Ravencoin: Ein elektronisches Peer-to-Peer-System für die Erstellung und Übertragung von Assets

Bruce Fenton
Tron Black
www.ravencoin.org
3. April 2018

In der fiktiven Welt von Westeros werden Raben als Boten benutzt, die Wahrheitsaussagen tragen. Ravencoin ist eine anwendungsfokussierte Blockkette, die entwickelt wurde, um Wahrheitserklärungen darüber zu verbreiten, wem welche Vermögenswerte gehören.

Vielen Dank an den Gründer und Entwickler von Bitcoin. Das Ravencoin-Projekt wurde auf der Grundlage der harten Arbeit und der kontinuierlichen Bemühungen von über 430 Bitcoin-Entwicklern gestartet, die bis zum Datum der Ravencoin-Codegabel über 14.000 Commits gemacht haben. Wir sind Ihnen ewig dankbar für Ihre Sorgfalt bei der Herstellung eines sicheren Netzwerks und für Ihre Unterstützung bei der Entwicklung von freier und Open-Source-Software. Das Ravencoin-Projekt baut auf dem von Ihnen errichteten Fundament auf.

Abhandlung. Ravencoin ist eine Blockchain und Plattform, die für die Übertragung von Assets, wie z.B. Token, von einem Halter zum anderen optimiert ist. Basierend auf der umfangreichen Entwicklung und dem Test des UTXO-Modells des Bitcoin-Protokolls basiert Ravencoin auf einem Fork des Bitcoin-Codes. Zu den wichtigsten Änderungen gehören eine Blockbelohnungszeit von einer Minute, eine Änderung der Anzahl der ausgegebenen Münzen, jedoch nicht der gewichtete Verteilungsplan und die Hinzufügung von Funktionen zur Vermögensbildung und Nachrichtenübermittlung. Ravencoin ist kostenlos und Open Source. Alle Ravencoin (RVN) werden fair ausgegeben und öffentlich und transparent unter Verwendung von Proof of Work (POW) unter Verwendung des x16r-Algorithmus, der für Ravencoin erstellt wurde, abgebaut. Es gibt keine private, öffentliche, Gründer- oder Entwicklerzuweisung. Ravencoin soll Sicherheit, Benutzerkontrolle, Datenschutz und Zensurschutz in den Vordergrund stellen. Es ist offen für die Nutzung und Entwicklung in jeder Gerichtsbarkeit und ermöglicht gleichzeitig einfache zusätzliche Funktionen für Benutzer nach Bedarf.

1. Einleitung:

Eine Blockchain ist ein Ledger, das die Menge eines von einem Benutzer kontrollierten Objekts anzeigt. Es ermöglicht es, die Kontrolle über diese digitale Darstellung auf einen anderen zu übertragen. Von den vielen Einsatzmöglichkeiten der Blockchain-Technologie ist die Berichterstattung darüber, wem das Eigentum gehört, eine ihrer Kernfunktionen. Aus diesem Grund ist Bitcoin der erste und bisher erfolgreichste Use Case für die Blockchain-Technologie, der von Satoshi Nakamoto am 31. Oktober 2008 angekündigt wurde[1].

Das Ethereum ERC20-Protokoll und andere Projekte zeigen tokenisierte Assets, die eine andere Blockchain verwenden, die mit einer Vielzahl von Zwecken und Strukturen erstellt werden kann. Token bieten mehrere Vorteile gegenüber traditionellen Aktien oder anderen Beteiligungsmechanismen, z.B. schnellere Übertragungsgeschwindigkeiten, erhöhte Benutzerkontrolle und Zensurwiderstand sowie eine Reduzierung oder Eliminierung der Notwendigkeit eines vertrauenswürdigen Dritten.

Bitcoin hat auch die Fähigkeit, als Schienen für Token zu dienen, indem es Projekte wie Omnilayer, RSK oder Counterparty verwendet. Allerdings wurden weder Bitcoin noch Ethereum speziell entwickelt, um den Besitz zusätzlicher Assets zu erleichtern, und die Benutzer und Entwicklungsteams legen generell Wert auf andere Funktionen.

Ravencoin wurde entwickelt, um eine bestimmte Funktion effizient zu erfüllen: die Übertragung von Vermögenswerten von einer Partei zur anderen. Ein Ziel des Raven-Protokolls ist es, eine *anwendungsfokussierte Blockchain* und einen Entwicklungsaufwand zu schaffen, der Code erzeugen kann, der Vorteile für spezifische Anwendungsfälle bietet und gleichzeitig zu Open-Source-Code beiträgt, der von Bitcoin oder anderen Projekten verwendet werden kann.

Wenn die Weltwirtschaft von Akteuren mit verschiedenen Blockketten beeinflusst wird, dann könnte sich auch die heutige Funktionsweise der Kapitalmärkte ändern. Grenzen und Gerichtsbarkeiten können an Bedeutung verlieren, wenn mehr Vermögenswerte handelbar werden und der grenzüberschreitende Handel immer reibungsloser wird. In einer Zeit, in der Menschen mit Bitcoin sofort erhebliche Vermögensmengen bewegen können, werden globale Verbraucher wahrscheinlich die gleiche Effizienz für ihre Wertpapiere und ähnlichen Vermögenswerte verlangen.

2. Hintergrundtoken und andere Vermögenswerte

Am 3. Januar 2009 wurde Bitcoin als Peer-to-Peer Electronic Cash System eingeführt. Jahre später, nachdem es ein beachtliches Sicherheitsniveau erreicht hatte, wurde anerkannt, dass Vermögenswerte "on top of" oder eingebettet in die Bitcoin-Blockkette erstellt werden können. Neue Assets können der Bitcoin-Blockkette hinzugefügt werden, indem sichere, signierte, unveränderliche Bitcoin-Transaktionen erstellt werden, die auch Informationen über die Ausgabe und Übertragung von Assets enthalten.

Es gab mehrere Projekte, die der Bitcoin-Blockkette Token hinzugefügt haben. Der erste war Mastercoin[2] von JR Willett, gefolgt von Counterparty[3] und anderen Projekten. Eine Kategorie von Protokollen, die entwickelt wurden, um die Erstellung von Assets auf der Bitcoin-Blockkette zu erleichtern, wurde als Colored Coins[4] bekannt, da sie Bitcoin-Transaktionen mit speziell gestalteten Transaktionen im OP_RETURN[5] markieren, was einem Kommentarfeld im Bitcoin-Protokoll entspricht.

Der Vorteil der Einbettung von Assets in die Bitcoin-Blockchain liegt in der hohen Sicherheit. Bitcoin wird von vielen als die sicherste Blockkette angesehen, da es eine enorme Menge an verteilter Minenleistung gibt, die jeden Block mit einem "High-Level-Hash" sichert[6]. Da die verteilten Bitcoin-Knoten den Aufwand zur Erstellung eines High-Level-Hash erkennen, ist es

nahezu unmöglich, die Blockchain ohne unerschwinglich hohe Mining-Investitionen neu zu schreiben oder zu modifizieren. Die Bitcoin-Blockkette zu manipulieren, ihr Hauptbuch neu zu schreiben oder zu modifizieren, würde erhebliche Anstrengungen von einem Investor auf der Ebene eines Nationalstaates erfordern.

Der Nachteil der Einbettung von Assets in die Bitcoin-Blockchain besteht darin, dass die Bitcoin-Regeln wie ursprünglich geschrieben befolgt werden müssen und die Bitcoin-Knoten nicht wissen, dass Assets eingebettet werden. Das bedeutet, dass für jede Asset-Transaktion eine Bitcoin-Transaktion verwendet werden muss, und dass sie genügend Bitcoin senden muss, um als gültige Transaktion betrachtet zu werden, auch wenn der Hauptzweck der Transaktion darin besteht, den Asset zu senden. Das ist unangenehm, aber ein großer Nachteil ist, dass ein Bitcoin-Client, der dieses Bitcoin ausgibt, ohne von der Transaktion für eingebettete Assets Kenntnis zu haben, das Asset zerstört. So könnte beispielsweise ein Inhaber der privaten Schlüssel von Bitcoin zu Bitcoin, die die Vermögenswerte der Gegenpartei halten, diese Bitcoin versehentlich an eine Börse oder Wallet schicken und diese Vermögenswerte verlieren. Eine Teillösung zur Lösung dieses Problems besteht darin, ein spezielles Adressformat zu erstellen, das für die Anlage verwendet wird, aber nicht den Fehler verhindert, der die Anlage zerstören kann. Es liefert nur mehr Hinweise darauf, dass ein Asset in die Transaktion eingebettet ist.

Andere Token-Standards wie ERC20, ERC721 und ERC223 basieren auf Ethereum oder anderen Blockketten, die Smart Contracts unterstützen. Ein anderes Problem besteht bei der Verwendung dieser intelligenten Verträge. Da das Ethereum-Netzwerk diese intelligenten Vertrags-Token nicht erkennt, kann es sich derzeit nicht gegen einige häufige Probleme schützen. Intelligente Verträge können für Benutzer verwirrend sein, da es mehrere ERC20-Token mit identischen Namen geben kann. Der einzige Unterschied zwischen Verträgen mit identischen Namen ist der Vertragshash.

3. Vollständiges, Asset-bewusstes Protokoll-Level-System

Wer will nicht einen Raben gegen eine Taube tauschen? Der Wille des Menschen ist durch seine Vernunft beeinflusst. - William Shakespeare

Die Lösung besteht darin, ein bitcoinähnliches System zu schaffen, das vollständig asset-bewusst ist. Ein System, das sich über Vermögenswerte im Klaren ist, bietet zwei wesentliche Vorteile. Erstens ermöglicht es den Client- und RPC-Befehlen, das Asset vor einer versehentlichen Zerstörung zu schützen. Zweitens ermöglicht es einem einzelnen nativen Client, die Assets auszugeben, zu verfolgen und zu übertragen.
Schließlich, um die Sicherheit für die zugrunde liegenden Vermögenswerte zu gewährleisten, funktioniert das bitcoin-ähnliche System nur mit einem Marktwert, einer starken Minengemeinschaft und einer breiten Streuung.

Vermögenswerte
Assets sind Token, die von Benutzern des Raven-Protokolls ausgegeben werden können, ohne dass sie abgebaut werden müssen. Benutzer des Raven-Protokolls erstellen diese Assets und bestimmen deren Zweck und Regeln unabhängig vom Protokoll. Diese Vermögenswerte oder Token existieren auf der Ravencoin-Blockkette und können jeder Name, jede Bezeichnung oder jeder Zweck sein, der von den Erstellern der einzelnen Vermögenswerte, Münzen oder Token ausgewählt wurde. Die Token sind übertragbar und bewegen sich mit der gleichen Leichtigkeit wie Bitcoin oder andere ähnlich funktionierende Kryptowährungen. In Ravencoin ist ein Vermögenswert nur eine begrenzte Menge eines einzigartigen Symbols und kann auf jede beliebige Ravencoin-Adresse übertragen

werden. Vermögenswerte sind seit einiger Zeit auf anderen Plattformen wie Open Assets, Mastercoin, Counterparty und als ERC20[7] oder ERC223[8] Token auf Ethereum[9] verfügbar. Assets, die mit dem Raven-Protokoll erstellt wurden, haben mehrere Vorteile: Sie sind einfacher zu handhaben, straff und straff.

integriert mit einer nativen Münze und gesichert durch faires POW-Mining und Open-Source-Code, der nicht von einer zentralen Organisation betrieben wird.

Verwendung von Assets
Vermögenswerte oder Token können für alles verwendet werden, was die Fantasie des Schöpfers hervorrufen kann. Die hier vorgestellten Ideen sind eine Auswahl.

Darstellung von realen, verwahrten physischen oder digitalen Assets auf Token

- Goldbarren
- Silberne Münzen
- Physische Euros
- Grundstücksurkunden
- DC Comics präsentiert #26
- Energiekredite (Strom, Holz, Gas, Öl, Wind)

Vertretung eines Teils eines Projekts

- **Wertpapier-Token:** Aktien einer Gesellschaft, bei der die Aktien durch ein Token und nicht durch eine physische Aktienurkunde repräsentiert werden.
- Wertpapiere oder Beteiligungen mit der eingebauten Dividendenfähigkeit im RVN (in vielen Ländern des freien Marktes legal)
- Token, die eine Coop-, Kommandit-, Royalty-Sharing oder Profit-Sharing-Plattform darstellen.
- Ein Token, das einen von der Menge finanzierten Gegenstand darstellt, mit der Möglichkeit, den Gegenstand zu übertragen oder weiterzuverkaufen.

Darstellung virtueller Güter

- Tickets für eine Veranstaltung wie ein Baltimore Ravens-Spiel mit der Möglichkeit, diese weiterzuverkaufen.
- Eine Lizenz, um eine Aktivität zu erlauben.
- Ein Zugriffstoken zur Nutzung eines Dienstes
- Währung und Gegenstände im Spiel, die außerhalb der Spielplattform transferierbar sind.

Darstellung eines Kredits

- Geschenkgutscheine
- Flugmeilen
- Belohnungspunkte

Satoshi Nakamoto beschrieb Bitcoin als eine Implementierung von Wei Dai's bmoney[10], die darauf abzielt, den Benutzern mehr Kontrolle, Sicherheit und Privatsphäre zu bieten als zentralisierte Systeme. Ein Design, das angesichts des Bitcoin-Inhabers das Potenzial hat, Gewalt und Diskriminierung zu verhindern, bleibt privat.
Ravencoin beabsichtigt, diese Implementierung fortzusetzen, indem es sich auf andere

Vermögenswerte als Barmittel konzentriert und eine optimale Lösung bietet.

Plattform, die Benutzer leicht nach den Regeln, die sie auf einer sicheren Blockchain festlegen, ausgeben können.

4. Ravencoin Einführung und Algorithmus

Ravencoin wurde am 31. Oktober 2017 angekündigt[11] und veröffentlichte Binärdateien für den Bergbau am 3. Januar 2018,[12] dem jeweiligen neunten Jahrestag der Ankündigung und Einführung von Bitcoin. Ravencoin ist das bitcoinähnliche System, das es den Benutzern ermöglicht, Assets auszugeben und in ihre Blockkette zu integrieren. Dies geschieht in Phasen, die aufeinander aufbauen.

- In Bearbeitung

Erstellen Sie eine Plattform wie Bitcoin mit einem neuen Mining-Algorithmus, x16r[13], der eine sofortige Dominanz durch Mining-Pools und eine zukünftige Dominanz durch ASIC-Mining-Ausrüstung verhindern soll.

Starten Sie den Token ohne Vorbergung und mit einem fairen Start, um die Token breit zu verteilen.

Lassen Sie die Abbaurate steigen und den Wert des RVN-Tokens natürlich wachsen und verteilen Sie es schrittweise an Inhaber, die den Wert der Plattform verstehen.

Nutzen Sie den Beweis für das Work Mining, nicht weil es eine knappe Ressource an Strom verbrennt, oder den Bedarf an Computerhardware, sondern konzentrieren Sie sich auf den wertvollsten Teil der "Arbeit", der eine immer größere und zeitbasierte Wand aufbaut, die Benutzerdaten vor zukünftigen Manipulationen und Zensur mit jeder neuen Schicht schützt.

5. Ausgabe und Übertragung von Vermögenswerten

Tief in dieser Dunkelheit stand ich da und wunderte mich, fürchtete
mich, bezweifelte, träumte Träume, die kein Sterblicher jemals gewagt
hatte zu träumen;
Aber die Stille war ungebrochen, und die Stille gab kein Zeichen.
- Edgar Allen Poe, The Raven

Token-Namen sind garantiert eindeutig. Der erste, der ein Token mit einem bestimmten Namen ausgibt, ist der Eigentümer dieses Token-Projekts.

Der Aussteller eines Token brennt RVN und muss einen eindeutigen Token-Namen angeben. Der Emittent bestimmt die Ausgabemenge, die Anzahl der Dezimalstellen und ob er in Zukunft mehr von demselben Token ausgeben darf.

Erlauben Sie die Ausgabe anderer Token mit ähnlicher Methode wie Mastercoin, Counterparty oder CoinSpark[14].

Integrieren Sie Assets eng mit der GUI-Wallet und erstellen Sie neue RPC-Aufrufe, die eine intuitive Anlagenverwaltung ermöglichen. Stellen Sie mühelos neue Anlagen bereit, melden Sie aktuelle Salden und übertragen Sie diese an andere Benutzer.

Die Kombination von Open Source und den gemeinsamen Anreizmechanismen, die durch blockchainbasierte Token ermöglicht werden, ermöglicht es, Interessen so auszurichten, wie es traditionelle Strukturen nicht können.

Faire und Open-Source-Token-Projekte können Chefs, Herrscher, Mitarbeiter und Unternehmensstruktur durch abgestimmte Interessen und wirtschaftliche Entscheidungen der Teilnehmer ersetzen.

So kann in einigen Fällen, ob man selbstlos oder egoistisch motiviert ist, Open Source ein besseres Modell für viele neue und interessante Arten von Projekten sein als andere Strukturen. Ravencoin wird es Projekten ermöglichen, Token auszugeben, die Genossenschaften, Unternehmen oder Partnerschaften repräsentieren.

Genossenschaften sind beispielsweise eine gemeinsame Organisationsform, in der Mitarbeiter und Teilnehmer Eigentümer sind. Große Unternehmen wie Credit Agricole, REI, Land O' Lakes, Ace Hardware, Co-op Kobe, Sunkist und Ocean Spray sind als Kooperativen organisiert. Obwohl sie den Teilnehmern viele Vorteile bieten, sind Genossenschaften manchmal schwer zu strukturieren und zu pflegen. Die Tokenisierung von Kooperationsbeteiligungen eröffnet viele neue Möglichkeiten, diese Struktur zur Allokation von Ressourcen und Kapital zu nutzen. Da die Regeln für jeden Token von jedem Emittenten geändert werden können und die Protokollierung auf der Ravencoin-Blockkette mit der verteilten Arbeit erfolgt, können Unternehmen eine Vielzahl von Beteiligungsstrukturen anpassen und einsetzen.

Da die Token vom Emittenten entweder einzigartig, begrenzt oder fungibel gemacht werden können, können Token-Projektmanager Kategorien von Token-Inhabern wie "Class A-Aktionäre", "Lifetime Social Club-Mitglieder", "Gönner" oder "Inhaber von In-Game-Items" einrichten.

Token ermöglichen eine einfachere Ausgabe kleinerer öffentlicher Angebote.

"In Zukunft wird sich die Größenverteilung der multinationalen Unternehmen derjenigen der lokalen Wirtschaft annähern. Der Phasenwechsel zwischen diesen Staaten kann recht schnell erfolgen, da die Telekommunikations- und Transportkosten einen "Schmelzpunkt" durchlaufen und eine Vielzahl neuer multinationaler Kleinunternehmen und Branchen entstehen, um diese Unternehmen zu unterstützen". Nick Szabo, Sichere Eigentumsrechte mit Eigentümerbehörde, 1998[15].

Dies könnte auch den Betrug verringern, stellte der Ökonom Dr. Robert Shapiro fest, dass es signifikante Beweise für Betrug in der Wall Street gibt, die mit Sorgerechtsfragen verbunden sein

können (Dr. Patrick Byrne, PhD[16]).

Nur ein offenes Protokoll wird in einer globalen Wirtschaft, in der es mehrere Gerichtsbarkeiten mit jeweils komplexen und widersprüchlichen Vorschriften gibt, funktionieren.

6. Belohnungen

Erlauben Sie die Auszahlung von Belohnungen (oder Dividenden) im nativen Token. Mit einem einzigen Befehl wird die auf RVN lautende Belohnung automatisch gleichmäßig aufgeteilt und anteilig an die Inhaber des Vermögenswertes gesendet.

Beispiel:

Ein Kleinkind in einem Land, das es erlaubt, könnte ein Token kreieren, das ein Limonadenstandunternehmen repräsentiert. Angenommen, sie erstellt 10.000 LEMONADE-Token. Diese Token könnten verwendet werden, um Gelder für den Limonadenstand in Höhe von AUD$0,01 pro LEMONADE-Token zu sammeln, so dass sie AUD$100 für den Aufbau ihres Unternehmens aufbringen kann. Diese Token können von den Eigentümern leicht verkauft und übertragen werden. Angenommen, der Limonadenstand schneidet außerordentlich gut ab, weil die Nachbarschaft in dieses unternehmerische Projekt investiert wird. Jetzt will unsere fiktive Achtjährige diejenigen belohnen, die an ihr Projekt geglaubt haben. Mit einem Befehl kann sie Gewinne - auf einen beliebigen Wert, den RVN haben kann - an LEMONADE-Token-Inhaber senden. Es könnte sogar neue Besitzer von LEMONADE-Token geben, die sie nie getroffen hat. Die integrierte Benutzerfreundlichkeit sollte es jedem auf der ganzen Welt ermöglichen, dies auf einem Mobiltelefon oder Computer mit Windows, Mac oder Linux zu tun.

Damit ein solches globales System funktionieren kann, muss es unabhängig von den Regulierungsbehörden sein. Dies ist nicht auf ideologische Überzeugungen zurückzuführen, sondern auf praktische Aspekte: Wenn die Schienen für die Übertragung von Blockchain-Assets nicht zensurresistent und die Gerichtsbarkeit agnostisch sind, kann eine bestimmte Gerichtsbarkeit mit einer anderen in Konflikt geraten. In alten Systemen war das Vermögen im Allgemeinen in der Gerichtsbarkeit des Inhabers beschränkt und daher auf der Grundlage der Richtlinien dieser Gerichtsbarkeit leicht zu kontrollieren. Aufgrund des globalen Charakters der Blockchain-Technologie wird jede Fähigkeit auf Protokollebene, den Reichtum zu kontrollieren, potenziell Rechtsordnungen in Konflikt bringen und nicht fair funktionieren können.

7. Einzigartige Token

Einzigartige Token ermöglichen es den Token-Inhabern, einzigartige Assets zu erstellen. Wie ERC721-Token sind auch einzigartige Token garantiert einzigartig und es wird nur einer existieren. Eindeutige Token können den Besitzer wechseln, indem sie das eindeutige Token an die Adresse eines anderen Benutzers senden.

Einige Beispiele für eindeutige Token:

- Stellen Sie sich vor, ein Kunsthändler stellt den Gegenstand ART aus. Der Händler kann dann einzigartige ART-Assets erstellen, indem er jedem Kunstwerk einen Namen oder eine Seriennummer anhängt. Diese einzigartigen Token können zusammen mit dem Kunstwerk als Echtheitsnachweis an den neuen Besitzer übertragen werden. Die Token ART:MonaLisa und ART:VenusDeMilo sind nicht fungibel und stellen unterschiedliche

Kunstwerke dar.

- Ein Softwareentwickler kann die Anlage mit dem Namen seiner Software ABCGAME ausstatten und jedem ABCGAME-Token eine eindeutige ID oder einen eindeutigen Lizenzschlüssel zuweisen. Die Spielmarken können bei der Lizenzübertragung übertragen werden. Jeder Token ABCGAME:398222 und ABCGAME:423655 sind eindeutige Token.

- In Game Assets. Ein Spiel ZYX_GAME könnte einzigartige In-Game-Vermögenswerte in limitierter Auflage erstellen, die dem Spieler gehören und von ihm verwendet werden. Beispiel: ZYX_GAME:SwordOfTruth005 und ZYX_GAME:HammerOfThor
  Diese In-Game-Ressourcen können dann behalten, mit anderen Spielern über QR-Codes und Wallets gehandelt oder in ein Upgrade oder eine andere Version eines Spiels hochgeladen werden.

- RVN-basierte einzigartige Assets können mit realen Assets verknüpft werden. Erstellen Sie eine Anlage namens GOLDVAULT. Jede Goldmünze oder jeder Goldbarren in einem Tresor kann serialisiert und auditiert werden. Zugehörige einzigartige Vermögenswerte GOLDVAULT:444322 und GOLDVAULT:555994 können erstellt werden, um die spezifischen Vermögenswerte im physischen Goldtresor darzustellen. Der öffentliche Charakter der Kette ermöglicht eine vollständige Transparenz.

Beispiel:

Der Inhaber des Token CAR könnte für jedes Fahrzeug einen eindeutigen Token ausstellen, indem

er die Fahrgestellnummer angibt. Beispiel: CAR:19UYA31581L000000

Einige Anwendungsfälle für einzigartige Assets sind unter anderem:

- Software-Lizenzierung
- Kfz-Zulassung
- Nachweis der zu übertragenden Echtheitsmarken zusammen mit Gegenständen, die gefälscht werden könnten.
- Ein Token, das die Kommunikation auf einem Kanal ermöglicht (siehe Messaging).

8. Messaging-Stakeholder

"Wenn die Raben des Tower of London verloren gehen oder wegfliegen, wird die Krone fallen und Großbritannien mit ihr." - Unbekannt

Ein häufiges Problem bei Token/Assets ist, dass der Tokenaussteller nicht mit den Tokeninhabern kommunizieren kann. Dies muss sehr vorsichtig behandelt werden, da die Token-Inhaber nicht immer identifiziert werden wollen. Die Mitteilung sollte es dem Inhaber des Token ermöglichen, sich jederzeit abzumelden. Das Nachrichtensystem sollte nur ausgewählten Parteien erlauben, den Nachrichtenkanal zu nutzen, so dass es sich nicht um eine Spam-Routine handelt.

Das Messaging-System verwendet eindeutige Token, um die Kommunikation auf dem Haupt-Token-Kanal zu ermöglichen. Beispielsweise hätte der COMPANY-Token einen ~COMPANY:Alert Token, der es ermöglicht, Alerts an alle Inhaber von COMPANY zu senden.

Newsletter, Spieleentwickler, gemeinnützige Organisationen, Aktivisten, Unternehmen und andere Einrichtungen können Token für bestimmte Benutzer ausgeben und diese dann benachrichtigen, aber im Gegensatz zu E-Mail oder anderen Messaging-Diensten wird das Messaging selbst nur für Token-Inhaber aktiviert, wodurch der Token übertragbar wird.

Nachrichten an Token-Inhaber durch autorisierte Absender werden über die eindeutigen Assets geschichtet. Die einzigartigen Assets fungieren als "talking stick", so dass Nachrichten vom Channel-Besitzer gesendet werden können. *Das KAAAWWWW-Protokoll* wird mit weiteren Informationen dazu separat veröffentlicht.

9. Wahlen

Eines der Probleme unter vielen mit dem bestehenden US-Finanzsystem besteht darin, dass alle Aktien im Straßennamen gehalten werden. Das macht es im Zeitalter der schnellen Kommunikation lächerlich schwierig, eine Abstimmung durchzuführen. Eine Aktiengesellschaft, die beispielsweise Aktien an der Nasdaq ausgibt, muss eine Quasi-Monopolgesellschaft bezahlen, nur um die Postanschriften ihrer eigenen Aktionäre zu einem bestimmten Zeitpunkt zu erhalten. Anschließend muss den Aktionären ein physisches (toter Baum) Mailing mit Informationen zur Stimmabgabe zusammen mit einem Stimmrechtsvertreter zugesandt werden.

Durch die Verwendung des Messaging-Systems können die Inhaber eines Token über die Abstimmung informiert werden, und durch die automatische Ausgabe eines VOTE-Tokens an jeden Inhaber eines Token kann die Abstimmung vom Client aus oder über eine Web- oder mobile Schnittstelle unter Verwendung des in Ravencoin integrierten Protokolls automatisiert werden.

Token werden erstellt, um Stimmen zu repräsentieren. Ravencoin erstellt eine genaue Anzahl von VOTE-Token und verteilt diese 1:1 an die Inhaber der Token. Diese Stimmen können über das Protokoll an Adressen gesendet werden, die den Stimmen entsprechen. Da sich die Stimmmarken wie Vermögenswerte bewegen, ist eine Stimmrechtsübertragung - manchmal auch als delegierte oder flüssige Demokratie bezeichnet[17] - möglich.

10. Datenschutz

Es ist eine Gemeinschaft, in der die Androhung von Gewalt machtlos ist, weil Gewalt unmöglich ist, und Gewalt ist unmöglich, weil ihre Teilnehmer nicht mit ihren wahren Namen oder physischen Orten verbunden werden können. (Wei Dai)

Datenschutz ist der Schlüssel zu Investitionen und Token, weil Finanzsysteme besser funktionieren, wenn Vermögenswerte fungibel sind und reibungslos handeln können. Das Projekt sollte darauf

abzielen, die Privatsphäre in jeder erdenklichen Weise zu stärken, wenn zukünftige technologische Verbesserungen vorgenommen werden.

Da Funktionen wie Messaging, Assets und Belohnungen hinzugefügt werden, wird die Privatsphäre auf die gleiche Weise geschützt, wie UTXO-basierte Kryptowährungen die Identität von öffentlichen Adressen trennen.

"Da wir den Datenschutz anstreben, müssen wir sicherstellen, dass jede Partei einer Transaktion nur Kenntnis hat von
das, was für diese Transaktion direkt notwendig ist. Da über alle Informationen gesprochen werden kann, müssen wir sicherstellen, dass wir so wenig wie möglich preisgeben. In den meisten Fällen ist die persönliche Identität nicht hervorstechend.
.... Wenn meine Identität durch den zugrunde liegenden Mechanismus der Transaktion offenbart wird, habe ich keine Privatsphäre. Ich kann mich hier nicht selektiv offenbaren; ich muss mich immer offenbaren.
"Daher erfordert der Datenschutz in einer offenen Gesellschaft anonyme Transaktionssysteme. Bislang war Bargeld das wichtigste derartige System. Ein anonymes Transaktionssystem ist kein geheimes Transaktionssystem. Ein anonymes System ermöglicht es dem Einzelnen, seine Identität zu offenbaren, wenn er es wünscht und nur wenn er es wünscht; das ist die Essenz der Privatsphäre." (E. Hughes) [18].

11. Zusätzliches

Andere Projekte können diese Kette nutzen. Second-Layer-Lösungen, insbesondere solche, die für Projekte entwickelt werden, die die Codebasis von Bitcoin teilen, können auf dem Ravencoin-Projekt aufgebaut werden. Die RSK, das Lightning Network, vertrauliche Transaktionen und andere Verbesserungen der Skalierbarkeit usw. zu verschiedenen Open-Source-Projekten könnten von Projekten auf dieser Plattform profitieren.

12. Conclusion

Ravencoin ist eine Plattformmünze, die auf dem UTXO[19] Modell von Bitcoin basiert. Das Modifizieren von Bitcoin-Code, um diese Funktionen hinzuzufügen, ist nicht praktikabel, aber Ravencoin ist eine Plattform, die aus einer Code-Gabel und der Ausgabe von neu abgebauten RVNs besteht. Ravencoin wird Vermögenswerte, Belohnungen, einzigartige Vermögenswerte, Messaging und Abstimmungen hinzufügen. Die Fähigkeiten des Raven-Protokolls werden in Phasen eingeführt, die als geplantes Hard Fork Upgrade durchgeführt werden. Die Codebasis ist so konzipiert, dass Benutzer und Entwickler ein sicheres, dezentrales und manipulationssicheres Netzwerk pflegen können.

Das Ravencoin-Projekt kann auch als Basis und Ausgangspunkt für Projekte, Second-Layer-Lösungen, Experimente und Geschäftsideen dienen, die entweder von der Bitcoin-basierten Codebasis mit Anpassungen oder den nativen zusätzlichen Funktionen der Ravencoin-Blockkette profitieren könnten.

Die Inuit, Tlinglit, Tahitianer, Chukchi, Sioux, die Haida und viele andere nennen Raven den

magischen Hüter der Geheimnisse, den Trickser, Freund der Ersten Menschen und Schöpfer der Welt - eine Idee oder Kraft, die in der Lage ist, etwas aus dem Nichts zu verschieben, zu verändern und zu erschaffen. In Open Source kann die Macht der Menge viel mehr erreichen als jede einzelne Person oder Organisation. Alle sind herzlich eingeladen, einen Beitrag zu leisten.

Referenzen

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf
[2] https://bravenewcoin.com/assets/Whitepapers/2ndBitcoinWhitepaper.pdf
[3] https://counterparty.io/
[4] https://en.bitcoin.it/wiki/Colored_Coins
[5] https://en.bitcoin.it/wiki/OP_RETURN
[6] https://bitcoinwisdom.com/bitcoin/difficulty
[7] https://theethereum.wiki/w/index.php/ERC20_Token_Standard
[8] https://github.com/Dexaran/ERC223-token-standard
[9] https://www.ethereum.org/
[10] W. Dei, “B-Money” http://www.weidai.com/bmoney.txt
[11] B. Fenton, “Ravencoin: A digital peer to peer network for the facilitation of asset transfers.” https://medium.com/@ravencoin/ravencoin-4683cd00f83c
[12] https://github.com/RavenProject/Ravencoin
[13] T. Black, J. Weight “X16R” Algorithm White Paper https://ravencoin.org/wp-content/uploads/2018/03/X16R-Whitepaper.pdf
[14] http://coinspark.org/developers/assets-introduction/
[15] N. Szabo, “Secure Property Titles with Owner Authority” http://nakamotoinstitute.org/secure-property-titles/#selection-7.7-7.50
[16] https://www.forbes.com/2008/09/23/naked-shorting-trades-oped-cx_pb_0923byrne.html#63076e102e6c
[17] https://en.wikipedia.org/wiki/Delegative_democracy
[18] E. Hughes https://www.activism.net/cypherpunk/manifesto.html
[19] https://bitcoin.org/en/glossary/unspent-transaction-output