The Pirate Code

Der Piraten Code

V1.0

Autoren: Flexatron, FishyGuts, jl777c & KMD community

Deutsche Fassung: Seko1900 & Acura

Kurzfassung

Eine vollständig private Kryptowährung und abgeschirmte Blockchain, die aus den Federn des Komodo-Ökosystems stammt. Pirate löst Zcashs "Fungibilitätsproblem" durch die Eliminierung von Transaktionsfunktionen für transparente Adressen in der Blockchain und macht die private Nutzung "narrensicher". Diese Funktion führt zu einer vollständig abgeschirmten Benutzermünzbasis in der Piratechain. Durch die konsequente Nutzung der zk-SNARK-Technologie hinterlässt die Pirate-Münze keine brauchbaren Metadaten von Benutzertransaktionen auf der Blockchain. Alle ausgehenden Transaktionen, mit Ausnahme von Mining-Blockbelohnungen und Notartransaktionen, werden an abgeschirmte Sapling-Adressen geschickt, um die Effizienz und Geschwindigkeit der Kette zu maximieren. Pirate verwendet den Konsensalgorithmus Equihash Proof-of-Work aus Zcash mit einer zusätzlichen Sicherheitsschicht (dPoW) aus Komodo, die der Pirate Blockchain ein höheres Sicherheitsniveau als BTC bietet.

Die Zukunft des privaten dezentralen Zahlungsverkehrs ist da!

Inhalt

Der PIRATE Code

Leitbild

Die Mission von Pirate ist es, die finanzielle Privatsphäre der Menschen in einem von transparenten Transaktionen dominierten System zu schützen.

Leistungsversprechen

- *Alle Transaktionen in der Blockchain von Pirate sind standardmäßig privat und damit anonym.*

Dies mildert die Fungibilitätsprobleme, die viele Kryptowährungen mit optionalem Datenschutz in ihrem Protokoll haben. Dieses vollständige Datenschutzprotokoll bietet den Benutzern mehr Sicherheit, dass keine Behörde behaupten kann, sodass die Gelder der Benutzer durch frühere Transaktionen jetzt und in Zukunft negativ belastet sind.

- *Der Pirate Coin ist vollständig dezentralisiert.*

Es gibt zu keinem Zeitpunkt einen Dritten, der für Ihr Geld verantwortlich ist. Private Transaktionen werden auf der Blockchain vertrauenswürdig bestätigt, d.h. Sie brauchen keinen Dritten, um die Gültigkeit Ihrer Transaktionen zu überprüfen, dafür sorgt der Piratencode.

- *Pirate ermöglicht einen sicheren und schnellen Wertetransfer.*

Die Piratechain wird durch einen Mechanismus gesichert, der schwerer zu knacken ist als Bitcoin selbst, der als delayed Proof-of-Work (dPoW) (verzögerter Arbeitsnachweis) bezeichnet wird. Nutzungsentgelte sind sowohl für den Kunden als auch für den Lieferanten sehr günstig. Darüber hinaus gibt es keine Chance auf betrügerische Rückbuchungen, keine fehlerhaften Verifizierungszeiträume für Fonds, und Transaktionen werden innerhalb von Minuten bestätigt und gesichert. Diese Funktionen allein können Händlern und Verkäufern auf der ganzen Welt Milliarden von Dollar sparen, indem sie die Vermittlungsgebühren abschaffen.

- ❖ *Pirate verwendet das strengste Datenschutzprotokoll.*

Das hochentwickelte und respektierte Datenschutzprotokoll zk-SNARKS verlangt nicht, dass die Daten aus Ihrer Transaktion in den öffentlichen Ledgern sichtbar sind. Dies wird von vielen prominenten Entwicklern als eine der stärksten Methoden angesehen, um Ihre Finanzdaten auf der Blockchain zu verstecken.

Warum der Fokus auf den Datenschutz?

Krypto bietet Vorteile für Anwender und Unternehmen, aber das sollte nicht zu Lasten der finanziellen Privatsphäre gehen.

Die heutigen FIAT-Währungen machen bereits einen Massenaustritt in Richtung digitaler Systeme (Japparova en Rupeika-Apoga 2017). Krypto hat gezeigt, dass es zahlreiche Vorteile für Unternehmen bietet, wie Kosteneinsparungen bei Gebühren und Transaktionsgeschwindigkeit. Unserer Meinung nach verdienen die Nutzer bei diesen Transaktionen Datenschutz.

Warum sollte man dem Ladenbesitzer die Größe seines Vermögens oder seiner Konsumgewohnheiten zeigen?

Der finanzielle Datenschutz kann daher von allen Parteien, die Kryptowährung akzeptieren wollen, benötigt werden, wie z.B. von Verkäufern, Distributoren, Händlern, Käufern, Lieferanten, Dienstleistern und Kunden. Unternehmen können ihren Kunden und sich selbst versichern, dass beide Parteien der Transaktion durch den Einsatz von Pirate die beste Kombination aus Datenschutz, Geschwindigkeit und Kosteneinsparungen erhalten.

Die Mannschaft

Als wirklich dezentrale Kryptowährung begrüßt Pirate Entwickler und Mitwirkende aller Skillsets.

Bereits über 30 Mitwirkende haben seit ihrer Gründung Dienstleistungen für das Wachstum und die Entwicklung der Piratenkette erbracht. Entwickler arbeiten in einem zusammenhängenden Team, um Wissen und Erfahrung aus allen Bereichen der Krypto-Welt einzubringen. In unserer vielfältigen Gruppe gibt es immer eine Person, die weiß, wie man eine benötigte Aufgabe erledigt, oder jemanden, der eine Verbindung zu jemandem hat, der es kann.

Pirate hat viele erste Erfolge in der Kryptowährungsbranche erzielt, wenn es um den Schutz der Privatsphäre geht (siehe Roadmap), und

Pirate wird weiterhin mit Dritten an innovativen Techniken arbeiten, um mehr Privatsphäre für alle zu ermöglichen.

Einführung

Kryptowährungen

Seit der Veröffentlichung des berühmten Whitepapers von Satoshi Nakamoto im Jahr 2008 (Nakamoto 2008) hat sich Bitcoin zu einem Multi-Milliarden-Dollar-Marktkapitalisierung Digital Asset entwickelt. Seitdem sind eine Reihe alternativer Kryptowährungen entstanden, die versuchen, die Lücke einer Vielzahl von Anwendungsfällen mit ihren eigenen Gemeinschaften zu füllen. Die Verwendung von Kryptowährungen als Zahlungsmittel ist einer der beliebtesten Anwendungsfälle und auch der Hauptzweck, für den Satoshi das Whitepaper geschrieben hat. Das Ziel von Bitcoin ist es, jedem Menschen zu ermöglichen, jederzeit und überall auf der Welt Werte zu transferieren, indem er eine Internetverbindung auf eine vertrauenswürdige Weise von Mensch zu Mensch nutzt. Bitcoin verwendet ein verteiltes Ledger, um Transaktionen zu erleichtern und aufzuzeichnen, deren Wahrhaftigkeit durch den Konsensalgorithmus Proof-of-Work (PoW) bestimmt wird.

Privatsphäre

Ein großes Anliegen beim Einsatz dieser Technologie ist die Fähigkeit der Beobachter, ihr Ausgabeverhalten und ihren Vermögensstatus zu analysieren (Moser 2013). Dies beeinträchtigt die finanzielle Privatsphäre des Benutzers erheblich. Es wurden eine Reihe von Kryptowährungsprotokollen entwickelt, die darauf abzielen, die Datenschutzaspekte von Bitcoin zu verbessern. Die bemerkenswertesten Protokolle, die bisher entwickelt wurden, sind CryptoNote (Van Saberhagen 2013) und Zerocash (Sasson et al. 2014). Das erste Protokoll verwendet Ring Confidential Signatures, während das zweite Protokoll Zero-Knowledge-Proofs verwendet, um Transaktionen und Kontensalden zu verbergen, genauer dazu später. Beide Protokolle haben ihre Vor- und Nachteile. Dieses Whitepaper behandelt, wie Pirate (ARRR) versucht, die Datenschutzaspekte der aktuellen dezentralen Zahlungsprotokolle zu verbessern.

Wichtigste Nachteile aktueller dezentraler Zahlungsprotokolle

Monero Ring CT Signatures scheme

Monero, ein Fork von Bytecoin, die auf dem CryptoNote-Protokoll basiert, verwendet in ihren Transaktionen ein Ringsignaturschema, kombiniert mit Stealth-Adressen, zufälligen Einmaladressen für jede Transaktion im Namen des Empfängers. Ringsignaturen erschweren die Rückverfolgung des Absenders in Abhängigkeit von der Ringgröße zunehmend. Dies lässt den Parteien jedoch die Möglichkeit, die verfügbaren Daten mit ausgefeilten Analysewerkzeugen jetzt und in Zukunft zu analysieren.

Aufgrund der Verwendung von Ringsignaturen ist die Analyse der Blockchain von Monero schwierig, wie folgend dargestellt:

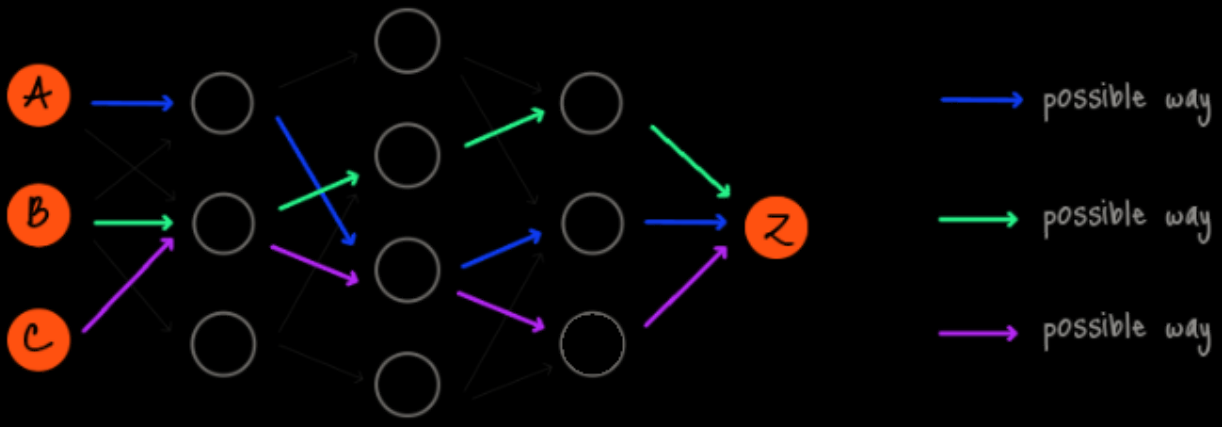

Abbildung 1 ***Ring signature blockchain Analyse****.*

Quelle: https://cryptonote.org/inside#untraceable-payments

Die Schwierigkeit, den richtigen Absender zu finden, wird bei größeren Ringgrößen immer schwieriger. Die Ringgröße ist die Gesamtzahl der möglichen Unterzeichner, einschließlich Ihrer, was wiederum die Komplexität und Schwierigkeit bestimmt, die "reale Ausgabe" zu finden. Eine höhere Ringgrößenzahl bietet daher ein höheres Maß an Privatsphäre als eine niedrigere Zahl. Es ist jedoch nicht ratsam, eine ungerade erkennbare Ringgrößenzahl wiederzuverwenden, um sich nicht von anderen Transaktionen abzuheben[3].

Das grundlegende Problem der Münzmischverfahren besteht jedoch darin, dass Transaktionsdaten nicht durch Verschlüsselung versteckt werden. RingCT ist ein System der Disassoziation, bei dem

Informationen in der Blockkette noch sichtbar sind. Beachten Sie, dass in Zukunft möglicherweise eine Schwachstelle entdeckt wird, die eine Rückverfolgbarkeit ermöglicht, da die Blockchain von Monero eine Aufzeichnung jeder stattgefundenen Transaktion liefert.

Zcash's abgeschirmte Lösung befasst sich mit der Implementierung und den Ausgabenarten.

Zcash, eine Implementierung des dezentralen anonymen Zahlungsschemas Zerocash, fügt dem bestehenden transparenten Zahlungsschema von Bitcoin (Hopwood et al. 2016) ein abgeschirmtes Zahlungsschema hinzu, das durch prägnante nicht-interaktive Wissensargumente (zk-SNARKs) gesichert ist. Die Verwendung von geschirmten oder nicht geschirmten Zahlungen ist dem Nutzer freigestellt. Es wird davon ausgegangen, dass der Prozentsatz der abgeschirmten Transaktionen steigt, da die jüngste Implementierung von "Sapling" durch Zcash die Verarbeitung der abgeschirmten Transaktionen nur einen Bruchteil rechenintensiver als die der nicht abgeschirmten Transaktionen macht (Bowe 2017). Leider beeinträchtigt der relativ hohe Anteil an nicht abgeschirmten Transaktionen und Salden die Fungibilität der Münzen, da es möglich ist, Transaktionen während der "privaten" Zahlungsaktivität zu verknüpfen und sie somit möglicherweise mit der Münzmischung in Verbindung zu bringen. Dies ist insbesondere bei der Durchführung einer "Round-Trip-Transaktion" der Fall, d.h. dem Senden der genauen Anzahl der Münzen von einer transparenten (t-addr) an eine geschirmte Adresse (z-addr) und zurück an eine andere transparente Adresse (Quesnelle 2017). Wir bezeichnen in diesem Beitrag dieses Phänomen als das "Fungibilitätsproblem".

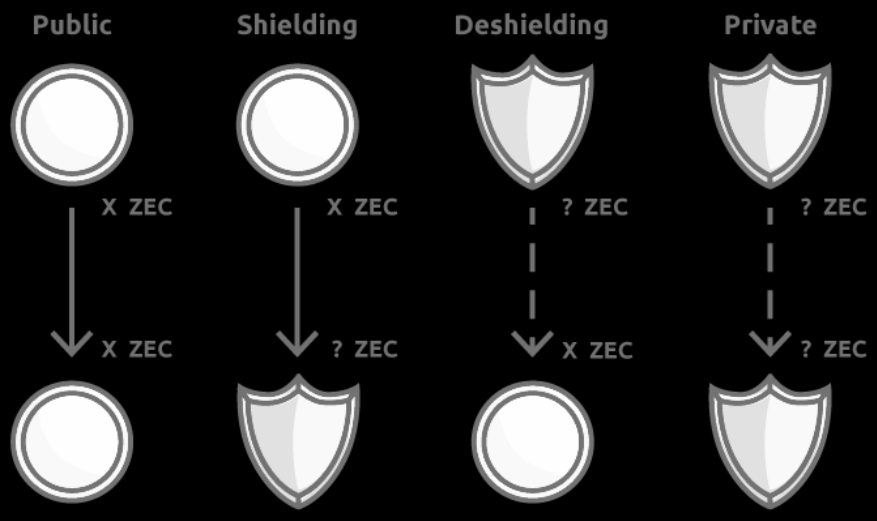

Abbildung 2: ***User von Zcash haben 4 verschiedene Möglichkeiten Zcash auszugeben***

Source: https://z.cash/blog/sapling-transaction-anatomy/

Wie in obiger Abbildung 2 dargestellt, erhalten Zcash-Benutzer die Möglichkeit, 4 verschiedene Arten von Transaktionen im aktuellen

Zcash-Protokoll durchzuführen. Die Möglichkeit, von der Öffentlichkeit an geschützte Adressen zu senden und umgekehrt, stellt eine große Gefahr für die Fungibilität der Münzen dar. Es ist möglich, Münzmischmuster zwischen den verschiedenen Arten von Transaktionen zu identifizieren, wenn Benutzer Münzen an transparente Adressen zurücksenden, wie beispielsweise bei "Round-Trip-Transaktionen", da dieses Verhalten eine hohe Verknüpfbarkeit aufweist (Quesnelle 2017).

Die Leistungssteigerungen von Sapling gehen leider zu Lasten des Datenschutzes, da Sapling-Transaktionen mehr Metadaten enthalten als die "alten" JoinSplit-Aktivitäten. Sapling-Transaktionen zeigen die Anzahl der verwendeten Ein- und Ausgänge an. Diese Funktionalität erweitert die Möglichkeiten, zwischen Transaktionsarten zu unterscheiden, Transaktionsdaten zu analysieren und möglicherweise das Verhalten beim Mischen zu identifizieren.

Um dieses Risiko zu reduzieren oder zu eliminieren, ist es wichtig, entweder die Verwendung transparenter Adressen zu reduzieren oder sie in einer neuen Blockchain wie Pirate von Anfang an einfach zu deaktivieren.

Unsere Lösung

Pirate will die Datenschutz- und Sicherheitsmerkmale von Monero erheblich verbessern und das "Fungibilitätsproblem" von Zcash beheben. Die Piratenkette tut dies, indem sie nur "Sapling" abgeschirmte Transaktionen (z-tx) akzeptiert, abgesehen von Mining-Belohnungen und Beglaubigungen, wie im Abschnitt dPoW erläutert. Darüber hinaus wird die Piratenkette durch den verzögerten Proof-of-Work-Mechanismus gesichert, der ihre Datenschutz- und Sicherheitsmerkmale im Vergleich zu bestehenden Datenschutzmünzen derzeit in der Blockkettenbranche unübertroffen macht.

Die Piratechain: Datenschutz, Fungibilität und Sicherheit

29. August 2018 - Der Ruf nach voller Anonymität

Pirate startete am 29. August in Discord als Idee einer 100% zk-SNARKS-Münze. Die Entwicklungsarbeit von *jl777c* an Komodo Asset-Ketten ermöglichte die Durchsetzung der Nutzung abgeschirmter Transaktionen durch die Anpassung der Parameter der Asset-Chain in einer neuen Asset-Chain (Grewal 2018). Eine Asset Chain ist ein Komodo Runtime Fork und ist eine eigentliche unabhängige Blockchain.

Pirate begann zunächst als Experiment, um zu beobachten, ob erzwungene Z-Transaktionen funktionieren können, aber die Community erkannte schnell das Potenzial, nachdem *jl777c* erfolgreich **delayed Proof-of-Work** eingeführt hatte, wodurch Pirate vervollständigt wurde.

Komodo – Zcash fork – zk-SNARKs

Pirate ist ein Teil des Komodo-Plattform Ökosystems. Das Komodo-Projekt konzentriert sich darauf, Blockchain-Unternehmer und den durchschnittlichen Benutzer der Kryptowährung durch die Blockchain-Technologie mit Freiheit und Benutzerfreundlichkeit zu unterstützen (Lee 2018). Komodo begann als ein Fork der beliebten Datenschutzmünze Zcash. Das Zcash-Projekt selbst ist eine Weiterentwicklung von Bitcoin. So sind alle von Satoshi Nakamoto im Bitcoin-Protokoll entwickelten Funktionen auch in Komodo verfügbar.

Daher verfügt Komodo über die gleichen inhärenten Datenschutzfunktionen wie Zcash. Zu diesen Merkmalen gehören die Zcash-Parameter und die zk-SNARK-Technologie.

Zk-SNARKS ist eine der mächtigsten Formen der Blockchain-Privatsphäre, die es gibt, da die gebotene Privatsphäre effektiv dauerhaft ist.

Diese Aussage wird sogar vom Hauptvertreter von Monero, *Riccardo "fluffypony" Spagni*, hervorgehoben:

> *"ZCash's zkSNARKs provide much stronger untraceability characteristics than Monero (but a much smaller privacyset and much higher systemic risks)."*

Komodo Asset Chains

Eine Asset Chain (offiziell Parallel Chain) ist eine unabhängig erstellte Blockchain, die alle Funktionen von Komodo wie

BarterDEX-Kompatibilität, Zero Knowledge Privacy und den verzögerten Arbeitsnachweis (dPow) etc. übernimmt, aber auch zahlreiche kundenspezifische Spezifikationen wie Custom Coin Supply und Custom RPC-Port hat. Weitere kundenspezifische Funktionen sind derzeit in Vorbereitung (PTYX 2018).

Weitere Beispiele für Komodo-Anlagenketten sind Bitcoin Hush (BTCH), ChainZilla (ZILLA), DEX, Equalizer (EQL), KMDice, Monaize (MNZ), PUNGO, REVS, SuperNET, Utrum und ZEX.

Erzwungene Z-Transaktionen

Die beste Lösung für das "Fungibilitätsproblem" besteht unserer Meinung nach darin, die Möglichkeit des Versands an transparente Adressen zu deaktivieren. Dies eliminiert die Existenz von Transaktionen von abgeschirmten Salden bis hin zu transparenten Salden, die oft die Ursache für eine verminderte Fungibilität sind. Wie vom Hauptentwickler von Zcash selbst als Reaktion auf das Papier "Über die Verknüpfbarkeit von Zcash-Transaktionen" von *Jeffrey Quesnelle* zitiert:

“But my answer is instead we're going to ban unshielded transactions. Even simpler.”

Delayed Proof of Work: Maximale Sicherheit und Flexibilität

Was ist der verzögerte Arbeitnsachweis?
Der verzögerte Arbeitsnachweis (delayed Proof of Work) stammt von Komodo und bietet eine einzigartige und innovative Form der Sicherheit, die so stark ist wie das Netzwerk, an das sie angeschlossen ist, aber nicht die Kosten für den Betrieb dieses Netzwerks erfordert. Delayed Proof-of-Work ist eine Lösung, die mehrere bestehende Methoden in einem einzigen hybriden Konsensus-System nutzt, das so energieeffizient ist wie Proof-of-Stake (PoS), während es durch Bitcoins Proof-of-Work gesichert ist. User, die unabhängige Blockchains (Asset-Chains) im Komodo-Ökosystem aufbauen, können sich für einen Block-Hash entscheiden, der als "Snapshot" ihrer eigenen Blockchain in die Komodo-Hauptkette eingefügt wird. Auf diese Weise werden die Aufzeichnungen der Asset-Chain indirekt in den Block-Hash von Komodo einbezogen, der auf die Blockchain des stärksten Netzwerks (jetzt Bitcoin) geschoben wird.

So ermöglicht dPoW auch den schwächsten Blockchains, von der Hash-Rate Bitcoins zu profitieren, was wiederum den Stromverbrauch von Bitcoin umweltfreundlicher macht, da es das gesamte Ökosystem

von dPoW zusätzlich zu sich selbst sichert (Jl777c 2016). Neben Pirate wurde dPoW in einer Vielzahl von Asset-Chains wie u.a. Game Credits, Einsteinium (EMC2), Pungo und HUSH (Komodostats 2018) erfolgreich eingesetzt.

Was sind die Mechanismen hinter delayed Proof-of-Work?

Der Komodo-Sicherheitsdienst wird von Notarknoten erbracht, die benötigt werden, um Block-Hashes auf die Bitcoin-Blockchain, die als notarielle Beglaubigung bezeichnet wird, aufzuzeichnen (Abb. 3). Die Beurkundung beinhaltet die Erstellung einer gruppensignierten Bitcoin-Transaktion, die den jüngsten Blockhash von Komodo enthält, unterzeichnet von einer unbekannten Kombination von 33 von 64 Notarknoten (Jl777c 2016). Block-Hashes der Piratechain werden mit der gleichen Methode ebenfalls zeitnah in die Komodo-Blockchain eingefügt.mDie Notarknoten zahlen die BTC-Transaktionsgebühr für die Beglaubigung der Komodo-Blockkette. Die Bitcoin-Transaktionsgebühren für Notarknoten werden durch Blockprämien und Transaktionsgebühren der Komodo-Blockkette an Notarknoten ausgeglichen. Es wird daher erwartet, dass die finanziellen Interessen der Beteiligten für Notarknoten stimmen, mit denen sich die Beteiligten wohlfühlen. 64 weitgehend verteilte Notarknoten stehen zur Wahl und sollen eine optimale Darstellung eines dezentralen Ökosystems sein, was jede Art von 51% Angriff höchst unwahrscheinlich macht.

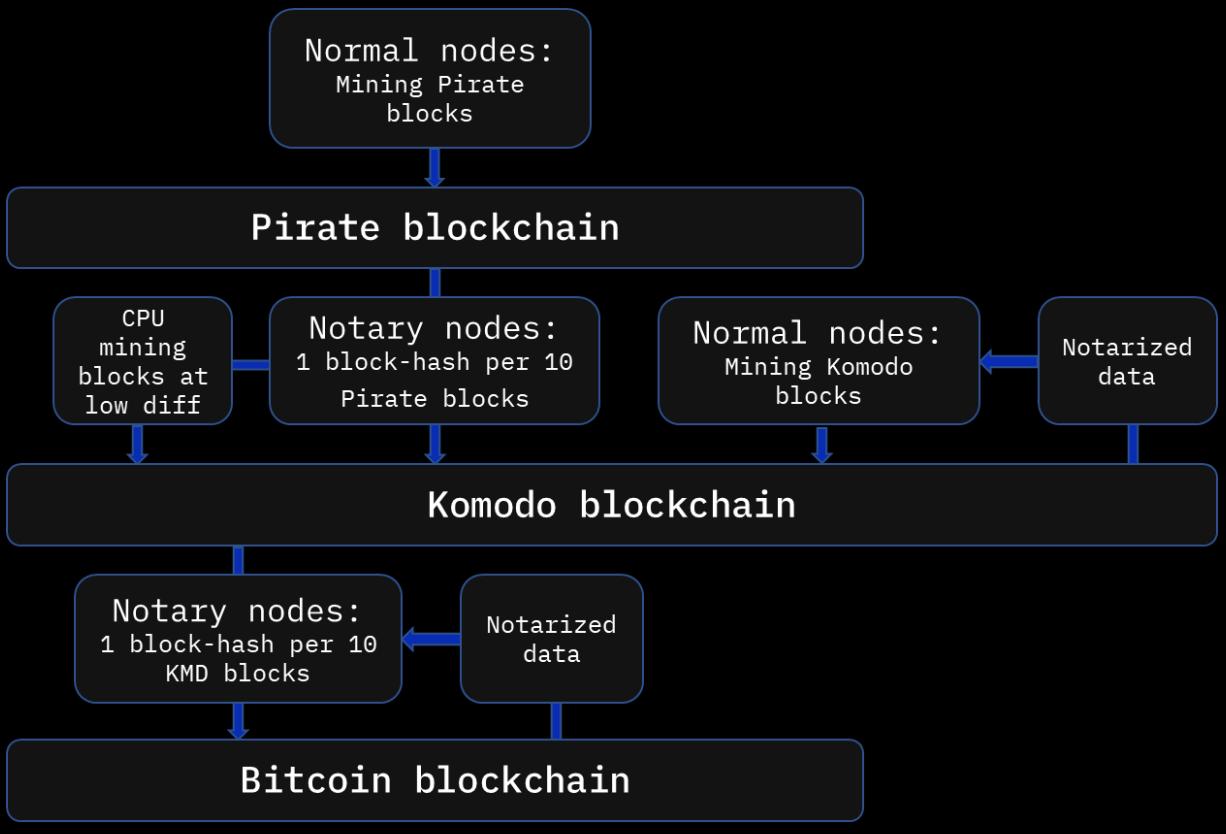

Abbildung 3 ***Eine schematische Darstellung des verzögerten Arbeitsnachweises***

Um also Pirate zu reorganisieren und anzugreifen, müsste der Angreifer folgendes zerstören:

- alle vorhandenen Kopien der Piratechain;
- alle Kopien der Komodo-Mainchain;
- das PoW-Sicherheitsnetzwerk (Bitcoin), in das die notariellen Daten der Komodo-Blockchain eingefügt werden.

Darüber hinaus haben Notarknoten die Freiheit, den Beurkundungsprozess auf ein anderes PoW-Netzwerk umzustellen, wenn es in Zukunft zu einer Verschiebung der Hash-Raten zwischen den großen Blockchains kommen sollte.

Der verzögerte Arbeitsnachweis (dPoW) bietet Pirate eine höhere Sicherheit als Bitcoin, während die überhöhten finanziellen und umweltfreundlichen Kosten vermieden werden. Durch die Flexibilität von dPoWs bietet es einen flexibleren und anpassungsfähigeren Charakter als Bitcoin selbst.

Beispiele für Angriffe auf Blockchains

Es gibt eine Reihe von Beispielen, die die Notwendigkeit eines Mechanismus wie des dPoW hervorheben:

Im April 2018 wurde ein Fehler im Retargeting-Mechanismus der Algorithmen von Vergecurrency (XVG) durch einen 51%igen Angriff ausgenutzt. Mit gefälschten Zeitstempeln wurde die Notwendigkeit eines anderen Algorithmus für jeden Block umgangen. Die Hacker konnten Blöcke mit einer Minining-Geschwindigkeit von 1 Block pro Sekunde an die Kette übergeben, wodurch 99% der Blöcke der legitimen Pools geleugnet wurde und Geld verloren wurde (Ocminer 2018a). Im Mai 2018 geschah der gleiche Angriff, aber mit einem anderen Ansatz: Hacker schickten einen Block mit Scrypt-Algorithmus, der einen gefälschten Zeitstempel enthielt, gefolgt von einem Block mit Lyra2re-Algorithmus, der einen gefälschten Zeitstempel enthielt, und durch die Wiederholung dieses Prozesses und die damit verbundene Verringerung der Schwierigkeit konnten die Hacker mehrere Blöcke pro Minute abbauen (Ocminer 2018b).

Am 16. Mai 2018 wurde Bitcoin Gold von einem unbekannten Hacker angegriffen, der es schaffte, über 388.000 BTG von

Kryptowährungsbörsen zu stehlen, die Münzen waren während des Angriffs 17,5 Millionen Dollar wert (Roberts 2018).

NiceHash bietet derzeit mehr als genug Hash-Power zur Miete, um eine Reihe von kleinen bis mittleren Kryptowährungen anzugreifen. Der Begriff "Nicehashable" wurde für die Möglichkeit geprägt, Hash zu mieten, um eine Münze anzugreifen. Es existieren bereits Webseiten, um die Hacking-Möglichkeiten zu präsentieren (EXAKING 2018).

Sapling Integration and Aktivierung

Sapling Integration

Die Integration von Sapling in die Piratenkette war ein Erfolg dank der Zusammenarbeit zwischen den Mitgliedern des Komodo-Ökosystems, mit einem besonderen Dank an Mike Toutonghi vom Veruscoin-Projekt.

Pirate steht für schnelle, billige und 100% private Transaktionen und Sapling ist die beste Version der zk-SNARKS-Technologie, die das bietet. Aus diesem Grund ist der Einsatz von Sapling ab dem 15. Februar 2019 gezwungen, um sicherzustellen, dass die Kette effizient und privat funktioniert. Benutzer, die Pirate (ARRR) besitzen, müssen ihre Münzen vor diesem Datum von ihren Sprout-Adressen zu den Sapling-Adressen migrieren.

Das Timing des Hardforks für die Aktivierung von Sapling basierte auf einem Blockzeitstempel um den 15. Dezember, 1:00 AM UTC. Die Frist für die Migration von Sprout nach Sapling wurde auf den 15. Februar 2019 festgelegt, um ein Gefühl der Dringlichkeit zu schaffen und alle, die Pirate besitzen, einzubeziehen. Je früher die Migration abgeschlossen ist, desto besser ist die Situation für zentrale Vermittlungen und andere Drittanbieteranwendungen.

Eine dezentrale App (dApp) namens "zMigrate", die die Gelder des Benutzers in Sprout-Adressen automatisch in eine Sapling-Adresse umwandelt, wurde von *jl777c* entwickelt, um den Migrationsprozess nach Sapling zu optimieren. Alle Knoten wurden benötigt, um diesen Prozess bis zum 15. Februar 2019 abzuschließen, und Pools machten ebenfalls den Sprung zu den Sapling-Adressen nach der harten Arbeit.

Die Migration zu Sapling

Die dApp **zMigrate** ist ein eigenständiges Programm, das mit dem Daemon "Komodod" interagiert. Die dApp sendet den Pirate-Coin in der Sprout-Adresse(n) des Benutzers an eine einmalig verwendete, zufällige, transparente Adresse in Höhe von maximal 10.000 Pirate (ARRR) pro Transaktion. Es werden beliebig viele einmalige t-Adressen angelegt, um alle Gelder zu verschieben, wobei die letzte Transaktion wahrscheinlich weniger als 10K enthält (es sei denn, die Gelder sind durch 10K teilbar). Folglich werden die Gelder von jeder t-addr an die angegebene geschirmte Adresse von Sapling geschickt. Auf diese Weise hat der Nutzer die gesamte Zeit die Kontrolle über die Gelder und die Bewegung transparenter Gelder wird so homogen wie möglich aussehen, um den Schaden an der Fungibilität der Kette zu reduzieren. Das Ergebnis des Prozesses ist, dass alle Gelder des Benutzers von der alten Sprout-dresse auf seine bevorzugte Sapling-Adresse übertragen werden.

Die technischen Verbesserungen von Sapling ermöglichen die Entwicklung der folgenden Merkmale:

- Point-of-Sale Integration
- Hardware Wallets
- Web Shop Plugins (Fast)
- Mobile Wallets durch Aktivierung der Simple Payment Verification (zSPV) (in Entwicklung)

Emissions-Schema und technische Merkmale

Die Piratenkette enthält die folgenden technischen Merkmale und Merkmale nach dem 15. Dezember:

- Mining Algorithmus: Equihash Proof-of-Work
- Delayed Proof-of-Work (verzögerter Arbeitsnachweis)
- Blockzeit: 60 Sekunden
- Transaktionsgebühr: 0.0001 ARRR
- Transaktionssignierung in Sekundenschnelle
- Transaktionen pro Sekunde: 50–80 TPS
- Senden an bis zu 100 Adressen in einer einzigen Transaktion
- Tx-Größen von +- 2000 Bytes mit max. 200 kB
- Speicherbedarf von nur 40 MB (Raspberry Pi)
- Blockgröße von maximal 4 MB max.
- Anzeigen von Keys, die die Möglichkeit bieten, alle gesendeten Transaktionen einer zugewiesenen Adresse anzuzeigen.
- Möglichkeit, eine "endlose" Anzahl von "Lite"-Wallets

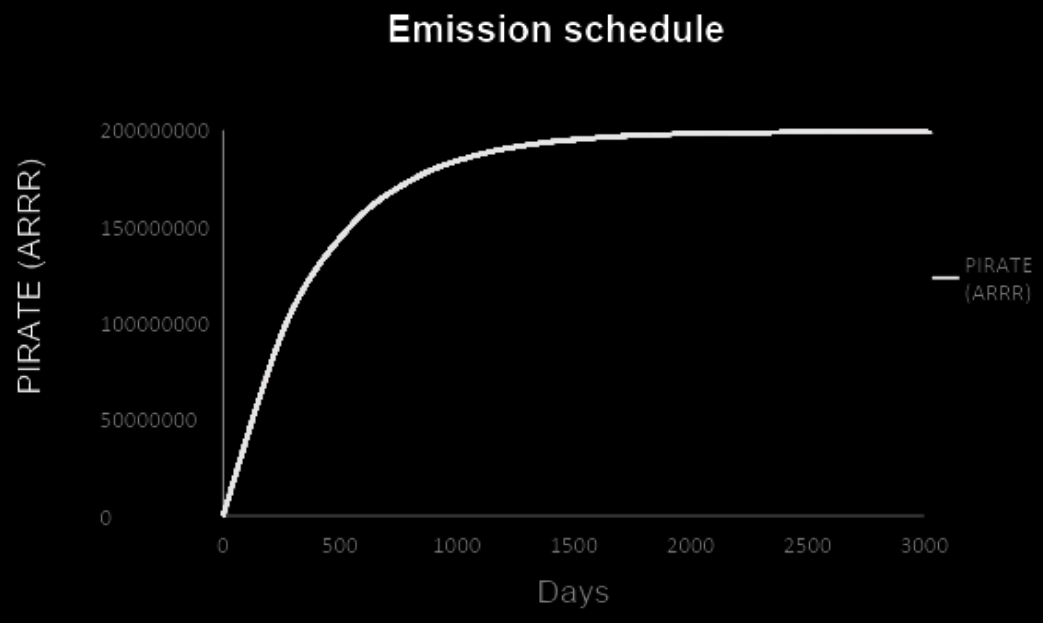

Abbildung 4 ***Der Emissionsplan von Pirate (ARRR)***

Alle 388885 Blöcke gibt es ein halbes Event bei den Blockbelohnungen, was etwa 270 Tage pro Belohnungszeitraum entspricht. Die Versorgung ist auf rund 200 Millionen Pirate (ARRR) begrenzt.

TOR-Unterstützung

Es ist möglich, die Piratechain über das TOR-Netzwerk zu betreiben und Ihre IP-Adresse zu verschleieren. Eine Zahl, die mit Ihrem geografischen Standort verbunden ist. Als Benutzer benötigen Sie einen TOR-Browser und die Komodo-Binärdateien, um die Piratenkette ausführen zu können. Eine Schritt-für-Schritt-Anleitung ist unter pirate.black verfügbar. Die TOR Supportanfrage wurde mit Agama Wallet Entwicklern geteilt. Einmal erledigt, ist die Einrichtung von Tor für eine Coin oder Asset-Kette sehr einfach.

Unterstützung für zentralisierte Börsen

Die Community war sich nicht sicher, ob ein zentralisierter Austausch in der Lage sein würde, Pirate zunächst zu akzeptieren, da es an transparenten Adressen fehlte. Kurz nach der Gründung von Pirate hat Pirate mit Exchange-Entwicklern und Codern zusammengearbeitet, um die Verwendung von Ein- und Auszahlungen mit Z-Adressen als Weltneuheit zu erleichtern. Diese spezielle Börse ist DigitalPrice und hat Ende Oktober 2018 erfolgreich den Handel aufgenommen.

Roadmap

Die Daten der folgenden Pirate-Features und Entwicklungen von Drittanbietern (wie Tortuga) sind Schätzungen, die auf vierteljährlicher Basis erstellt und in der Reihenfolge der Erwartungen aufgelistet werden.

- TOR Browser Support — Q3 2018 (Complete)
- 100% Z-address payout mining pools — Q3 2018 (Complete)
- Erster Z-addressen Discord Tipbot — Q3 2018 (Complete)
- Ermöglichgung z-Adresse auf einer CEX — Q3 2018 (Complete)
- Paper Wallet — Q4 2018
- Website Rebrand — Q4 2018
- Onboarding referrals — Q4 2018
- Pirate Lotterie Bot — Q4 2018
- Sapling — Q1 2019 (Complete)
- Pirate Foundation — Q1 2019
- Tortuga (CEX) — Q1 2019
- Z Simple Payment Verification (zSPV) — Q2 2019
- Hardware Wallet Integration — Q3 2019

Der Pirate-Leitfaden

An Board von Pirate kommen

Kaufen Sie einfach und sicher kleine Mengen von ARRR:

https://dexstats.info/onboarding.php

Wie minen?

Berechnen Sie Ihren geschätzten Gewinn:

https://dexstats.info/piratecalc.php

Mine Pirate mit ASIC/GPU:

https://medium.com/piratechain/how-to-mine-pirate-step-by-step-with-gpu-s-4c98f3dbcf5e

Mine Pirate ohne ASIC/GPU (Miete)

https://medium.com/@flexatron/how-to-mine-pirate-arrr-without-owning-an-expensive-rig-b8c26e409ae5

Behalte die PIRATE Hash-Rate im Auge:

https://dexstats.info/piratehash.php

Kaufe und handele mit PIRATE

Registriere Dich auf DigitalPrice und trade ARRR für BTC, ETH oder KMD:

https://digitalprice.io/?inviter=4fdaf7 (Offizieller PIRATE Ref-Link)

Soziale Medien

Pirate ist aktiv auf Bitcointalk, Discord, Medium, Reddit, SteemIt, Telegram, Twitter und auf der Coin Statistik-Website CoinPaprika gelistet.

https://coinpaprika.com/coin/arrr-pirate/

https://discord.gg/mBZhZgz

https://medium.com/@piratechain

https://www.reddit.com/user/piratechain

https://steemit.com/@piratechain

https://twitter.com/PirateChain

https://t.me/piratechain

https://bitcointalk.org/index.php?topic=4979549.0

Deutschsprachige Community

Die deutschsprachige Pirate-Community gehört zu den größten und aktivsten und ist online auf folgenden Portalen zu finden.

https://medium.com/@seko1900 (Medium)

https://t.me/GermanPirate (Telegram)

https://twitter.com/PiratechainDE (Twitter)

Source Code und Wallets

Github: https://github.com/PirateNetwork

Agama Wallet: https://github.com/KomodoPlatform/Agama/releases

PIRATE GUI Wallet: https://github.com/leto/TreasureChest

Quellen

Bowe, S. 2017. “Cultivating Sapling: Faster zk-SNARKs--Zcash Blog”. *Zcash Blog*.

EXAKING. 2018. “PoW 51% Attack Cost”. 2018. https://www.exaking.com/51.

Grewal, Satinder. 2018. “Satinder’s notes on the PIRATE chain”. 2018. https://blog.komodoplatform.com/pirates-of-komodo-platform-cdc991b424df.

Hopwood, Daira, Sean Bowe, Taylor Hornby, en Nathan Wilcox. 2016. “Zcash protocol specification”.

Japparova, Irina, en Ramona Rupeika-Apoga. 2017. “Banking Business Models of the Digital Future: The Case of Latvia”. *European Research Studies* 20 (3A). Professor El Thalassinos: 846.

Jl777c. 2016. “Delayed Proof of Work (dPoW) Whitepaper”. Github. 2016. https://github.com/KomodoPlatform/komodo/wiki/Delayed-Proof-of-Work-(dPoW)-Whitepaper.

Kappos, George, Haaroon Yousaf, Mary Maller, en Sarah Meiklejohn. 2018. “An Empirical Analysis of Anonymity in Zcash”. *arXiv preprint arXiv:1805.03180*.

Komodostats. 2018. “Asset Chains Notarizations Summary”. 2018. https://komodostats.com/acs.php.

Lee, James. 2018. “Komodo: An Advanced Blockchain Technology, Focused on Freedom.” Komodo. 2018.

Moser, Malte. 2013. “Anonymity of bitcoin transactions”.

Nakamoto, Satoshi. 2008. “Bitcoin: A peer-to-peer electronic cash system”. Working Paper.

Ocminer. 2018a. “Network Attack on XVG / VERGE”. Bitcointalk. 2018. https://bitcointalk.org/index.php?topic=3256693.0.

———. 2018b. “Network Attack on XVG / VERGE (Page 57)”. Bitcointalk. 2018. https://bitcointalk.org/index.php?topic=3256693.msg38135174#msg38135174.

PTYX. 2018. “What is a Parallel Chain (Asset Chain)?” Komodo Platform. 2018. https://komodoplatform.atlassian.net/wiki/spaces/KPSD/pages/71729160/What+is+a+Parallel+Chain+Asset+Chain.

Quesnelle, Jeffrey. 2017. “On the linkability of Zcash transactions”. *arXiv preprint arXiv:1712.01210*.

Roberts, Jeff John. 2018. “Bitcoin Spinoff Hacked in Rare ‘51% Attack’”. FORTUNE. 2018. http://fortune.com/2018/05/29/bitcoin-gold-hack/.

Saberhagen, Nicolas Van. 2013. “CryptoNote v 2.0”.

Sasson, Eli Ben, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, en Madars Virza. 2014. “Zerocash: Decentralized anonymous payments from bitcoin”. In *2014 IEEE Symposium on Security and Privacy (SP)*, 459–74.