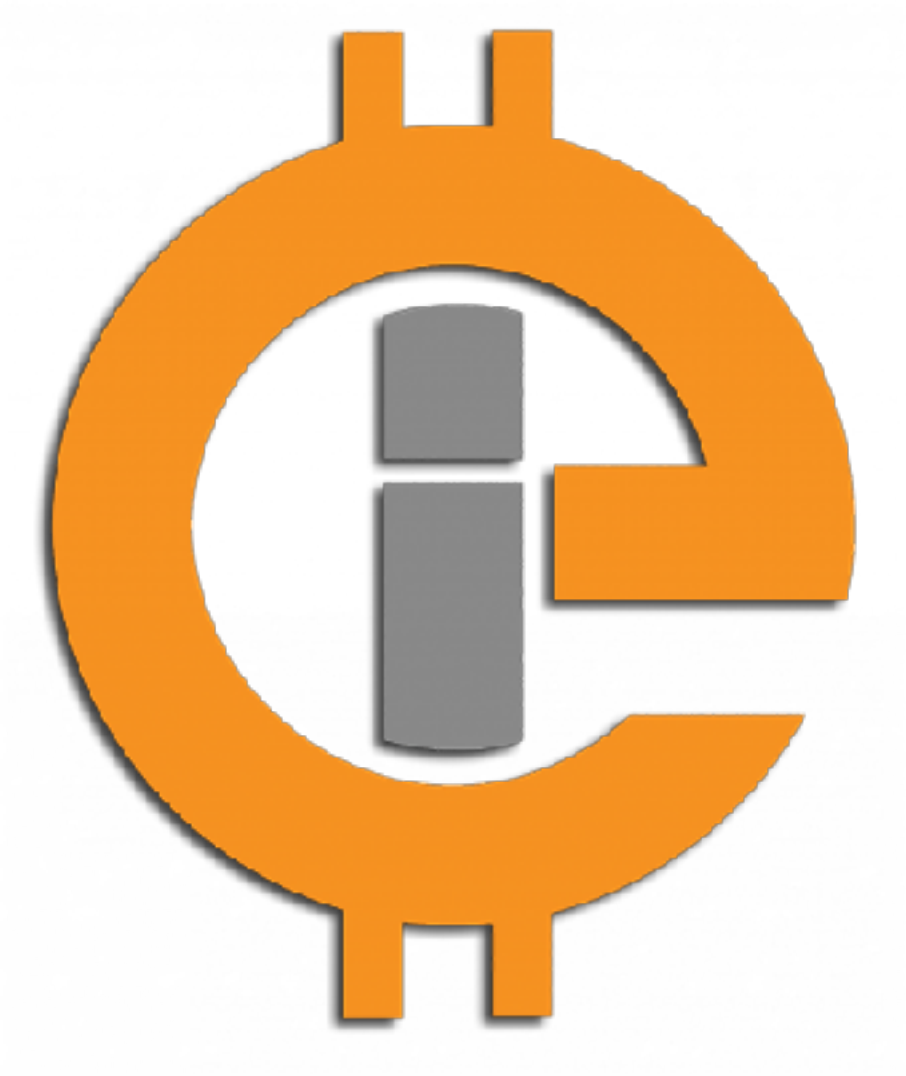

! Wichtig
für Übersetzung kann keine gewähr gegeben werden, maßgebend ist das original Whitepaper in englisch!
Zu finden auf der Seite von Infinity Economics:

http://www.infinity-economics.org/docs/infinity_whitepaper.txt

Erstellt von T.H am 08.10.2017

INFINITY ECONOMICS PLATTFORM (IEP) WHITEPAPER

Erstellt von der IEP Community

FINAL ENTWURF - UNTER PEER REVIEW

v.0.2 - 3. Oktober 2017

www.infinity-economics.org

Inhaltsverzeichnis

1. Zusammenfassung

3. Januar 2009 markierte den Beginn einer neuen Ära der Globalisierung und der Weltvernetzung, als die erste Bitcoin-Transaktion durchgeführt wurde. Satoshi Nakamoto [1] machte möglich, was man einmal für unmöglich hielt - ein Währungs- und Zahlungssystem, das nicht von einer Person oder Organisation kontrolliert wurde. Wir kennen diese Währung als Bitcoin und die zugrundeliegende Technologie, die es als Blockchain versorgt. Es ist schon 8 Jahre her, seit die Leute mit Bitcoin begonnen haben, aber erst jetzt beginnen wir, das echte Potenzial der Blockchain-Technologie zu verstehen, auf der Bitcoin gegründet ist. Blockchain tut den ökonomischen Prozessen, was das Internet mit Informationen gemacht hat: Heute kann jeder Zugang zu der Weltwirtschaft zu gleichen Bedingungen mit anderen haben. In diesem Dokument sprechen wir über IEP, eine Mehrzweck-Blockchain-Plattform für Benutzer.

1.1 Was ist eine Blockkette?

Eine Blockkette ist eine verteilte Datenbank, die die Erstellung eines digitalen Ledgers von Transaktionen und die gemeinsame Nutzung des Ledgers unter einem verteilten Netzwerk von Computern ermöglicht. Es nutzt fortgeschrittene Kryptographie, um jedem Teilnehmer im Netzwerk zu ermöglichen, mit dem Ledger auf eine sichere Weise zu interagieren, ohne die Notwendigkeit einer zentralen Autorität. Es behält eine ständig wachsende Liste von Datensätzen (Blöcke), die jeweils einen Zeitstempel und eine Verknüpfung zum vorherigen Block enthalten.

1.2 Zusammenfassung

Krypto-Währungen, Münzen, Digitale Münzen und andere digitale Assets auf der Basis von Blockchain-Technologie sind ein Mega-Trend, der direkt die Finanzen von Milliarden von Menschen rund um den Globus über eine finanzielle Autobahn direkt. Die finanzielle superhighway bringt Milliarden von Einzelpersonen über Grenzen hinweg, um direkt Produkte und Dienstleistungen untereinander überall über das Internet zu handeln. Mit Hilfe von Blockchain-Technologien werden der Wert solcher Finanzprodukte und -dienste - und die Transaktionen selbst - in einem System gespeichert, das nicht durch Politik, Überversorgung oder Dritten verdünnt werden kann. Die Verwendung von Blockchain wird die Zukunft der finanziellen Interaktionen erheblich beeinträchtigen, das traditionelle Modell eines zentralisierten Finanzsystems zu vermitteln - wo Einzelpersonen auf gebuchte Zahlen auf einem zentralisierten Computer reagieren - für die extrem große Anzahl komplexer Transaktionen, die täglich auf der Finanzautobahn durchgeführt werden, unzureichend ist. IEP ist eine benutzer- und

serviceorientierte Mehrzweck-Blockchain-Plattform und eine Krypto-Währung, die auf bewährten Krypto-Open-Source-Projekten basiert. IEP fungiert als Krypto-Tech-Integrator und kombiniert und ergänzt bestehende und neue Krypto-Tech-Features und -Dienstleistungen zu einer einzigen leistungsstarken Plattform für die digitale Wirtschaft.

1,3 TF; LR

IEP ist das finanzielle Ökosystem. Sein Hauptziel ist es, Kryptokurrenzen in die traditionelle Finanzwelt zu integrieren und ein einziges Tor zum Markt für normale Benutzer, Händler, Investoren und Finanzinstitute zu schaffen, indem sie einen neuen Full-Service und ein grenzenloses dezentrales Finanz-Ökosystem und eine digitale Wirtschaft aufbauen. In der Anfangsphase zielt IEP primär auf gemeinschaftsbasierte und humanitäre Entwicklung und Projekte. Zu diesem Zweck werden dezentralisierte Abstimmungen und Messaging implementiert, um eine DAO-ähnliche Erfahrung (Hybrid Governance) bei der Verwaltung von Community-Projekten zu ermöglichen, während sie aus technischer Sicht einfach bleiben.

1.4 Schlüsselwörter

cryptocurrency, blockchain, XIN, IEP, intelligente Verträge, dezentrale Dienstleistungen,
Asset Exchange, Währungen, Escrow, Blöcke, Knoten, Erweiterungen, Proxies.

2. Einleitung

Seit ihrer Gründung ist die Blockchain-Technologie mit Kontroversen über ihre natürliche Anwendung - Wert-Transfer mit einem Netzwerk-Token. Dezentrales Geld ist eine bahnbrechende Entwicklung, aber Blockchain-Technologie kann nicht allein darauf reduziert werden. Im Wesentlichen eine verteilte Datenbank, die Blockkette ermöglicht verschiedene Arten von verteilten Ledger-Einträgen, deren Art von ihrer Interpretation durch die Benutzer der Blockkette abhängt. IEP ist ein innovatives, sicheres, dezentrales und kostengünstiges Transaktionskosten-System, das mit modernsten Kryptoeffiziententechnologien entwickelt wurde, um ganze digitale Volkswirtschaften mit traditionellen Finanzdienstleistungen zu schaffen.

2.1 Mission und Ziele

IEPs Mission ist es, den erschreckenden Krypto-Markt für alle zugänglich zu machen, die Beschleunigung der Blockchain-Technologie und die Demokratisierung des Eigentums an Kryptokurrenzen zu beschleunigen. IEP macht Kryptokurrenzen leichter zu erwerben und zu übertragen, so dass die durchschnittliche Person an der New Economy teilnehmen kann. Die IEP-Stiftung glaubt an die philosophische Mission von Satoshi

Nakamoto. Durch die Schaffung einer sicheren Schicht, die für die durchschnittliche Person zugänglich ist, setzen sie die Macht in die Hände der Menschen - wo es hingehört.

2.2 Aktuelle Herausforderungen im Markt

Der zukünftige Erfolg der Kryptokurrenzen beruht auf ihrem weitverbreiteten Einsatz. Während Krypto sicherlich das Potenzial hat, als globale Zahlungsmethode zu steigen, bleibt es das Opfer von Spekulationen. Derzeit sind die meisten Benutzer behandeln Kryptokurrenzen als spekulative Vermögenswerte anstatt sie im täglichen Leben zu verwenden. Angesichts des exponentiellen Wachstums des Sektors und der Art und Weise, wie die Blockchain-Technologie zunehmend Mainstream wird, sind viele optimistisch, dass digitale Währungen mehr als Währung und weniger als spekulativer Vermögenswert verwendet werden. Obwohl in den vergangenen Jahren mehrere neue Blockchain-Technologien und Kryptokurrenzen entstanden sind, hat noch niemand den Durchbruch erreicht, der für die Mainstream-Adoption erforderlich ist - vor allem aufgrund von negativen Publikationen, Blasenspekulationen, Betrug und komplizierten User-Interfaces. Hacking und andere Cyberattacken an Krypto-Börsen,

2.3 Adressierte Probleme

Cryptocurrency ist ein dezentrales Blockchainbasiertes Finanzsystem mit Unveränderlichkeit und Autonomie, das seine gefeiertesten Features ist. Kryptokurrenzen ermöglichen es, Intermediäre zu umgehen und unabhängig von traditionellen Finanzinstituten zu bleiben. Allerdings hat keine Krypto-Währung, einschließlich Bitcoin, es geschafft, ein häufig verwendetes monetäres Vermögen zu werden. Händler und Dienstleister zögern, Krypto-Währungszahlungen zu akzeptieren, da es sich um zusätzliche Risiken von Wechselkursverlusten und regulatorischen Fragen sowie hoher Volatilität handelt. Ein Instrument, das in der Lage ist, ein perfektes globales Zahlungssystem zu werden, wird häufig als spekulativer Vermögenswert verwendet. Dieses Projekt wird als Lösung für das jeweilige Grundproblem konzipiert und berücksichtigt die Probleme und Herausforderungen des aktuellen globalen Finanzsystems.

3. Technologie

IEP ist eine 100% ige Proof-of-Stake Cryptocurrency [11], konstruiert aus bewährten Open-Source-Projekten [3] in Java geschrieben. Der einheitliche Proof-of-Stake-Algorithmus von IEP hängt nicht von der Implementierung des "Münzalter" -Konzepts ab, das von anderen Proof-of-Stake-Kryptokurrenzen verwendet wird, und ist resistent gegen so genannte "nichts auf dem Spiel" Angriffe. Eine Gesamtmenge von 9 Milliarden vorhandenen Token wurde im Geneseblock verteilt. Curve25519 [8] Kryptographie wird verwendet,

um ein Gleichgewicht der Sicherheit und erforderliche Rechenleistung, zusammen mit häufiger verwendeten SHA256 Hash-Algorithmen [13].

3.1 Technischer Hintergrund

Blöcke werden alle 60 Sekunden generiert, im Durchschnitt durch Konten, die freigeschaltet sind
auf Netzwerkknoten. Da die vollständige Token-Versorgung bereits vorhanden ist, wird IEP durch die Einbeziehung von Transaktionsgebühren neu verteilt, die auf ein Konto vergeben werden, wenn es erfolgreich einen Block erstellt. Dieser Vorgang wird als Schmieden bekannt und verwandt mit dem "Bergbau" - Konzept, das von anderen Kryptokurrenzen angewendet wird. Transaktionen werden nach 10 Block-Bestätigungen als sicher betrachtet, und die aktuelle Architektur- und Blockgrößen-Kappe von IEP ermöglicht die Verarbeitung von bis zu 367.200 Transaktionen pro Tag mit unbegrenztem Skalierbarkeitspotential. IEP-Transaktionen basieren auf einer Reihe von Kerntransaktionsarten, die keine Skriptverarbeitung oder Transaktions-Eingabe / Ausgabe-Verarbeitung auf Seiten von Netzwerkknoten erfordern.

3.2 Nachweis des Einsatzes (POS)

IEP nutzt ein System, bei dem jeder "Token" in einem Konto als winziges Bergbau-Rigg gedacht werden kann [11]. Je mehr Token, die auf dem Konto gehalten werden, desto größer ist die Chance, dass das Konto das Recht erhält, einen Block zu erzeugen. Die Gesamtzahl der "Belohnung", die als Ergebnis der Blockgenerierung erhalten wurde, ist die Summe der Transaktionsgebühren, die sich innerhalb des Blocks befinden. IEP erzeugt keine neuen Token als Ergebnis der Blockerstellung. Die Umverteilung von IEP erfolgt als Folge von Blockgeneratoren, die Transaktionsgebühren erhalten, so dass der Begriff "Schmieden" (dh in diesem Kontext "eine Beziehung oder neue Bedingungen" zu schaffen) anstelle von "Bergbau" verwendet wird verifizierbare, eindeutige und fast unvorhersehbare Informationen aus dem vorangehenden Block. Die Blöcke sind durch diese Verbindungen verknüpft, eine Kette von Blöcken (und Transaktionen) zu schaffen, die bis hin zum Geneseblock zurückverfolgt werden können. Die Blockgenerierungszeit ist auf 60 Sekunden gezielt, aber Variationen der Wahrscheinlichkeiten haben zu einer durchschnittlichen Blockgenerierungszeit von 80 Sekunden geführt, mit gelegentlich längeren Blockintervallen. Die Sicherheit der Blockkette ist immer besorgniserregend im Beweis von Stake-Systemen. Die folgenden Grundprinzipien gelten für IEP Proof of Stake Algorithmus:

- In jedem Block wird ein kumulativer Schwierigkeitswert als Parameter gespeichert und jeder nachfolgende Block leitet seine neue "Schwierigkeit" aus dem vorherigen Block ab Wert. Im Falle

von Mehrdeutigkeit erreicht das Netzwerk einen Konsens durch Auswahl das Block- oder Kettenfragment mit der höchsten kumulativen Schwierigkeit.

- Um zu verhindern, dass die Kontoinhaber ihren Anteil von einem Konto an bewegen ein anderes als Mittel zur Manipulation ihrer Wahrscheinlichkeit der Blockgenerierung, Token müssen in einem Konto für 1.440 Blöcke stationär sein, bevor sie kann zum Blockgenerierungsprozess beitragen. Token, die das treffen Kriterium trägt zu einem effektiven Gleichgewicht des Kontos bei, und dieses Gleichgewicht ist verwendet, um die Schmiedewahrscheinlichkeit zu bestimmen.

- Um einen Angreifer davon abzuhalten, eine neue Kette aus dem Genese-Block, das Netzwerk erlaubt nur Ketten-Re-Organisation 720 Blöcke hinter der aktuellen Blockhöhe. Jeder Block, der in einer niedrigeren Höhe eingereicht wurde als diese Schwelle abgelehnt wird. Diese Bewegungsschwelle kann als betrachtet werden IEP nur fester Checkpoint.

- Aufgrund der extrem geringen Wahrscheinlichkeit eines Kontos, das die Kontrolle über die blockchain durch die Erzeugung einer eigenen Kette von Blöcken, Transaktionen werden als erachtet sicher, wenn sie in einen Block codiert sind, der 10 Blöcke hinter dem Strom ist Blockhöhe

3.3 Token

Die Gesamtversorgung beträgt 9 Milliarden Token, die auf acht Dezimalstellen teilbar sind. Alle Token wurden mit der Erstellung des Genese-Blocks (der erste Block in der IEP-Blockkette) ausgegeben, wobei das Genesis-Konto [C] mit einem anfänglichen negativen Bilanz von 9 Milliarden Token verbleibt. Die Existenz von Anti-Token in der Genese-Konto hat ein paar interessante Nebenwirkungen:

- das Genese-Konto kann keine Transaktionen jeglicher Art ausgeben, da sein Gleichgewicht ist negativ und es kann keine Transaktionsgebühren bezahlen.

- irgendwelche Token, die an das Genese-Konto geschickt werden, werden effektiv zerstört Konto negatives Gleichgewicht wird sie auslöschen.

Die Wahl des Wortes Token ist beabsichtigt wegen der Absicht von IEP, verwendet zu werden als Basisprotokoll, das zahlreiche weitere Funktionen bietet. IEP ist am einfachsten Funktion ist eine von einem traditionellen Zahlungssystem, aber es wurde entworfen, um weit mehr zu tun.

3.4 Knoten

Ein Knoten auf dem IEP-Netzwerk ist ein beliebiges Gerät, das Transaktionen durchführt oder Daten in das Netzwerk blockiert. Jedes Gerät, das die IEP-Software ausführt, wird als Knoten angezeigt. Die Knoten können in zwei Typen unterteilt werden: markiert und normal. Ein markierter Knoten ist einfach ein Knoten, der mit einem verschlüsselten Token versehen ist, das aus dem privaten Schlüssel eines Kontos abgeleitet ist. Dieses Token kann decodiert werden, um eine bestimmte Token-Account-Adresse und Balance anzuzeigen, die mit einem Knoten verknüpft sind. Der Akt der Platzierung eines Markenzeichens auf einem Knoten fügt ein Maß an Rechenschaftspflicht und Vertrauen hinzu, so dass markierte Knoten mehr vertrauenswürdiger als nicht-markierte Knoten im Netzwerk sind. Je größer die Balance eines Kontos an einen markierten Knoten gebunden ist, desto mehr Vertrauen wird diesem Knoten gegeben. Während ein Angreifer vielleicht einen Knoten markieren möchte, um Vertrauenswürdigkeit im Netzwerk zu gewinnen und dann dieses Vertrauen für böswillige Zwecke zu nutzen; die Eintrittsbarriere (Kosten für das Token, die erforderlich sind, um ein angemessenes Vertrauen aufzubauen), entmutigt diesen Missbrauch. Jeder Knoten im IEP-Netzwerk hat die Möglichkeit, sowohl Transaktionen zu verarbeiten als auch zu übertragen und Informationen zu sperren. Blöcke werden validiert, wenn sie von anderen Knoten [I] empfangen werden, und in Fällen, in denen die Blockvalidierung fehlschlägt, können die Knoten vorübergehend "aufgelistet" werden, um die Ausbreitung von ungültigen Blockdaten zu verhindern. Jeder Knoten verfügt über integrierte DDOS-Verteidigungsmechanismen (Distributed Denial of Services), die die Anzahl der Netzwerkanforderungen von jedem Peer auf 30 pro Sekunde beschränken. und in Fällen, in denen die Blockvalidierung fehlschlägt, können die Knoten vorübergehend "aufgelistet" werden, um die Ausbreitung von ungültigen Blockdaten zu verhindern. Jeder Knoten verfügt über integrierte DDOS-Verteidigungsmechanismen (Distributed Denial of Services), die die Anzahl der Netzwerkanforderungen von jedem Peer auf 30 pro Sekunde beschränken. und in Fällen, in denen die Blockvalidierung fehlschlägt, können die Knoten vorübergehend "aufgelistet" werden, um die Ausbreitung von ungültigen Blockdaten zu verhindern. Jeder Knoten verfügt über integrierte DDOS-Verteidigungsmechanismen (Distributed Denial of Services), die die Anzahl der Netzwerkanforderungen von jedem Peer auf 30 pro Sekunde beschränken.

3.5 Blöcke

Wie in anderen Kryptokurrenzen wird das Ledger von Token-Transaktionen gebaut und in einer verknüpften Reihe von Blöcken gespeichert, die als Blockkette bekannt sind. Dieses Ledger bietet eine permanente Aufzeichnung der Transaktionen, die stattgefunden

haben, und stellt auch die Reihenfolge fest, in der Transaktionen aufgetreten sind. Eine Kopie der Blockkette bleibt erhalten

jeder Knoten im IEP-Netzwerk und jedes Konto, das auf einem Knoten freigeschaltet ist (durch die Bereitstellung des privaten Schlüssels des Kontos), hat die Möglichkeit, Blöcke zu erzeugen, solange mindestens eine eingehende Transaktion auf das Konto 1440 mal bestätigt wurde. Jedes Konto, das diese Kriterien erfüllt, wird als aktives Konto bezeichnet. In IEP enthält jeder Block bis zu 255 Transaktionen, die alle von einem 192-Byte-Header vorangestellt sind, der identifizierende Parameter enthält. Jede Transaktion in einem Block wird durch maximal 160 Bytes dargestellt und die maximale Blockgröße beträgt 32 KB. Alle Bausteine enthalten folgende Parameter:

- Eine Blockversion, Blockhöhenwert und Blockkennung
- Ein Block-Zeitstempel, ausgedrückt in Sekunden seit dem Genese-Block
- Die ID des Kontos, das den Block erzeugt hat, sowie das Konto Öffentlicher Schlüssel
- Die ID und das Hash des vorherigen Blocks. Die Anzahl der gespeicherten Transaktionen im Block
- Der Gesamtbetrag des Tokens, der durch Transaktionen und Gebühren im Block dargestellt wird
- Transaktionsdaten für alle im Block enthaltenen Transaktionen, einschließlich deren Transaktions-IDs
- Die Nutzlastlänge des Bausteins und der Hash-Wert der Baustein-Nutzlast

3.6 Bausteinerstellung

Drei Werte sind der Schlüssel, um festzustellen, welches Konto berechtigt ist, einen Block zu generieren, wobei das Konto das Recht hat, einen Block zu erzeugen, und welcher Block in autoritativer Weise als maßgebend eingestuft wird: Basiszielwert, Zielwert und kumulative Schwierigkeiten.

Basis-Zielwert

Um das Recht zu gewinnen, einen Block zu erstellen (generieren), alle aktiven IEP-Konten 'konkurrieren' durch den Versuch, einen Hash-Wert zu erzeugen, der niedriger als ein gegebener ist Basis-Zielwert. Dieser Basiszielwert variiert von Block zu Block und ist abgeleitet aus dem Basis-Zielwert des vorherigen Blocks.

Zielwert

Jedes Konto berechnet seinen eigenen Zielwert, basierend auf seinem aktuellen effektiven
Anteil. Dieser Wert ist: $T = Tb \times S \times Be$

woher:

T ist der neue Zielwert
Tb ist der Basiszielwert
S ist die Zeit seit dem letzten Block, in Sekunden
Be ist die effektive Bilanz des Kontos

Wie aus der Formel ersichtlich ist, wächst der Zielwert mit jeder Sekunde Pässe seit dem Zeitstempel des vorherigen Blocks. Der maximale Zielwert ist 0.17080318 x 10e17 und der minimale Zielwert ist die Hälfte des vorherigen Block-Basis-Zielwert. Dieser Zielwert und der Basiszielwert sind der Gleiches für alle Konten, die versuchen, oben auf einen bestimmten Block zu schmieden. Der einzige kontospezifische Parameter ist der effektive Balance-Parameter.

Kumulative Schwierigkeit
Der kumulative Schwierigkeitswert ergibt sich aus dem Basis-Zielwert, mit der Formel: Dcb = Dpb + 264 / Tb
woher:

Dcb ist die Schwierigkeit des aktuellen Blocks
Dpb ist die Schwierigkeit des vorherigen Blocks
Tb ist der Basiszielwert für den aktuellen Block [j]

Der Schmiede-Algorithmus

Jeder Block auf der Kette hat einen Generierungs-Parameter. Um an dem Block-Forging-Prozess teilzunehmen, unterschreibt ein aktives Konto die Generierungssignatur des vorherigen Blocks mit einem eigenen öffentlichen Schlüssel kryptografisch. Dies erzeugt eine 64-Byte-Signatur, die dann mit SHA256 gehasht wird. Die ersten 8 Bytes des resultierenden Hashs geben eine Zahl an, die als der Treffer des Kontos bezeichnet wird. Der Treffer wird mit dem aktuellen Zielwert verglichen. Wenn der berechnete Treffer niedriger als das Ziel ist, kann der nächste Block erzeugt werden. Wie in der Zielwertformel angemerkt, steigt der Zielwert mit jeder vorangehenden Sekunde an. Auch wenn es nur wenige aktive Konten im Netzwerk gibt, wird einer von ihnen schließlich einen Block generieren, da der Zielwert sehr groß wird. Die Korollar von diesem

ist, dass Sie die Zeit abschätzen können, die für ein Konto erforderlich ist, um einen Block zu fälschen, indem er den Wert des Kontos auf den Zielwert vergleicht. Wenn ein
Das aktive Konto gewinnt das Recht, einen Block zu erzeugen, bündelt bis zu 255 verfügbare, unbestätigte Transaktionen in einen neuen Block und füllt den Block mit all seinen erforderlichen Parametern. Dieser Block wird dann als Kandidat für die Blockkette an das Netzwerk übertragen. Der Nutzdatenwert, die Erzeugung des Kontos und alle Signaturen auf jedem Block können von allen Netzwerkknoten überprüft werden, die ihn empfangen. In einer

Situation, in der mehrere Blöcke erzeugt werden, werden die Knoten den Block mit dem höchsten kumulativen Schwierigkeitswert als den maßgeblichen Block auswählen. Da Blockdaten zwischen Peers geteilt werden, werden Gabeln (nicht autorisierende Kettenfragmente) detektiert und demontiert, indem die in jeder Gabel gespeicherten kumulativen Schwierigkeitswerte der Ketten untersucht werden.

3.7 Konten

IEP implementiert eine Hirnbörse als Teil seines Designs: alle Konten werden gespeichert das Netzwerk mit privaten Schlüsseln für jede mögliche Kontoadresse, die direkt aus der Passphrase jedes Kontos mit einer Kombination von SHA256- und Curve25519-Operationen abgeleitet wird. Jedes Konto wird durch eine 64-Bit-Zahl dargestellt, und diese Zahl wird als Kontoadresse unter Verwendung einer Reed-Solomon [k] Fehlerkorrektur-Notation ausgedrückt, die die Erkennung von bis zu vier Fehlern in einer Kontoadresse oder eine Korrektur von oben ermöglicht zu zwei fehler Dieses Format wurde in Erwiderung auf Bedenken umgesetzt, dass eine falsche Kontoadresse dazu führen könnte, dass Token, Aliase oder Vermögenswerte irreversibel auf fehlerhafte Zielkonten übertragen werden. Kontoadressen werden immer von "XIN-" vorangestellt, so dass Token-Account-Adressen leicht erkennbar und von Adressformaten unterscheidbar sind, die von anderen Kryptokurren verwendet werden.

1. Die geheime Passphrase ist mit SHA256 gehasht, um das Konto abzuleiten

Privat Schlüssel.

2. Der private Schlüssel wird mit Curve25519 verschlüsselt, um das Konto abzuleiten

Öffentlicher Schlüssel.

3. Der öffentliche Schlüssel wird mit SHA256 gehasht, um die Konto-ID abzuleiten.

4. Die ersten 64 Bits der Konto-ID sind die sichtbare Kontonummer.

5. Reed-Solomon-Codierung der sichtbaren Kontonummer, vorangestellt

"XIN-", erzeugt die Kontoadresse.

Wenn ein Konto zum ersten Mal durch eine geheime Passphrase zugegriffen wird, ist es nicht durch einen öffentlichen Schlüssel gesichert. Wenn die erste ausgehende Transaktion von einem Konto gemacht wird, wird der aus der Passphrase abgeleitete 256-Bit-Public-Key auf der Blockkette gespeichert und sichert das Konto.

Der Adressraum für öffentliche Schlüssel (2256) ist größer als der Adressraum für Kontonummern (264), so dass keine Eins-zu-Eins-Abbildung von Passphrasen auf Kontonummern und Kollisionen möglich ist. Diese Kollisionen werden auf folgende Weise erkannt und verhindert: Sobald eine bestimmte Passphrase für den Zugriff auf ein Konto verwendet wird und dieses Konto durch einen 256-Bit-öffentlichen Schlüssel gesichert ist, darf kein anderes öffentlich-privates Schlüsselpaar auf diese Kontonummer zugreifen.

Kontoausgleichseigenschaften

Für jedes IEP-Konto stehen verschiedene Arten von Salden zur Verfügung. Jeder Typ dient einem anderen Zweck, und viele dieser Werte werden als Teil der Transaktionsvalidierung und -verarbeitung überprüft.

- Der effektive Kontostand wird als Grundlage für ein Konto verwendet forging Berechnungen [L]. Die effektive Bilanz eines Kontos besteht aus allen Token die in diesem Konto für 1440 Blöcke stationär gewesen sind. In Ergänzung, Die Account Leasing-Funktion ermöglicht eine effektive Balance des Kontos einem anderen Konto für einen vorübergehenden Zeitraum zugewiesen.

- Der garantierte Kontostand eines Kontos besteht aus allen Spielmarken stationär in einem Konto für 1440 Blöcke. Anders als das effektive Gleichgewicht, das Balance kann keinem anderen Konto zugeordnet werden.

- Der Grundsaldo eines Kontos stellt alle Transaktionen dar hatte mindestens eine Bestätigung.

- Der geschmiedete Kontostand eines Kontos zeigt die Gesamtmenge des Tokens an wurden durch erfolgreiches Blockieren von Blöcken verdient.

- Der unbestätigte Saldo eines Kontos ist derjenige, der im IEP angezeigt wird Klienten. Es repräsentiert den aktuelle Kontostand eines Kontos, abzüglich der Token an unbestätigten, geschickten Transaktionen beteiligt.

- Garantierte Vermögensguthaben listet die garantierten Salden aller Vermögenswerte auf mit einem bestimmten Konto verbunden.

- Unbestätigte Vermögensguthaben listet die unbestätigten Guthaben aller Vermögenswerte auf mit einem bestimmten Konto verbunden.

3.8 Transaktionen

Transaktionen sind die einzigen Mittel, die IEP-Konten haben, ihren Zustand zu verändern oder

Balance. Jede Transaktion führt nur eine Funktion aus, deren Aufzeichnung
dauerhaft im Netzwerk gespeichert, sobald diese Transaktion aufgenommen wurde
Ein Block.

Transaktions Gebühren

Transaktionsgebühren sind der primäre Mechanismus, durch den Token zurück in das Netzwerk zurückgeführt werden. Jede Transaktion erfordert eine Mindestgebühr von 1 Token, während mehrere Dienste wie Aliase, Vermögenswerte oder Stimmabgaben höhere Gebühren erfordern. Wenn ein IEP-Konto einen Baustein schmiedet, werden alle in diesem Block enthaltenen Transaktionsgebühren dem Schmiedekonto als Belohnung verliehen. Bis die Größe aller Transaktionen in einem Block die aktuelle 32 Kilobyte Blockgrösse überschreitet, reicht die Mindestgebühr aus, damit alle Transaktionen in Blöcken enthalten sind. In Situationen, in denen die Anzahl der unbestätigten Transaktionen die Zahl überschreitet, die in einem Block platziert werden kann, werden die Konten automatisch Transaktionen mit den höchsten Gebühren auswählen. Dies deutet darauf hin, dass die Transaktionsverarbeitung durch eine Gebühr, die höher als das Minimum ist, priorisiert werden kann.

Transaktionsbestätigungen

Alle IEP-Transaktionen gelten als unbestätigt, bis sie in einem gültigen Netzwerkblock enthalten sind. Neu erstellte Blöcke werden durch den Knoten (und das zugehörige Konto), die sie erzeugt, an das Netzwerk verteilt, und eine Transaktion, die in einem Block enthalten ist, gilt als eine Bestätigung erhalten. Da nachfolgende Blöcke der vorhandenen Blockkette hinzugefügt werden, fügt jeder zusätzliche Block eine weitere Bestätigung der Anzahl der Bestätigungen für eine Transaktion hinzu. Wenn eine Transaktion vor Ablauf ihrer Frist nicht in einen Baustein einbezogen wird, läuft sie ab und wird aus dem Transaktionspool entfernt.

Transaktionstermine

Jede Transaktion enthält einen Deadline-Parameter, der auf eine Anzahl von Minuten ab dem Zeitpunkt eingestellt ist, zu dem die Transaktion an das Netzwerk übermittelt wird. Die Frist beträgt 1440 Minuten (24 Stunden). Eine Transaktion, die an das Netzwerk gesendet wurde, aber nicht in einen Baustein aufgenommen wurde, wird als unbestätigte Transaktion bezeichnet. Wenn eine Transaktion nicht in einen Satz aufgenommen wurde, bevor die Transaktionsfrist abgelaufen ist, wird die Transaktion aus dem Netzwerk entfernt. Transaktionen können unbestätigt bleiben, weil sie ungültig oder fehlerhaft sind oder weil Blöcke gefüllt werden, Transaktionen, die angeboten haben, höhere Transaktionsgebühren zu zahlen. In Zukunft können Funktionen wie Multi-Signatur-Transaktionen in der Lage sein, die Fristen als Mittel zur Durchsetzung eines Verfalldatums zu nutzen.

Vorgangsarten

Die Kategorisierung von IEP-Transaktionen in Typen und Subtypen ermöglicht das modulare Wachstum und die Entwicklung des IEP-Protokolls, ohne Abhängigkeiten von anderen "Basis" -Funktionen zu erzeugen. Da dem IEP-Kern Funktionen hinzugefügt werden, können neue Transaktionsarten und Subtypen hinzugefügt werden, um sie zu unterstützen. Während der Integration werden weitere Transaktionsarten wie Abonnements, Escrow und automatisierte Transaktionen hinzugefügt, die als erweiterte Transaktionen bezeichnet werden.

Transaktionserstellung und -verarbeitung
Die Einzelheiten der Erstellung und Verarbeitung einer IEP-Transaktion sind wie folgt:

1. Der Absender gibt die Parameter für die Transaktion an. Arten von Transaktionen variieren, und der gewünschte Typ wird bei der Transaktionserstellung angegeben, aber mehrere Parameter müssen für alle Transaktionen angegeben werden:

   - der private Schlüssel für das sendende Konto
   - eine angegebene Gebühr für die Transaktion
   - eine Frist für die Transaktion
   - eine optionale referenzierte Transaktion

2. Alle Werte für die Transaktionseingänge werden geprüft. Zum Beispiel obligatorisch Parameter müssen angegeben werden Gebühren können nicht kleiner oder gleich Null sein; ein Transaktionsfrist kann nicht weniger als eine Minute in die Zukunft sein; wenn ein referenzierte Transaktion angegeben ist, dann kann die aktuelle Transaktion nicht sein verarbeitet, bis die referenzierte Transaktion verarbeitet wurde.

3. Werden infolge der Parameterüberprüfung keine Ausnahmen ausgelöst:

(a) Der öffentliche Schlüssel für das generierende Konto wird mit dem lieferte geheime Passphrase

(b) Kontoinformationen für das generierende Konto werden abgerufen und Transaktionsparameter werden weiter validiert:
- Der Saldo des Sendekontos darf nicht null sein
- Die unbestätigte Saldo des sendenden Kontos darf nicht niedriger sein als der Transaktionsbetrag plus die Transaktionsgebühr

4. Wenn das sendende Konto über ausreichende Mittel für die Transaktion verfügt:

(a) Eine neue Transaktion wird erstellt, wobei ein Typ- und Subtyp-Wert auf gesetzt ist passen die Art der Transaktion gemacht

werden. Alle angegebenen Parameter sind inklusive. Mit der Erstellung wird eine eindeutige Transaktions-ID erzeugt des Gegenstandes

(b) Die Transaktion wird mit dem privaten Schlüssel des sendenden Kontos unterzeichnet

(c) Die verschlüsselten Transaktionsdaten werden innerhalb einer Meldung angezeigt, Netzwerke, um die Transaktion zu verarbeiten

(d) Die Transaktion wird an alle Peers im Netzwerk übertragen
(e) Der Server antwortet mit einem Ergebniscode:
- die Transaktions-ID, wenn die Transaktionserstellung erfolgreich war
- ein Fehlercode und eine Fehlermeldung, wenn eine der Parameterprüfungen fehlschlägt.

3.9 kryptographisch

Einführung

Elliptische Kurve Kryptographie (ECC) [8] ist eine Public-Key-Kryptographie-Methode, die elliptische Kurven algebraische Strukturen über endliche Felder verwendet. ECC bietet Sicherheit mit kleineren Schlüsseln als andere kryptographische Methoden. ECC kann für die Schlüsselvereinbarung, digitale Signaturen, Pseudozufallsgeneratoren usw. verwendet werden. ECC kann für die indirekte Verschlüsselung verwendet werden, indem ein symmetrisches Verschlüsselungsschema mit der Schlüsselvereinbarung verwendet wird.

Der Schlüsselaustausch in IEP basiert auf dem Curve25519-Algorithmus, der einen geteilten geheimen Schlüssel mit einer schnellen, effizienten, hochsicheren Elliptikkurve Diffie-Hellman-Funktion [7] erzeugt. Der Algorithmus wurde erstmals von Daniel J. Bernstein im Jahr 2006 gezeigt [8]. IEPs Message Signing in IEP wird mit dem Elliptic-Curve Korean Certificate basierten Digital Signature Algorithm (EC-KCDSA) implementiert, der im Jahr 1998 von der KCDSA Task Force-Team als Teil von IEEE P1363a bezeichnet wurde. [9]. Beide Algorithmen wurden für ihr Gleichgewicht von Geschwindigkeit und Sicherheit für eine Schlüsselgröße von nur 32 Bytes gewählt.

Verschlüsselungsalgorithmus

Wenn Alice einen verschlüsselten Klartext an Bob sendet, ist sie:
1. Berechnet ein gemeinsames Geheimnis:
   - shared_secret = Curve25519 (Alice_private_key,Bob_public_key)

2. Berechnet N Samen:
   - seedn = SHA256 (seedn-1), wobei seed0 = SHA256 (shared_secret)

3. Berechnet N Schlüssel:
   - keyn = SHA256 (Inv (seedn)), wobei Inv (X) die Inversion aller Bits ist von X

4. Verschlüsselt den Klartext:
   - ciphertext [n] = plaintext [n] XOR keyn

Nach dem Empfang beendet Bob den Chiffretext:

1. Berechnet ein gemeinsames Geheimnis:
   - shared_secret = Curve25519 (Bob_private_key,Alice_public_key)

2. Berechnet N Samen (dies ist identisch mit Alices Schritt):
   - seedn = SHA256 (seedn-1), wobei seed0 = SHA256 (shared_secret)

3. Berechnet N Tasten (dies ist identisch mit Alices Schritt):
   - keyn = SHA256 (Inv (seedn)), wobei Inv (X) die Inversion aller Bits ist von X

4. Entschlüsselt den Chiffretext:
   - plaintext [n] = ciphertext [n] XOR keyn

Anmerkung: Wenn jemand einen Teil des Klartextes errät, kann er einen Teil davon entschlüsseln
Folgende Nachrichten zwischen Alice und Bob, wenn sie die gleichen Schlüsselpaare verwenden.
Infolgedessen wird empfohlen, für jedes ein neues Paar privater / öffentlicher Schlüssel zu erzeugen
Kommunikation.

3.10 Architektur

Krypto-Klassen der ersten Generation wurden in erster Linie als Zahlungssysteme konzipiert. IEP erkennt an, dass dezentrale Blockchains eine breite Palette von Anwendungen und Diensten ermöglichen können, aber nicht präskriptiv ist, was diese Dienste sein sollen oder wie sie gebaut werden sollen. Durch Design entfaltet IEP unnötige Komplexität in seinem Kern, so dass nur die erfolgreichsten Komponenten seiner Vorgänger intakt sind. Als Ergebnis fungiert IEP-Funktionen wie ein Low-Level-Fundament-Protokoll: Es definiert die Schnittstellen und Operationen, die erforderlich sind, um eine leichte Blockkette, ein dezentrales Kommunikationssystem und ein schnelles Transaktionsverarbeitungs-Framework zu betreiben, so dass Komponenten höherer Ordnung auf diesen Merkmalen aufbauen können . Transaktionen in IEP machen einfache Anpassungen an Kontostände, anstatt Sätze von "Input" oder "Output" Credits zu verfolgen. In Ergänzung, Die Core-Software unterstützt keine Form von Skriptsprache. Durch die Bereitstellung eines Satzes von grundlegenden, flexiblen

Transaktionsarten, die schnell und einfach verarbeitet werden können, erstellt IEP eine Grundlage, die nicht die Art und Weise beschränkt, in der diese Transaktionstypen verwendet werden können, und erzeugt keinen signifikanten Overhead für deren Verwendung. Diese Flexibilität wird durch den geringen Ressourcen- und Energiebedarf von IEP weiter verstärkt und sein hochlesbarer, hoch organisierter objektorientierter Quellcode.

3.11 Werkzeugketten

IEP konzentriert sich auf Industriestandards für alle Plattformentwicklungen. Der Kern ist in unternehmensfreundlichen Java [D] geschrieben, die Backends werden von NodeJS [E] angetrieben und alle Frontends sind mit AngularJS [F] aufgebaut, so dass es einfach ist, Entwicklerressourcen jederzeit und überall zuzuordnen. Cross-Plattform-Apps werden mit Elektronen [G] aufgebaut. Der Standard-Backend-Speicher ist MongoDB [H]. Diese Toolchain gibt dem Fundament viel mehr Freiheit, die besten Entwickler / Auftragnehmer für alle anstehenden Programmieraufgaben zu wählen, da die Entwicklergemeinschaften für diese Werkzeuge gereift und groß sind mit vielen bewährten Komponenten annd Frameworks, gebrauchsfertig.

3.12 Integration

Die Kryptospace entwickelt sich sehr schnell. Neue Technologien und leistungsstarke Protokolle und Komponenten werden täglich entwickelt. Um dieses devstream zu beherrschen, überwacht IEP die gesamte Krypto-Entwicklung aufmerksam für zusätzliche Features, die es wert ist, die IEP-Plattform entweder für den Kern oder für die Dienste hinzuzufügen. Neue Transaktionsarten können hinzugefügt werden, um den Kern mit leistungsstarken Features zu erweitern. Auf diese Weise fungiert IEP als Krypto-Feature-Integrator, um immer den Stand der Technik Bausteine für die digitale Wirtschaft zu bieten. Alle neuen Features werden der Community zur Abstimmung und Akzeptanz vor der Umsetzung vorgestellt.

4. Eigenschaften

IEP ist darauf ausgelegt, Bausteine für die digitale Wirtschaft zu integrieren und setzt daher stark auf sichere und robuste Off-Chain-Infrastrukturen, um den Durchschnittsbenutzer zu erreichen. Um dieses Ziel zu erreichen, ist der IEP-Kern und der Client für eine einfache Erweiterbarkeit [14] und eine Verbindung zu anderen, sehr nützlichen Protokollen und Netzwerken aufgebaut. IEP ist nicht dazu bestimmt, als die meisten Kryptos zu handeln, als eine Insel, sondern um alle neuen Technologien zu umarmen und zu begrüßen, von sehr klassisch bis zu den modernsten. Die meisten

Die Dienste basieren auf den erweiterten Core-Implementierungen von IEP wie Proxies und Gateways. Dienste können öffentlich oder privat sein, als UI-weniger Bots oder sogar als Erweiterungen innerhalb der Brieftasche UI laufen. Die Dienstleistungen spielen in der zukünftigen Entwicklungs- und Wachstumsstrategie von IEP eine sehr wichtige Rolle, weshalb die Stiftung die Verbesserung dieser Dienste erleichtert und auch gemeinschaftsrelevante Dienste wie die erweiterten verschlüsselten Nachrichten- / Chat- oder Nachrichtendienste mit externen Auftragnehmern initiiert oder sogar entwickelt. Die Liste der realisierten / geplanten Dienstleistungen wächst stetig. Bitte beachten Sie die Brieftaschen-Erweiterungen, um einen Überblick über bereits umgesetzte und geplante Leistungen zu erhalten.

4.1 Zahlungen

Token (XIN) sind für den Benutzer am relevantesten. Eine Übertragungsvorgangsart wird verwendet, um Token von einem Konto zu einem anderen zu übertragen. Eine kleine verschlüsselte Nachricht kann jeder Transaktion für eine zusätzliche Gebühr beigefügt werden. Die Gebühr für einen einfachen Transfer ist 1 Token. Token Transfers sind einfach und schnell und kostengünstig und meist innerhalb von nur 60 Sekunden abgewickelt. Anonyme Transfers sind mit der eingebauten Münz-Shuffling-Funktion möglich.

4.2 Aliase

Die IEP-Alias-System-Funktion erlaubt im Wesentlichen, dass ein Text für ein anderes ersetzt wird, so dass Schlüsselwörter oder Keyphrasen verwendet werden können, um andere Dinge zu repräsentieren - Namen, Telefonnummern, physikalische Adressen, Webseiten, Kontonummern, E-Mail-Adressen, Produkt-SKU-Codes und mehr. Sofortige Anwendungen sind einfach: Sie können zum Beispiel einen einfach zu merkenden Alias für Ihr IEP-Konto erstellen. Da das Alias-System jedoch offen ist, kann es verwendet werden, um ein dezentrales DNS-System, Einkaufswagen, Proxies in andere Blockchains, Orakel, Verweise auf gespeicherte Dateien in bittorrent oder IPFS [6] oder sogar als Einstieg in dezentrales Webhosting wie ZeroNet [2]. Aliase können mit dem eingebauten Alias-Marktplatz bearbeitet, übertragen oder an öffentliche oder spezifische Konten verkauft werden.

4.3 Meldungen

Verschlüsselte Nachrichten nehmen gewöhnlich die Form der SMS-Länge Kommunikation zwischen den Benutzern. Übertragung von verschlüsselten Datennachrichten bis zu 160 Bytes Länge von jedem Konto zu einem anderen Konto als einzelne Nachricht. Verschlüsselte Nachrichten können auch an viele Transaktionen wie Token Transfer, Asset Transfer, Währungsübertragung angehängt

werden. Verschlüsselte Nachrichten werden dauerhaft in der Blockkette gespeichert und in der Größe begrenzt, um Blockchain Bloat zu verhindern. Verschlüsselte Nachrichten benötigen eine dynamische Gebühr, basierend auf ihrer Größe und sollte für wichtige und unveränderliche Nachrichten verwendet werden. Der Verschlüsselungsalgo ist AES. Der kommende, gemeindebasierte Messenger-Service ermöglicht bis zu 1.000 Bytes und letzten 1.000 Nachrichten ohne Servicegebühr. Meldungen können auch verwendet werden, um Transaktionsereignisse zum Beispiel zu Kettenzahlungen auszulösen oder verteilte Dienste aufzurufen.

4.4 Vermögenswerte

Die Asset Exchange ist IEPs integrierte dezentrale Handelsmaschine. Mit dem Asset Exchange können Sie Vermögenswerte erstellen, kaufen und verkaufen, die Daten über einfache Münztransfers hinausgeben, die weitreichende Möglichkeiten eröffnen. Die Asset Exchange basiert auf dem "farbigen Münzen" - Konzept, wobei eine Münze oder ein Satz von Münzen bezeichnet werden kann ("farbig"), um etwas zu vertreten. Im Gegensatz dazu sind viele Krypto-Währungen nur immer so einfach - Währungen und nichts mehr. Da jedoch die Blockkette eine vertrauenswürdige und permanente Ledger aller Transaktionen bietet, kann sie verwendet werden, um viel vielfältigere Informationen aufzuzeichnen als reine Währungstransaktionen. IEP-Token können als "farbig" bezeichnet werden, um andere Kryptomünzen, Aktien / Anleihen, Eigentum, Rohstoffe oder sogar Ideen darzustellen. Als Ergebnis, Das IEP-Netzwerk kann verwendet werden, um fast alles zu handeln. Die Asset Exchange eignet sich für die meisten Anwendungsfälle, in denen Benutzer gerne virtuelle Unternehmensaktien, Fiat-pegged Assets, Lohnpunkte oder sogar Krypto-Backed Asssets kaufen, aber nicht für den HFT-Handel, da die Asset Exchange dezentralisiert ist und mit einem 60er Jahre läuft. Blockzeitbestätigung. Der Asset Exchange ist vollständig dezentral und völlig unreguliert. Die erheblichen Vorteile dieser Angebote sind Freiheit, Kosteneinsparungen, Mangel an Intervention und so weiter, sondern kommt auch zu einem Preis. Es gibt keine Hand-Holding oder Polizei, und Betrug Vermögenswerte können und oft erstellt werden. Während die Gemeinde in der Regel auf diese relativ schnell aufnimmt, wenn man einen Fehler macht, dann gibt es sehr wenig Rückgriff, da Transaktionen irreversibel sind. Vor dem Kauf eines Vermögenswertes,

4.5 Währungen

Die Währungseinheit ist der Grundbaustein des IEP-Währungssystems. Eine Währung hat einen eindeutigen Namen und Code und Einzigartigkeit wird durch das Protokoll garantiert, Währungen können gelöscht werden und ihr Code kann unter bestimmten Bedingungen wiederverwendet werden. Die gesamte Währungsversorgung ist in Währungseinheiten unterteilbar. Wie Vermögenswerte,

Währungseinheiten unterstützt Dezimalstellen als Client-Side-Feature implementiert. Die maximale Anzahl der Währungseinheiten, die pro Währung ausgegeben werden können, ist ähnlich dem Zeichen 10 ^ 9 * 10 ^ 8. Die tatsächliche maximale Versorgungseinheit wird vom Währungsaussteller festgelegt. Der Währungsaussteller ist das Konto, das die Währung ausgibt und die Emissionsgebühr bezahlt. Der Emittent ist verantwortlich für die Festlegung der Währungseigenschaften und in einigen Konfigurationen hat eine zusätzliche Kontrolle über die Währungsnutzung. Wie Vermögensguthaben können Währungseinheiten zwischen Konten übertragen werden.

4.6 Crowdfunding

Crowdfunding ist die Praxis der Finanzierung eines Projektes oder Venture durch die Erhöhung der monetären Beiträge von einer großen Anzahl von Menschen. Crowdfunding ist eine Form von Crowdsourcing und alternativen Finanzen. Crowdfunding basiert in der Regel auf drei Arten von Akteuren: dem Projektinitiator, der die Idee und / oder das Projekt vorschlägt, Einzelpersonen oder Gruppen, die die Idee unterstützen, und eine moderate Organisation (die "Plattform"), die die Parteien zusammen bringt die Idee. Im Jahr 2013 wurden $ 5,1 Mrd. USD von Millionen von Einzelpersonen angehoben! Allerdings ist die größte Anreiz für die Nutzung von Websites wie Kickstarter ihre Gebühren. Kickstarter verlangt 5% des Geldes, das als Gebühr erhoben wird, und Zahlungsabwicklungsgebühren sind weitere 5%, was im Zeitalter der Blockchain-Technologie ein wenig schwer zu rechtfertigen ist. Basierend auf dem eingebauten Währungsmerkmal bietet IEP diese "Plattform" als vollautomatische dezentrale Lösung für einfaches, schnelles und erschwingliches Crowdfunding an. Crowdfunding wurde verwendet, um eine breite Palette von gewinnorientierten unternehmerischen Ventures wie künstlerische und kreative Projekte, medizinische Kosten, Reisen oder gemeindeorientierte soziale unternehmerische und wohltätige und humanitäre Projekte zu finanzieren.

4.7 Escrow

Ein Escrow-Service ermöglicht eine sicherere Zahlung durch sicheres Halten eines Käufers Münzen in Escrow, bis die Bedingungen des Verkaufs erfüllt sind und als Ergebnis der Käufer veröffentlicht Zahlung an den Verkäufer. In den meisten Fällen wird kein Streit eingereicht und es ist keine Drittanbieteraktion erforderlich. IEP bietet einen dezentralisierten Escrow-Service auf Basis der neuen erweiterten Transaktionsarten. Wenn Sie verkaufen Ihr Auto oder Haus mit IEP dezentralisierten Asset-Service können Sie ganz einfach die Mittel in Escrow und wenn der Titel in Ihrem Namen geliefert wird, geben Sie das Geld. Sogar der Titel kann mit einem IEP Smart Contract geliefert werden und bekomme dies, es kostet weniger als ein paar Pennies, um all dies

geschehen und im Gegensatz zu traditionellen Banken und Verkauf von Transaktionen kostet es nicht Hunderte oder Tausende von Dollar.

4.8 Abonnements

Verwalten und Skalieren Abonnements waren komplex. Bis jetzt. IEP bietet dezentralisierte wiederkehrende Zahlungen an, die Benutzer jederzeit einleiten und abbrechen können. Wiederkehrende Zahlungen funktionieren gut für Dienstleistungen, die mehrere Zahlungen im Laufe der Zeit erfordern oder nur um spezielle Konten zu finanzieren, um eine minimale Ausgleichshöhe zu gewährleisten. Abonnements basieren auf dem neuen erweiterten Transaktions-Framework und ermöglichen es Benutzern, Zahlungen von beliebiger Größe und Intervall auf andere Konten zu leisten. Abonnements sind ein wichtiges neues Feature für den kommenden digitalen Marktplatz.

4.9 Mischen

CoinShuffle [5] verbessert die Benutzer Privatsphäre durch frustrierende Versuche, Transaktionen mit einem bestimmten Benutzer zu verknüpfen. Ein Teilnehmer kann seine Anonymität erhöhen, indem er es unmöglich macht, genau zu bestimmen, wer bezahlt hat, weil Ein- und Ausgänge nicht zu unterscheiden sind (auch für andere Teilnehmer). Jeder Teilnehmer weiß, welche Ausgabe sie besitzen, aber die Eingänge und Ausgänge des anderen Teilnehmers können nicht verknüpft werden. CoinShuffle erlaubt auch die Identifizierung und Beseitigung von böswilligen Teilnehmern, die sich schlecht benommen haben. Coin Shuffling ist eine effektive Datenschutzerklärung und ermöglicht es den Teilnehmern, ihre Fonds schnell und effizient mit anderen Teilnehmern zu mischen, indem sie eine zufällige Zuordnung zwischen vorhandenen Teilnehmerkonten und neuen Empfängerkonten, die von den Benutzern zur Verfügung gestellt werden, erstellen. Der Shuffling-Algorithmus basiert auf einem Papier von Tim Ruffing [5] und wurde ursprünglich entwickelt, um in Bitcoin selbst implementiert zu werden. CoinShuffle unterscheidet sich von anderen bestehenden Lösungen wie ZeroCash [12] in Bezug auf Geschwindigkeit und Komplexität.

4.10 Abstimmung

Die Blockchain-Technologie eignet sich gut für die Wahl in Abstimmungssystemen. Durch die Bereitstellung eines sicheren Wegs für jede Person, um ihre Stimme auf eine öffentliche Aufzeichnung zu registrieren, während immer noch die Möglichkeit für die Benutzer anonym bleiben, und mit wenig Möglichkeit für jedermann, um diese Stimmen zu manipulieren, ist die Blockkette in der Lage, erhebliche Verbesserungen gegenüber aktuellen Systemen bieten in Bezug auf Sicherheit und Transparenz. Die sichere, verschlüsselte,

konsensbasierte Natur des IEP-Netzwerks ermöglicht die Umsetzung eines Abstimmungssystems, das Anonymität und Sicherheit garantiert, ohne sich auf eine zentrale Autorität zu konzentrieren. Das IEP Voting System ermöglicht es jedem Konto, eine Umfrage mit einer Frage und bis zu 10 Antworten zu erstellen. Konten sind berechtigt, in der Umfrage zu stimmen, die auf einem Mindestbedarf aus Token, einem Vermögenswert oder einer Währung basiert. Die Abstimmung besteht darin, einen Integer-Bereichswert auszuwählen, der mit einer oder mehreren Antworten verknüpft ist, wie sie bei der Umfrage erstellt wurden. Eine Antwort wird auf der Grundlage eines von vier Abstimmungsmodellen gegeben und dann wird ihr Gewicht mit dem zugehörigen Bereichswert multipliziert, um ein entsprechendes Ergebnis zu berechnen. Die vier stimmberechtigten Modelle geben das Gewicht als: eine pro Stimmkonto oder gleich dem Saldo pro Stimmkonto des Tokens, eines Vermögenswerts oder einer Währung an. Ein Gesamtgewicht für jede Antwort wird als Summe aller individuellen Abstimmungsgewichte berechnet; Ebenso wird ein Gesamtergebnis berechnet. Einzelne Stimmen werden bis mindestens 1441 Blöcke gespeichert, nachdem die Umfrage abgeschlossen ist, in der Regel mehr als einen Tag. Nach dieser Zeit werden die Stimmen gelöscht und nur die Gesamtgewichte und Ergebnisse bleiben verfügbar. Eine Antwort wird auf der Grundlage eines von vier Abstimmungsmodellen gegeben und dann wird ihr Gewicht mit dem zugehörigen Bereichswert multipliziert, um ein entsprechendes Ergebnis zu berechnen. Die vier stimmberechtigten Modelle geben das Gewicht als: eine pro Stimmkonto oder gleich dem Saldo pro Stimmkonto des Tokens, eines Vermögenswerts oder einer Währung an. Ein Gesamtgewicht für jede Antwort wird als Summe aller individuellen Abstimmungsgewichte berechnet; Ebenso wird ein Gesamtergebnis berechnet. Einzelne Stimmen werden bis mindestens 1441 Blöcke gespeichert, nachdem die Umfrage abgeschlossen ist, in der Regel mehr als einen Tag. Nach dieser Zeit werden die Stimmen gelöscht und nur die Gesamtgewichte und Ergebnisse bleiben verfügbar. Eine Antwort wird auf der Grundlage eines von vier Abstimmungsmodellen gegeben und dann wird ihr Gewicht mit dem zugehörigen Bereichswert multipliziert, um ein entsprechendes Ergebnis zu berechnen. Die vier stimmberechtigten Modelle geben das Gewicht als: eine pro Stimmkonto oder gleich dem Saldo pro Stimmkonto des Tokens, eines Vermögenswerts oder einer Währung an. Ein Gesamtgewicht für jede Antwort wird als Summe aller individuellen Abstimmungsgewichte berechnet; Ebenso wird ein Gesamtergebnis berechnet. Einzelne Stimmen werden bis mindestens 1441 Blöcke gespeichert, nachdem die Umfrage abgeschlossen ist, in der Regel mehr als einen Tag. Nach dieser Zeit werden die Stimmen gelöscht und nur die Gesamtgewichte und Ergebnisse bleiben verfügbar. oder gleich dem Saldo pro Stimmkonto von Token, einem Vermögenswert oder einer Währung. Ein Gesamtgewicht für jede Antwort wird als Summe aller individuellen Abstimmungsgewichte berechnet; Ebenso wird ein Gesamtergebnis berechnet. Einzelne Stimmen werden bis mindestens 1441 Blöcke gespeichert, nachdem die Umfrage abgeschlossen ist, in der Regel mehr als einen Tag. Nach dieser Zeit werden die Stimmen gelöscht und nur die Gesamtgewichte

und Ergebnisse bleiben verfügbar. oder gleich dem Saldo pro Stimmkonto von Token, einem Vermögenswert oder einer Währung. Ein Gesamtgewicht für jede Antwort wird als Summe aller individuellen Abstimmungsgewichte berechnet; Ebenso wird ein Gesamtergebnis berechnet. Einzelne Stimmen werden bis mindestens 1441 Blöcke gespeichert, nachdem die Umfrage abgeschlossen ist, in der Regel mehr als einen Tag. Nach dieser Zeit werden die Stimmen gelöscht und nur die Gesamtgewichte und Ergebnisse bleiben verfügbar.

4.11 Automatisierte Transaktionen

Eine der vielversprechendsten Anwendungen der Blockkettestechnik sind intelligente Verträge. Intelligente Verträge sind Computerprogramme, die die Vertragsbedingungen automatisch ausführen können. Jeder, der mit der Computerprogrammierung vertraut ist, würde sich dessen bewusst sein, was als if-then-else-Anweisung bekannt ist, wo ein Programm eine bestimmte Aufgabe ausführt, wenn bestimmte Bedingungen erfüllt sind und nicht, wenn die Bedingungen nicht vorhanden sind. Smart-Verträge implementieren dies auf der Blockkette und haben das Potenzial, dies in ein weiteres wachsendes Feld zu erweitern, und das ist das Internet der Dinge, die die Welt der Science-Fiction näher an die Realität bringen. Zum Beispiel ermöglichen Atomic Cross Chain Transactions einen wirklich dezentralisierten Handel zwischen Kryptokurrenzen. Dies kann zum Beispiel einem Händler erlauben, Token mit einer Münze auszutauschen, die einen Mischdienst für die Zwecke der Privatsphäre bietet, und schick es dann zu einer neuen Brieftasche. Ein weiteres klares Vertragsbeispiel, das IEP unterstützen könnte, sind Auktionen. IEP ermöglicht es Ihnen, einen intelligenten Auktionsvertrag zu erstellen. Die Teilnehmer an der Auktion würden dann Geld an den Vertrag schicken, und immer wenn jemand mehr Geld als der vorherige Bieter sendet, wird das Geld des vorherigen Bieters automatisch zurückerstattet. Zukünftige intelligente Verträge, die IEP zu unterstützen beabsichtigt, umfassen autonome Konzerne, Glücksspiel, Selbstmischung und intelligente Eigenschaften. Intelligente Verträge werden als die "Killer-App" der Krypto-Indoor-Industrie angepriesen, und das Rennen ist auf der Entwicklung von Anwendungen, die radikal verändern unsere Arbeit, Leben und Spiel in die Zukunft gehen. Die Teilnehmer an der Auktion würden dann Geld an den Vertrag schicken, und immer wenn jemand mehr Geld als der vorherige Bieter sendet, wird das Geld des vorherigen Bieters automatisch zurückerstattet. Zukünftige intelligente Verträge, die IEP zu unterstützen beabsichtigt, umfassen autonome Konzerne, Glücksspiel, Selbstmischung und intelligente Eigenschaften. Intelligente Verträge werden als die "Killer-App" der Krypto-Indoor-Industrie angepriesen, und das Rennen ist auf der Entwicklung von Anwendungen, die radikal verändern unsere Arbeit, Leben und Spiel in die Zukunft gehen. Die Teilnehmer an der Auktion würden dann Geld an den Vertrag schicken, und immer wenn jemand mehr Geld als der vorherige Bieter sendet, wird das Geld

des vorherigen Bieters automatisch zurückerstattet. Zukünftige intelligente Verträge, die IEP zu unterstützen beabsichtigt, umfassen autonome Konzerne, Glücksspiel, Selbstmischung und intelligente Eigenschaften. Intelligente Verträge werden als die "Killer-App" der Krypto-Indoor-Industrie angepriesen, und das Rennen ist auf der Entwicklung von Anwendungen, die radikal verändern unsere Arbeit, Leben und Spiel in die Zukunft gehen.

4.12 Gateways

Ein Anwendungs-Gateway ist ein Gerät (Knoten), das als "Gate" zwischen zwei Netzwerken fungiert. Heute sind Service-Entwickler vor vielen Problemen beim Bau von kundenspezifischen Dienstleistungen, verteilt auf eine riesige Anzahl von Kunden. Erstens müssen sie mehrere verschiedene Technologien beherrschen und durch Framework-spezifische APIs gehen. Zweitens werden Anwendungen, die für ein Framework entwickelt wurden, nicht in einem anderen Framework funktionieren und drittens müssen die gesammelten Daten und die von den Geräten bereitgestellten Aktionen dem Service-Modell zugeordnet werden. Die IQ-Applikations-Gateways bieten eine komfortable Lösung für Service-Entwickler, um auf mehrere Services und Protokolle zuzugreifen. Gateways sind ein wichtiger zukünftiger Entwicklungsteil für die IE-Plattform, um Dienste wie IPFS [6] (Interplanetary Filesystem) zu verbinden, die für dezentrale Speicherung verwendet werden, ZERONET [2], verwendet für dezentrales Hosting und Tendermint [4], verwendet für Side- und Private-Chains-Lösungen [10]. Da Gateways innerhalb von Core-Scope-Diensten laufen, können die Dienste direkt mit den IKE-Blockchain- und Transaktionsmodellen interagieren. Wenn ein Client-Programm eine Verbindung zu einem Zieldienst herstellt, verbindet es sich mit dem IEP-Anwendungs-Gateway. Der Kunde verhandelt dann mit dem Knoten, um mit dem Zieldienst zu kommunizieren. In der Tat stellt der Kunde die Verbindung zum Ziel her und handelt im Auftrag des Kunden. Aufgrund des transparenten API-Zugriffs, falls konfiguriert, sind Gateways innerhalb der IEP-Smart-Brieftasche erreichbar. Dies erweitert die Brieftasche-Funktion stark eingestellt. Gateways können für öffentliche oder private Dienste genutzt werden. Da Gateways innerhalb von Core-Scope-Diensten laufen, können die Dienste direkt mit den IKE-Blockchain- und Transaktionsmodellen interagieren. Wenn ein Client-Programm eine Verbindung zu einem Zieldienst herstellt, verbindet es sich mit dem IEP-Anwendungs-Gateway. Der Kunde verhandelt dann mit dem Knoten, um mit dem Zieldienst zu kommunizieren. In der Tat stellt der Kunde die Verbindung zum Ziel her und handelt im Auftrag des Kunden. Aufgrund des transparenten API-Zugriffs, falls konfiguriert, sind Gateways innerhalb der IEP-Smart-Brieftasche erreichbar. Dies erweitert die Brieftasche-Funktion stark eingestellt. Gateways können für öffentliche oder private Dienste genutzt werden. Da Gateways innerhalb von Core-Scope-Diensten laufen, können die Dienste direkt mit den IKE-Blockchain- und Transaktionsmodellen

interagieren. Wenn ein Client-Programm eine Verbindung zu einem Zieldienst herstellt, verbindet es sich mit dem IEP-Anwendungs-Gateway. Der Kunde verhandelt dann mit dem Knoten, um mit dem Zieldienst zu kommunizieren. In der Tat stellt der Kunde die Verbindung zum Ziel her und handelt im Auftrag des Kunden. Aufgrund des transparenten API-Zugriffs, falls konfiguriert, sind Gateways innerhalb der IEP-Smart-Brieftasche erreichbar. Dies erweitert die Brieftasche-Funktion stark eingestellt. Gateways können für öffentliche oder private Dienste genutzt werden. Der Kunde verhandelt dann mit dem Knoten, um mit dem Zieldienst zu kommunizieren. In der Tat stellt der Kunde die Verbindung zum Ziel her und handelt im Auftrag des Kunden. Aufgrund des transparenten API-Zugriffs, falls konfiguriert, sind Gateways innerhalb der IEP-Smart-Brieftasche erreichbar. Dies erweitert die Brieftasche-Funktion stark eingestellt. Gateways können für öffentliche oder private Dienste genutzt werden. Der Kunde verhandelt dann mit dem Knoten, um mit dem Zieldienst zu kommunizieren. In der Tat stellt der Kunde die Verbindung zum Ziel her und handelt im Auftrag des Kunden. Aufgrund des transparenten API-Zugriffs, falls konfiguriert, sind Gateways innerhalb der IEP-Smart-Brieftasche erreichbar. Dies erweitert die Brieftasche-Funktion stark eingestellt. Gateways können für öffentliche oder private Dienste genutzt werden.

4.13 Proxies

Ein Proxy-Server ist ein Server (ein Computersystem oder eine Anwendung), der als Vermittler für Anfragen von Clients fungiert, die Ressourcen von anderen Servern suchen. Ein Client verbindet sich mit dem Proxy-Server und fordert einen Dienst an, z. B. eine Datei, eine Verbindung, eine Webseite oder eine andere Ressource, die von einem anderen Server verfügbar ist, und der Proxy-Server wertet die Anforderung als eine Möglichkeit aus, ihre Komplexität zu vereinfachen und zu steuern. Proxies wurden erfunden, um Struktur und Kapselung zu verteilten Systemen hinzuzufügen. IEP bietet mehrere In-Core-Proxies, die problemlos erweitert und mit einfachen HTTP GET-Anfragen abgerufen werden können. Proxies spielen eine wichtige Rolle in der IEP-Interkonnektivitätsstrategie und ermöglichen es der IE-Plattform, zusätzliche Dienste und Funktionen zu erreichen, die im Kernbereich laufen.

Das Ausführen innerhalb des Core-Space ermöglicht es, Proxy-Daten mit dem IKE-Blockchain-, Transaktions- und Benachrichtigungssystem zu interagieren, so dass es einfach ist, öffentliche oder private Dienste zu erstellen. Wegen des transparenten API-Zugangs sind Proxies auch von IEPs Smart-Brieftasche erreichbar. Aktuelle Proxies werden verwendet, um Echtzeit-Daten aus dem Austausch und

Blockexplorern für den Cryptocurrency Markt zu holen, aber sie sind nicht auf diese und mehr Proxies beschränkt, die Verbindung zu gemeinsamen Datendiensten sind in der Entwicklung.

4.14 Erweiterungen

Erweiterungen ermöglichen es Drittanbietersoftwareentwicklern, dem IEP Smart Client Interface Funktionalität hinzuzufügen. Erweiterungen / Dienstleistungen sind ein wichtiger Teil für die IEP-Plattform, um Traktion in gemeinsamen Märkten zu erzielen, die direkt von der Smart-Brieftasche zugänglich sind. In den meisten Fällen basieren diese Erweiterungen auf Diensten, die von Entwicklern aufgebaut werden, um diese mit der IE-Plattform zu verbinden, zum Beispiel aufgrund von Zahlungslogik oder Dataservices. Da Plugins uneingeschränkten Zugriff einschließlich sensibler Daten und Funktionalität haben, ist es sehr wichtig, nur vertrauenswürdige Erweiterungen zu installieren. Wenn es irgendwelche Zweifel gibt, installieren Sie eine Erweiterung nur auf dem Testnetz oder auf dem Hauptnetz mit Konten mit kleinen Waagen. Erweiterungen werden von Drittanbietern verfasst und erhalten eine intensive Peer-Review vor der Veröffentlichung. Die Stiftung wird eine "Best Practice" vorbereiten

4.15 Kontokontrolle

Konto-Sicherheit ist möglicherweise das führende Problem mit der Verwendung von Krypto-Währung: Wie kann ein Benutzer sichere digitale Fonds, so dass sie völlig sicher vor Diebstahl, angesichts der zunehmenden Raffinesse von Malware und Hacking-Techniken. Die Kontosteuerung erhöht die Sicherheit der Konten und stellt sicher, dass nur bestimmte Personen unter bestimmten Bedingungen Zugang zu Fonds haben. Multisignature (multisig) bezieht sich beispielsweise auf die Erfordernis mehrerer Schlüssel, eine Transaktion zu autorisieren. Dies ermöglicht es Benutzern, Konten zu erstellen, die nur mit der Genehmigung von Inhabern bestimmter Vermögenswerte oder Währungen tätig werden können, oder um Transaktionen vorbehaltlich der Votes bei den Ausgaben zu tätigen. Multisignatur (oft als Multisig bezeichnet) ist eine Form der Technologie, die verwendet wird, um zusätzliche Sicherheit für Token-Transaktionen hinzuzufügen. Multisignatur erfordert zusätzliche Benutzer zu unterzeichnen (genehmigen) eine Transaktion, bevor es auf die Blockkette hinzugefügt werden kann. Phasing ist ein weiteres Merkmal, das es ermöglicht, bestimmte phasensichere Transaktionen mit bedingter aufgeschobener Ausführung auf der Grundlage des Abstimmungsergebnisses, einer Liste verknüpfter Transaktionen oder einer Offenbarung eines Geheimnisses zu erstellen; oder einfach mit bedingungsloser aufgeschobener Ausführung.

4.16 leichter Kunde

Der klassische Bitcoin-Ansatz ist im Wesentlichen eine Möglichkeit, ein verteiltes System über gemeinsame Transaktionsprotokolle zu synchronisieren. Es erfordert, dass jeder Netzwerkknoten die vollständige Kopie der Transaktionshistorie speichert. Offensichtlich ist das nicht gut skaliert, da letztlich nicht jeder Knoten die ganze Geschichte speichern kann. Es gibt verschiedene Möglichkeiten, dies zu mildern - eine vereinfachte Zahlungsüberprüfungsprozedur, die die Speicherung nur der für einen bestimmten Knoten wesentlichen Daten ermöglicht; Off-Kette-Transaktionen; bidirektionale Zahlungstunnel; Verringerung der Blockkette Blähungen; direkt mit dem Systemzustand arbeiten. Mit dem einfachsten Ansatz, bei dem alle Knoten im Genesis-Block gleich sind, kann die Zentralisierung entstehen, da sich niederwertige Knoten auf volle, hochkapazitive Knoten verlassen müssen, die es sich leisten können, die volle Blockkette zu speichern. Natürlich bringt die aufkommende Zentralisierung Vertrauensprobleme, da leichte Knoten den vollen Knoten vertrauen müssen und ein Opfer eines vollkommenen Knotens werden können. Allerdings gibt es Möglichkeiten, dies zu mildern, wie z. B. das Abrufen mehrerer Knoten, die Aufrechterhaltung vertrauenswürdiger Knotenlisten und so weiter. IEP bietet eine neue Struktur für diese Aufgaben, indem sie den Peerexplorer nutzt. Die Stiftung unterhält eine Basis von vertrauenswürdigen Hochleistungs-Servern, um ausreichende Knoten für Kunden zur Verfügung zu stellen. Ein Knoten-Rating-Algo wird verwendet, um die Top-Knoten zu ordnen, in der CPU-Last zu zählen, verfügbare Prozessoren und mehr Knoten-Metriken in Echtzeit, um die Client-Anforderungen für eine optimale Leistung zu belasten. IEP bietet eine neue Struktur für diese Aufgaben, indem sie den Peerexplorer nutzt. Die Stiftung unterhält eine Basis von vertrauenswürdigen Hochleistungs-Servern, um ausreichende Knoten für Kunden zur Verfügung zu stellen. Ein Knoten-Rating-Algo wird verwendet, um die Top-Knoten zu ordnen, in der CPU-Last zu zählen, verfügbare Prozessoren und mehr Knoten-Metriken in Echtzeit, um die Client-Anforderungen für eine optimale Leistung zu belasten. IEP bietet eine neue Struktur für diese Aufgaben, indem sie den Peerexplorer nutzt. Die Stiftung unterhält eine Basis von vertrauenswürdigen Hochleistungs-Servern, um ausreichende Knoten für Kunden zur Verfügung zu stellen. Ein Knoten-Rating-Algo wird verwendet, um die Top-Knoten zu ordnen, in der CPU-Last zu zählen, verfügbare Prozessoren und mehr Knoten-Metriken in Echtzeit, um die Client-Anforderungen für eine optimale Leistung zu belasten.

5. e-Governance

Von Anfang an ist IEP entworfen, um als ein 100% gemeinschaftsorientiertes Projekt zu laufen, was bedeutet, dass die Macht, über alle plattformbezogenen Angelegenheiten zu entscheiden, allen Mitgliedern der Gemeinschaft gehört, die auf ihrer Stimmrechte basieren. Dieser Ansatz kann als DAO durch seine Kerndefinition gesehen werden, da alles von Plattform zu Service-

Entwicklung dezentralisiert ist, von laufenden Knoten bis hin zu Marketing und Dokumentation. IEP folgt diesen Grundsätzen von Anfang an, indem er die Macht übergibt, sich an die Benutzer zu entscheiden, die einzige Möglichkeit, eine solide und faire Krypto-Plattform zu etablieren, um einzelne Punkte des Versagens zu verhindern. Eine IEP-Stiftung wurde geschaffen, um die Gemeinden auszuführen, egal was Wale, Vip oder Entwickler entscheiden. Um eine manipulationssichere Umgebung zu schaffen, werden die integrierten E-Governance-Funktionen verwendet und verwendet, um die IEP-Plattform zu verbessern. Zum Beispiel alle IEP-Features, bei denen für die Freigabe durch die Community vor der Freigabe gestimmt wurde.

5.1 DAO Übersicht

Dezentrale autonome Organisationen [1] wurden von einigen als schwer zu beschreiben gesehen. Dennoch ist das konzeptionelle Wesen einer dezentralisierten autonomen Organisation als die Fähigkeit der Blockchain-Technologie charakterisiert, ein sicheres digitales Ledger zu schaffen, das finanzielle Interaktionen über das Internet verfolgt, gegen Fälschung durch vertrauenswürdiges Zeitstempeln und durch Verbreitung einer verteilten Datenbank verhärtet wird. Dieser Ansatz beseitigt die Notwendigkeit, einen bilateralen akzeptierten und vertrauenswürdigen Dritten in eine Finanztransaktion einzubeziehen und damit die Sequenz zu vereinfachen. Die ursprüngliche Theorie, die dem DAO zugrunde lag, bestand darin, dass die DAO die Fähigkeit der Direktoren und Fondsmanager, die delegierten Befugnisse von den Direktoren zu entfernen und direkt in die Hände von Eigentümern zu bringen, Der erste bekannte DAO war / ist Bitcoin, aber es fehlen einige wichtige Funktionen, um das "optimale" DAO zu erfüllen. Einfach definiert, fehlt ein Mechanismus namens e-Governance als Ausdruck des Willens des Token-Inhabers.

5.2 Smart Contracts Lösungen

Der erste Code, der nur DAO basiert, wurde als Smart Contract gestartet und läuft auf der Ethereum Blockchain als Investor-Directed Capital Fund ohne konventionelle Managementstruktur oder Board of Directors. Die DAO wurde im Mai 2016 über einen Token-Verkauf crowdfundiert. Sie stellte den Rekord für die größte Crowdfunding-Kampagne in der Geschichte fest, doch im Juni 2016 nutzten Hacker eine Schwachstelle im DAO-Code, um ein Drittel der DAO-Fonds abzuschöpfen ein Nebenkonto Durch diesen Hack trat eine harte Gabel auf, wo die ursprüngliche, nicht gegabelte Blockkette als Ethereum Classic gepflegt wurde, wodurch Ethereum in zwei getrennte aktive Kryptokurrenzen gebrochen wurde. Unabhängig von der Hacke, auch diese Code-basierte DAO benötigt Akteure in der physischen Welt, genannt "Kuratoren",

5.3 IEP-Lösung

Lernen aus den oben genannten Problemen und Definitionen, IEP DAO kann als Hybrid-DAO angesehen werden. Durch die Verwendung einer viel flexibleren und fortschrittlicheren e-Governance-Plattform, und der endgültige menschliche Input, der von der Stiftung zur Verfügung gestellt wird, zählt auch. Im Vergleich zu Code-basierten nur DAOs hat IEP die folgenden Vorteile.

1. Flexibilität in der E-Governance

IEP DAO bietet eine umfangreiche Reihe von bereits integrierten Governance-Tools zugänglich und einfach zu bedienen aus der Box für den durchschnittlichen Benutzer. Diese Werkzeuge sind transparent, einfach einzurichten und auch leicht zu überwachen, ohne kompliziert zu sein Code-Konstrukte, die schwer zu testen und vorherzusagen sind.

2. Common Sense Aktiviert

Während ein Maximum an Automatisierung hat es Vorteile, es fehlt Flexibilität, und Du kannst den gesunden Menschenverstand nicht beherrschen. Die Stiftung ist zutiefst davon überzeugt, dass gemeinsame Sinn ist ein wichtiger Bestandteil, um Missbrauch zu verhindern und dynamisch zu handeln unvorhersehbare Probleme Wie oben erwähnt, eine endgültige menschliche Ansicht mit einem gesunden Teil des gesunden Menschenverstandes bereichert das DAO und macht es viel robuster. Der gesunde Menschenverstand ist die letzte Bastion, wenn etwas mit dem DAO schief geht.

3. Fine Granulation für Vorschlag Votings Code-basiert

Vorschlagswahlen sind nur auf Transaktionen / Zählungen (ja / nein) beschränkt. Das IEP eingebaute Wahlsystem hat viele Vorteile, da es mehrere unterstützt Entscheidungen und Mehrfachwahlmodelle. Das ergibt viel genauer Vorschlag Votings im Vergleich zu einfachen Ja / Nein-Lösungen. In vielen realen Welt Entscheidungen ein einfaches Ja / Nein ist nicht ausreichend.

4. Vollständige Transparenz

Vorschläge und Abstimmungen zu diesen Vorschlägen sind nicht in Schwierigkeiten eingekapselt Lesen Sie Verträge / Code. Dies ermöglicht es Nicht-Entwicklern zu überprüfen und zu überwachen Ganzer Vorschlag und Abstimmungsergebnis einfach durch Betrachten der Kette. Blockexplorer und die bereits in die Brieftasche eingebauten Werkzeuge sind ausreichend volle Transparenz.

5. Automatisierte Transaktionen

als zusätzliche DAO-Lösung Während die Stiftung die oben beschriebene DAO - Struktur bevorzugt, Plattform unterstützt Code-basierte DAO's auch. Die automatisierten Transaktionen (AT) Feature (Alpha Status) kann verwendet werden, um Smart Contracts auf der IEP-Blockkette Es ist frei für jeden Benutzer / Entwickler zu bauen seine eigenen privaten oder öffentliches DAO zu minimalen Kosten. Weitere Informationen finden Sie unter AT-Funktionen Aufbau eines DAO auf der IEP-Blockkette.

6. Schlussfolgerung

In dieser Arbeit stellen wir das Konzept einer Plattform für eine digitale Wirtschaft vor. Kryptokurrenzen verändern die Welt jetzt, lösen die Probleme des Vertrauens und der Sicherheit, vereinen Finanzinstitute, große Investoren, alltägliche Benutzer und Vertreter von kleinen, mittleren und großen Unternehmen zu einem einzigen globalen System. Die IEP dezentrale Krypto-Ledger-Plattform ist ein ehrgeiziges Projekt, das verschiedene Änderungen der Integration, der Client-Side-Features und der Middleware-System-Arrangements zusammenführt, um die Basis für Softwarelösungen zu bilden, die für Finanzanwendungen von heute und in die Zukunft geeignet sind. Auf der Grundlage dieses neuen Modells werden die Vermittler ihre eigenen Finanzdienstleistungen entwickeln und über IEP einen verteilten Superfinanzmarkt aufbauen. Wir glauben, dass eine flexible, dezentralisierte, Wert-Austausch-System ist die Zukunft der neuen globalen Finanzinfrastruktur und wird dazu beitragen, die finanzielle Integration zu fördern und zukünftige Finanztransaktionen zu standardisieren. Die Designphilosophie von IEP ist in vielerlei Hinsicht das Gegenteil von dem, was heute von vielen anderen Kryptokurren genommen wurde, die sich auf die Zusammenarbeit und die Integration der Inszenierung von Insellösungen stützen.

7. Quellen, zusätzliche Papiere, Referenzen und Werkzeuge

IEP möchte allen, die mit dieser Ermutigung und ihrem konsequenten Engagement beigetragen haben, aufrichtige Dankbarkeit aussprechen.

7.1 Zusätzliche Ressourcen

7.1.1 IEP Doc Abschnitt, http://www.infinity-economics.org/docs/
7.1.2 IEP API Abschnitt, http://www.infinity-economics.org/api
7.1.3 IEP Download Abschnitt, http://www.infinity-economics.org/download/
7.1.4 IEP Chain Tools, http://infinity-economics.org/preview/

7.2 Kredite und Anerkennung

7.2.1 Whitepapers: Nxt, Burst, Hitze, Fimk, NEM, Ethereum, Tendermint, IPFS

7.3 Ergänzungen

[A] Dies ist definiert als die aktuelle Bilanz des Kontos, abzüglich der Beträge
zu allen unbestätigten, gesendeten Transaktionen. Im Allgemeinen ist dies das Konto
Balance, die in Echtzeit in einer Client-Schnittstelle angezeigt wird.

[B] Nxt, Burst, FIMK, NEM, IPFS, ZeroNet, Tendermint

[C] Die Entstehungskontoadresse ist XIN-NTLK-Z5GA-WNAV-GW378

[D] Java SE Runtime Umwelt
http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-
2133155.html

[E] Node.js ist eine JavaScript-Laufzeit auf Chrome V8 JavaScript-Engine gebaut
https://nodejs.org/en/

[F] AngularJS, Ein Rahmen. Mobile & Desktop
https://angularjs.org/

[G] Electron, Build Cross Plattform Desktop-Anwendungen mit JavaScript, HTML und CSS
https://electron.atom.io/

[H] MongoDB, Aufbauend auf dem Besten von Relational mit den Innovationen von NoSQL
https://www.mongodb.com/

[I] Alle möglichen Blockparameter werden überprüft, einschließlich der effektiven Balance
des Blockgenerators. Dies beweist, dass das generierende Konto
tatsächlich enthält die effektive Balance (Pfahl), die es das Recht zu gewann
den Block erzeugen

[j] Siehe 3.6 für eine Erläuterung dieser Parameter und wie sie verwendet werden.

[k] Für weitere Informationen:
http://de.wikipedia.org/wiki/ReedSolomon_error_correction

[l] Siehe 3.6 für weitere Informationen darüber, wie diese Waage verwendet wird.

7.4 referenzen

[1] Satoshi Nakamoto Bitcoin: ein Peer-to-Peer Electronic Cash System. (nd).
Abgerufen am 06. Juli 2014, ab https://bitcoin.org/bitcoin.pdf

[2] ZeroNet, Open, kostenlose und unzählige Webseiten mit Bitcoin Kryptographie und
BitTorrent Netzwerk, https://zeronet.io/

[3] Nxt Whitepaper, http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt

[4] Tendermint: Konsens ohne Bergbau, 2014
https://tendermint.com/static/docs/tendermint.pdf

[5] P2P Mischen und unvernetzbare Bitcoin-Transaktionen *
http://crypsys.mmci.uni-saarland.de/projects/FastDC/draft-paper.pdf

[6] IPFS ist das verteilte Web,
https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-
system.pdf

[7] Wikipedia, Diffie-Hellman Schlüsselaustausch,
https://de.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

[8] Yung, M., Dodis, Y., Kiayias, A., Malkin, T., & Bernstein, DJ (2006).
Curve25519: Neue Diffie-Hellman Speed Records. Public Key Cryptogra-
phy, 2006, 207-228 doi: 10.1007 / 11745853_14

[9] Der koreanische Certicate-basierte Digital Signature Algorithmus
http://grouper.ieee.org/groups/1363/P1363a/contributions/kcdsa1363.pdf

[10] Seitenketten. Einzahlungs- / Abhebungsseite,
https://www.blockstream.com/sidechains.pdf

[11] Welcher Stolz ist und warum es wichtig ist
http://bitcoinmagazine.com/6528/, 2013.

[12] Matthew Green et al. Zerocash: Dezentrale anonyme Zahlungen aus
bitcoin http://zerocash-project.org/media/pdf/zerocash-extended-

20140518.pdf, 2014

[13] Nationales Institut für Normen FIPS 180-2, Sicherer Hash-Standard, August
2000. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf.

[14] JavaScript, Objektnotation. Siehe http://json.org/

! Wichtig
für Übersetzung kann keine gewähr gegeben werden, maßgebend ist das original Whitepaper in englisch!
Zu finden auf der Seite von Infinity Economics:

http://www.infinity-economics.org/docs/infinity_whitepaper.txt