empfängers erst wenn er die Transaktion eingelesen und eine Anzahl Bestätigungen von anderen Benutzern gesammelt hat. Durch Synchronisation und zukünftige Transaktionen, welche von Sender und Empfänger getätigt werden verbreitet sich das Wissen über diese Transaktion und andere Benutzer bestätigen / beglaubigen sie.

Eine Transaktion benötigt eine gewisse Anzahl an Bestätigungen von anderen Benutzern um von bisher unbeteiligten Benutzern in Zukunft bei einer Transaktion anerkannt zu werden. Das Problem ist insbesondere bei der Überprüfung von abhängigen Zahlungen von Bedeutung, da die Zahlung von der der Sender abhängig ist unter Umständen noch nicht genug Bestätigungen hat um als gültig betrachtet zu werden. Aber auch sogenannte „*Stale Blocks*“, welche bei einer Double-Spend-Attacke entstehen, können so erkannt werden.

Damit eine Transaktion bei der Berechnung eines Kontostands berücksichtigt werden kann muss sie von **mindestens 2 Benutzern bestätigt** werden damit sie möglichst endgültig ist und der Sender diese Transaktion in Zukunft nicht mehr abstreiten kann („double-spending“- und „0 race“-Attacken).

Der Prozess der Statusänderung einer Zahlung (von *ungültig* über *teilweise gültig* hin zu *endgültig*) ist niemals endend d.h. eine Transaktion ist niemals total endgültig, sondern eine Transaktion wird mehr und mehr endgültig. An einem gewissen Punkt liegen genug Bestätigungen vor, dass sie als gültig erachtet werden kann.

Diese Bestätigung der anderen Benutzer über das Vorhandensein einer Transaktion nennt sich **Confirmation**. Die Anzahl *Confirmations* einer Transaktion ist ausschlaggebend dafür ab wann sie für andere Benutzer als gültig oder ausreichend bestätigt angesehen werden kann. Dieser Wert ist standardmäßig auf **2 Bestätigungen von anderen Benutzern** eingestellt. Diese Bestätigungen müssen von an der Transaktion nicht beteiligten Benutzern (weder Sender, noch Empfänger) getätigt werden. Diese Benutzer bestätigen / beglaubigen

dann als eine Art Notar diese Transaktion indem sie die Transaktions-Datei in ihrer Index-Datei mit auflisten.

Dass der Empfänger zur Verarbeitung 1 Transaktion mindestens 2 Confirmations benötigt, stellt eine exponentielle Verbreitung des Transaktionswissens sicher.

Hier eine Übersicht über die Anzahl an Bestätigungen einer Transaktion und die Gültigkeit (bei der Standardeinstellung):

<u>Bestätigungen</u>	<u>Gültigkeit</u>
0	Nicht Gültig (pending)
1	Nicht Gültig (pending)
2	Gültig (valid)
3	Gültig
...	...
∞	Entgültig (final)

Die aktuelle Anzahl an *Confirmations* einer Transaktion kann in der Transaktionshistorie des *Universal Credit Systems* eingesehen werden. Um sicherzustellen, dass alle Transaktionen, welche man getätigt oder empfangen hat ausreichend bestätigt werden macht es also Sinn sich so schnell wie möglich mit anderen Benutzern zu synchronisieren.

Scoring

Um zu verhindern, dass sich ein Benutzer eine beliebige Anzahl an weiteren Accounts erstellt findet ein sogenanntes Scoring des Benutzers statt. Dies bedeutet, dass die gesendeten Transaktionen, die empfangenen Transaktionen und das Guthaben des Benutzers gegeneinander abgewogen werden. Der Score-Wert eines Benutzers wird nach folgenden 5 Regeln berechnet:

- Jeden Tag erhöht sich der Score aller Benutzer um den Payout
- Direkt nach der Erstellung einer Transaktion verringert sich der Score um den Transaktionsbetrag
- Hat die Transaktion genügend Confirmations erlangt erhöht sich der Score des Sender des ursprünglichen Betrag
- Der Score kann nicht geringer sein als 0
- Der Score kann nicht höher sein als das Guthaben

Das Scoring stellt somit sicher, dass ein Benutzer nicht unendlich viele Credits von anderen Benutzern sammeln und sofort wieder ausgeben kann. Stattdessen werden im Laufe der Zeit immer mehr Credits des Guthabens freigeschaltet. Wenn ein Benutzer nicht genug Guthaben hat, um etwas zu kaufen, ist es für ihn unmöglich, dies zu umgehen, indem er mehrere andere Konten erstellt und die Auszahlungen einzieht, da er sie nicht auf einmal senden kann.

Beispiel ohne Scoring:

- Konto A hat Saldo 5 UCC Konto A möchte etwas zum Preis von 10 UCC kaufen
- Konto A erstellt die Konten B, C, D, E und wartet 1 Tag auf die erste Auszahlung
- Konto A hat am nächsten Tag hat einen Saldo von 6 UCC, die Konten B, C, D und E haben jeweils 1 UCC Saldo
- die Konten B, C, D, E senden jeweils 1 UCC an Konto A und erhöhen den Saldo von 6 UCC auf 10 UCC
- Konto A hat nun einen Saldo von 10 UCC

In diesem Beispiel ohne Wertung hat Konto A nun 10 UCC und könnte den Artikel kaufen.

Beispiel mit Scoring:

- Konto A hat einen Saldo von 5 UCC und einen Score-Wert von 5 UCC
- Konto A möchte etwas zum Preis von 10 UCC kaufen
- Konto A erstellt die Konten B, C, D, E und wartet 1 Tag auf die erste Auszahlung
- Konto A hat am nächsten Tag einen Saldo von 6 UCC, Konten B, C, D und E haben jeweils 1 UCC Saldo
- Die Konten B, C, D, E senden jeweils 1 UCC an Konto A und erhöhen den Saldo von 6 UCC auf 10 UCC
- Konto A hat nun einen Saldo von 10 UCC, aber nur einen Score-Wert von 6 UCC

A hat jetzt einen Saldo von 10 UCC, aber aufgrund des Score-Werts (Saldo ist gleich Score-Wert, so dass der Score-Wert nicht berührt wird) sind nur 6 UCC (die anfänglichen 5 UCC + 1 UCC Auszahlung für den Tag, den er gewartet hat) freigeschaltet und können ausgegeben werden. Wenn Sie die 6 UCC ausgeben wird der Rest des Guthabens freigeschaltet. Beim Scoring kann ein Benutzer also nur die täglichen Auszahlungen unbegrenzt ausgeben und muss die erhaltenen Credits freischalten. Im Beispiel ohne Scoring kann Konto A den gesamten Betrag in einer Transaktion ausgeben, während Konto A mit Scoring nicht den gesamten Betrag ausgeben kann.

Es ist sehr wichtig, dass der gesamte Betrag in einer einzigen Transaktion gesendet wird, wenn Sie dem Absender nicht vertrauen können. Dadurch wird sichergestellt, dass Angreifer keine Guthaben von einer potenziell unendlichen Anzahl von Konten, die sie erstellt haben, ausgeben können. Diese Vorsichtsmaßnahme auf Basis des Scoring-Prozess schützt Sie und alle anderen Teilnehmer vor betrügerischen Benutzern.
Ermittlung des Kontostands

Der Saldo eines Kontos wird von den Benutzern selbst ermittelt, wobei die Benutzer sich gegenseitig immer wieder selbst überprüfen.

Um den Kontostand eines Benutzers zu ermitteln wird zunächst beginnend beim beglaubigten Erstellungsdatum des Schlüssels die daraus resultierende *creditload* für diesen ersten Tag berechnet und dann eventuelle gesendete oder empfangene Transaktionen davon subtrahiert bzw. aufaddiert. Das Ergebnis ist der Kontostand am Ende dieses Tages und dient als Basiskontostand für den folgenden Tag auf den zunächst wieder die *creditload* aufaddiert wird und dann wieder eventuelle ausgehende oder eingehende Transaktionen subtrahiert bzw. aufaddiert werden.

Diese Berechnung wird Tag für Tag bis zum aktuellen Tag fortgesetzt, wobei der Kontostand nie die 0-Grenze unterschreiten darf. Das *Universal Credit System* ist so programmiert, dass ein Benutzer nie mehr Coins ausgeben kann, als er Guthaben besitzt. Im Umkehrschluss lassen sich Transaktionen von Konten, die nach allgemeinem Konsens kein Guthaben aufweisen, auch nicht gutschreiben da sie keine Confirmations erhalten.

Gemeinschaftlicher Konsens

Die Benutzer verifizieren sich bei einer Transaktion oder nach einer Synchronisation gegenseitig indem sie die gesammelten proofs-of-trust (Vertrauensnachweise) des jeweils anderen überprüfen.

Um es einfach auszudrücken:

Wenn ein Benutzer eine Transaktion tätigen möchte, muss er den anderen Teilnehmern und insbesondere dem Empfänger nachweisen, dass genügend Guthaben vorhanden ist, um diese Transaktion durchzuführen. Diesen Nachweis erbringt er durch die gesammelten proof-of-trusts.

Die Validierung einer Transaktion erfolgt permanent und wiederkehrend durch die anderen Teilnehmer. Durch Errechnung der Kontostände und der damit einhergehenden Überprüfung der Transaktionen unter Berücksichtigung der bisher vorzuweisenden Bestätigungen und des Score-Werts des Benutzers wird ein gemeinsamer Konsens erzielt.

Synchronisation mit anderen Benutzern

Benutzer können sich mit anderen Benutzern unabhängig von untereinander ausgetauschten Transaktionen synchronisieren um Vertrauen und Wissen aufzubauen. Dies sollten Benutzer auch regelmäßig und fortlaufend tun.

Ein Benutzer, der sich mit einem anderen Benutzer synchronisiert hilft gemeinsames Transaktionswissen aufzubauen und die Transaktionen anderer Nutzer zu verbreiten. Gleichzeitig schützt er sich vor Double-Spending-Attacken durch das Wissen über andere, für ihn bisher unbekannte Transaktionen.

Gemeinsames Transaktionswissen kann auch die Größe einer Transaktionsdatei erheblich verringern, da ein Benutzer A einem Benutzer B für die Transaktion nötige proof-of-trusts im besten Fall nicht mehr mitsenden muss.

Ein Benutzer und dessen Kontostand lassen sich umso glaubwürdiger bestätigen umso mehr Benutzer von diesem Benutzer und die ihn betreffenden Transaktionen wissen. Denn je mehr Benutzer von einer Transaktion Kenntnis haben und diese Bestätigen desto endgültiger ist diese Transaktion. Ein Benutzer, der eine Transaktion getätigt hat und diese im Nachhinein aus seiner Historie löscht kann nicht verhindern, dass sich das Wissen über diese Transaktion trotzdem rasant verbreitet. Des Weiteren hat der attackierende Benutzer keinen Einfluss mehr darauf wie schnell sich das Wissen über die Transaktion verbreitet. Im besten Fall wurde der nächste Transaktionspartner durch die Synchronisation bzw. Empfang einer Zahlung eines früheren Geschäftspartners/Freund bereits über die letzte Transaktion in Kenntnis gesetzt, sodass der attackierende Benutzer sie nicht abstreiten kann.

Abseits der Synchronisation mit UCAs/Benutzern sind in diesem Zusammenhang auch **Sync-as-a-Service-Modelle** denkbar bei denen Webseiten als Treffpunkt für sich synchronisieren wollende Benutzer agieren und gegen eine Anzahl an Coins die Funktion eines Notars übernehmen.

FAQ

Warum gibt es keine zentrale Blockchain?

Die im UCS verwendete Architektur setzt auf eine dezentrale Blockgitter-Struktur anstatt einer zentralen monolithischen Blockkette. Eine zentrale Blockchain ist nicht zwingend erforderlich um einen gemeinsamen Konsens zu bilden oder eine bestimmte Transaktion oder ein Konto zu überprüfen. Der proof-of-Trust (TSA-Dateien und Transaktionsdateien) ist genug. Als Folge kann ein Benutzer nur Transaktionen des Vertrauensnetzwerks bestätigen in dem er sich befindet. Nur mit diesen Vertrauensnetzwerk verbundene Netzwerke und Teilnehmer sind für den Benutzer sichtbar. Es ist nicht wie bei Bitcoin wo man Aufgrund der monolithischen Blockchain die ganze Transaktionshistorie aller Nutzer einsehen kann. Natürlich werden sich die sich bildenden Vertrauensnetze durch Handel und Synchronisation vergrößern und verbinden. Dadurch bildet sich im Laufe der Zeit einen mehr oder weniger zentrales Transaktionswissen, aber das Grundkonzept ist dezentral. Das Konzept ist vergleichbar mit dem von Nano. Die Blockchain eines Benutzers besteht im Grunde aus allen gesendeten und empfangenen Transaktionen, welche im Rahmen eines *distributed Ledger*-Konzeptes verwaltet werden.

Welche TSAs werden unterstützt?

Aktuell wird als TSA lediglich *FreeTSA* unterstützt. Konzepte für weitere TSAs werden aktuell diskutiert

ANMERKUNG: Es wurde bereits diskutiert, die Auswahl der TSAs auf OpenTimestamp zu erweitern oder den Benutzern die Möglichkeit zu geben selbst TSAs zu definieren. Ersteres würde jedoch bedeuten, dass man den Client von OpenTimestamp einbinden müsste, welcher wiederum auf die Blockchain von Bitcoin zugreift, was entweder eine weitere Abhängigkeit zu einem online-Dienst mit sich bringt oder die Notwendigkeit den Client samt Bitcoin Client Lokal zu installieren. Die Möglichkeit selbst TSAs zu definieren würde es Benutzern ermöglichen kompromittierte TSAs zu verwenden. Beides keine guten Lösungen!

Was ist der Proof-of-trust Algorithmus?

Der proof-of-trust Algorithmus stellt sicher, dass alles korrekt ist und keine Benutzer betrügen können. Ein Vertrauensnachweis besteht aus dem öffentlichen Schlüssel, welcher von der TSA beglaubigt wurde (und eventuell von weiteren Nutzern) inklusive aller ein- und ausgehenden Transaktionen eines Benutzers und seinen Kontakten. Das ist genug, um den aktuellen Saldo eines Kontos zu bestimmen und/oder um festzustellen ob eine Transaktion gültig ist oder nicht.

Was ist der Proof-of-trust?

Ein proof-of-trust (Vertrauensnachweis) setzt sich immer aus mehreren Dateien zusammen. Der Proof-of-trust eines Benutzers besteht mindestens aus:

- Public Key des Benutzers im /keys-Verzeichnis

optional: Public keys weiterer Benutzer, wenn Transaktionen abhängig sind

- freeTSA query file (*.tsq) und response file (*.tsr) des Public Keys im /proofs-Verzeichnis

optional: Query und Response anderer Public keys, wenn Transaktionen abhängig sind

- Transaktionen des Benutzers im /trx-Verzeichnis

optional: Transaktionen anderer Benutzer, falls Transaktionen abhängig sind

- Index-Datei für jeden Benutzer im /proofs-Verzeichnis

Enthält eine Liste aller Plausibler Transaktionen und wird zur Ermittlung der Confirmations verwendet

Mit Hilfe dieser Dateien ist es möglich ein Guthaben und damit verbundenen Transaktionen jederzeit zu überprüfen.

Was passiert, wenn ein Benutzer eine Transaktion manuell aus seiner Geschichte entfernt - kann er die gleiche Menge wieder ausgeben?

Wenn man sich an alle Regeln gehalten hat: Nein! Wenn ein Benutzer eine Transaktion an einen anderen Benutzer sendet, wird der Empfänger diese Transaktion in Zukunft verbreiten. Wenn der sendende Benutzer einfach eine Transaktion aus seiner Historie entfernen würde, würden die Benutzer, welche bereits Kenntnis von der Transaktion haben, sie in Zukunft trotzdem verbreiten. Wie schnell dies geschieht, darauf hat der ursprüngliche Sender keinen Einfluss mehr, lediglich der Empfänger. Eine zeitnahe Synchronisation mit anderen Teilnehmern verringert das Risiko einer solchen Attacke erheblich da ein Teilnehmer logischerweise keine Transaktion vorenthalten kann von der andere Benutzer bereits Kenntnis haben.

Warum universal credit system?

Es sind keine energieintensiven Berechnungen erforderlich, um Credit Coins zu erhalten. Credit Coins werden an alle Entitäten vergeben, denen es gelungen ist, ein Konto zu erstellen. Es ist unabhängig von einer zentralen Behörde, einem Staat oder einem Land. Es ist unabhängig vom Ort an dem es verwendet wird. Niemand kann es verbieten, niemand kann es schließen und niemand kann den Konsens ändern. Es kann einerseits als monetäres Medium fungieren und andererseits für Spekulationen eingesetzt werden. Der künstliche Mangel an Credits bietet potenziellen Nutzern einen Anreiz, so schnell wie möglich teilzunehmen und schließt gleichzeitig die spät hinzugekommenen Teilnehmer nicht aus. Es ist eine Art demokratische Währung, da jeder den gleichen Betrag erhält und niemand bevorzugt oder benachteiligt wird. Es gibt keine Tendenzen der Zentralisierung im Hinblick auf die Geldschöpfung wie bei den schon bestehenden Kryptowährungen. Jemand mit viel Geld bekommt die gleiche Anzahl Credits wie jemand mit wenig Geld. Es ist ein neuer Anfang von Grund auf und jeder Benutzer startet mit dem Kontostand 0 und den gleichen Chancen. Es ist ein universeller Währungsstandard, der auf Mathematik und dezentralem Vertrauen basiert. Es ist transparent, wo es für die Nachvollziehbarkeit und zur Erzielung des Konsens erforderlich ist, aber gleichzeitig müssen Teilnehmer außerhalb des etablierten Vertrauensnetzwerks nicht über Transaktionen usw.

informiert werden. Dies macht es wenig Anfällig für Betrug und insgesamt viel attraktiver als bereits bestehende Kryptowährungen.