DAPSCOIN

DECENTRALIZED-ANONYMOUS-PAYMENT-SYSTEM

WHITEPAPER 2019

«Privatsphäre ist ein Recht, kein Privileg»

Einleitung

DAPS ist eine geplante Blockchain mit dem Schwerpunkt auf Sicherheit, Skalierbarkeit und absoluten Datenschutz. Das DAPS Protokoll hat zum Ziel, einen vollständig anonymisierten Coin zu erschaffen und damit die Infrastruktur für ein Bezahlsystem mit zuverlässiger Verwaltung zu ermöglichen. Der Code basiert auf den neuesten Technologien von Monero und PIVX. **DAPS Blockchain Verifikation und Consensus basieren auf den PoS Nodes (Staking und Masternodes) sowie Proof of Audit (PoA) Miners.** In der Krypto-Welt stellt das ein Alleinstellungsmerkmal dar.
In erster Linie haben wir einige bereits in der Praxis bewährte Protokolle zusammengeführt. Diverse Eigenschaften dieser Protokolle ermöglichen ein neuartiges und 100% anonymes Blockchain-Netzwerk. Wir bauen das bisher umfassendste Privacy-Paket, mit einer On-Chain-Lösung für das "Vertrauensproblem", welches den Aufbau eines komplett anonymen Netzwerks bis dato verhindert hat. Unsere Lösung heißt **Proof of Audit** und ist der Grundstein des DAPS Protokolls.
Diese Basis ermöglicht es, Vermögenswerte zuverlässig zu anonymisieren und stellt die Infrastruktur für die Entwicklung zukunftsweisender Technologien dar. Datenschutz ist ein Recht und kein Privileg.

DAPS ist stolz verkünden zu können, dass es zum Zeitpunkt des Niederschriebs dieses Whitepapers, kein anderes Projekt erfolgreich geschafft hat, eine hybride Blockchain (PoW – PoS – PoA) mit der vollständigen Integration von RingCT und Bulletproofs zu implementieren.

Warum DAPS?

Ursprüngliche, sowie teilanonymisierte Blockchains sind der Öffentlichkeit zugänglich. Dadurch lassen sich Bewegungsprofile und Analysen ableiten, welche wiederum Missbrauch ermöglichen. Wir sind bestrebt, das Recht aller zu wahren, ihre Finanzen nach eigenem Ermessen zu kontrollieren und dadurch das Recht auf Anonymität und selbstbestimmte Datenpreisgabe durchzusetzen. DAPS wird erfolgreich getestete Datenschutzprotokolle zusammenführen, um die bisher anonymste Blockchain zu erstellen.

Entstehung des HARPOCRATES (DAPS) Protokolls

Das Zerocoin-Protokoll (libzerocoin) ist die Grundlage für viele der heute existierenden Privacycoins. Durch den breiten Einsatz ist dieses Protokoll bereits gründlich getestet und bietet einen relativ hohen Standard zur Implementierung von Datenschutz. Ein nennenswertes Beispiel für die Umsetzung der Zerocoin-Protokoll-Idee (libzerocoin) ist DASH.

Das DASH Team hat eine neue Ebene namens „Masternode“ erschaffen. Sie bietet Anreize für einen 24/7 Betrieb von Netzknoten und ist von großer Bedeutung für ein zuverlässiges Netzwerk. Darüber hinaus wird das Hinzufügen von neuen Funktionen („chain-features“) ermöglicht. Dazu gehören „Instantsend“ und „Privatesend“, ebenso wie eine Möglichkeit für Masternodes über Vorschläge abzustimmen und damit dezentral Entscheidungen bzgl. der weiteren Entwicklung zu treffen.

PIVX hat das Zerocoin-Protokoll mit dem Masternode-Protokoll zusammengeführt. Dabei wurde dieses Konzept erweitert, indem das "see-saw-reward-scheme" für Masternodes eingeführt wurde. Folglich konnten die Anreize für Masternodes gegenüber dem Staking deutlich ausgeweitet werden.

Bezogen auf Protokolldefinitionen eines dezentralen, anonymen Zahlungsschemas, beschrieben von Sasson et al (2014), ermöglicht diese Zahlungsmethode den Nutzern direkte und anonyme Zahlungen untereinander, wobei Herkunft und Ziel der Zahlung, ebenso wie der Betrag selbst verborgen bleiben. Dieser Ansatz verwendet “zero-knowledge-proofs“, wodurch das Analysieren von Transaktionen und Adressen verhindern wird.

Eine weitere Methode, die sich als äußerst robust und erfolgreich erwiesen hat, ist RingCT, wie es von Monero implementiert wurde. Nachfolgend finden Sie einen Auszug und einen Link.

"Eine naheliegende Möglichkeit, die Nachteile des CryptoNote-Protokolls zu überwinden... wäre die Implementierung versteckter Beträge für jede Transaktion.”

Shen Noether, Ring Signature Confidential Transactions for Monero]

Das Bitcoin Problem

Bitcoin ist nicht anonym. Durch das Konzept zur Vermeidung von Mehrfachausgaben ist die Blockchain vollständig öffentlich und für jeden einsehbar. Bitcoin ist „trustless“, was bedeutet, dass kein Vertrauen zu einem Bitcoin-Knotenbetreiber oder einer Person (z.B. welche Ihnen Bitcoin schickt) vorausgesetzt sein muss. Der Status der Bitcoin Blockchain kann mittels Werkzeugen überprüft werden. Salden und Transaktionen können in einem öffentlichen Verzeichnis eingesehen werden.
Dieses Vorgehen sichert die Netzwerkqualität und /-integrität. Weil Analysen und Tracking möglich sind, geschieht dies auf Kosten der Endanwender. Völlige Transparenz bringt auch immer die Möglichkeit von Missbrauch mit sich.
Vor diesem Hintergrund ist die Idee einer anonymen Blockchain zu einem Schwerpunkt der Branche geworden.

Anonymität und Sicherheit

Privacy Währungen sind nicht vollständig anonym. Auf absolut anonymen Blockchains, unabhängig der eingesetzten Protokolle, können Knoteninhaber theoretisch missbräuchlich agieren. Dies kann in vielerlei Hinsicht katastrophal für das entsprechende Netzwerk sein und stellt ein eingebautes Sicherheitsrisiko dar. Solch ein verstecktes Zusammenwirken von Knoten könnte bspw. für eine unendliche Erzeugung von Münzen ausgenutzt werden.
Weil solche Angriffe nicht einfach "zurückgesetzt" werden können, ohne dabei eine Abspaltung von Blockchains zu verursachen, ist es enorm wichtig, Angriffe oder Absprachen umgehend zu erkennen.
Wie überprüft man den Status eines Netzwerks, wenn Personen, die einem den Status mitteilen, Anreiz haben, unehrlich zu sein?
Die meisten Entwicklerteams meiden die Idee von privaten Blockchains aufgrund der inhärenten Ausnutzbarkeit. Diese Tatsache wird durch die Unfähigkeit verursacht, den Netzwerkstatus und die Emissionen mit Hilfe eines neutralen Dritten überprüfen zulassen. Das prominenteste Beispiel für diese kritische Schwäche ist die ständige Ausnutzung von "Zerocoin-Minting" und CryptoNote-Netzwerken.

Was ist das „Vertrauensproblem“?

Um vertrauenswürdig zu sein, muss ein objektiver Dritter in der Lage sein, die Münzversorgung und die Münzemissionen zu überprüfen und sicherstellen, dass die Knoten nicht missbraucht werden. Blindes Vertrauen in die Knotenbesitzer darf nicht der einzige Schutz vor missbräuchlichen Handlungen sein.

Bei Masternode-basierten, anonymen Blockchains muss diesen Masternodes als zentrale Steuerung der Münzversorgung, der Inflation und verschiedener Spezifikationen ein gewisses Maß an Vertrauen entgegengebracht werden. Andere anonyme Blockchains (ohne Masternodes) verwenden ZK-Snarks mit einer komplizierten „Bereitstellungs-Zeremonie“. Dabei sind gewisse Kontrollinformationen eines Netzwerks einer kleinen Gruppe von Mitgliedern zugänglich. Wenn diese Informationen nicht komplett gelöscht werden, könnten diese Mitglieder ein Netzwerk vollständig kontrollieren und manipulieren.
Genau das ist das "Vertrauensproblem". Es muss Knoten oder einer Gruppe von "Administratoren" Vertrauen entgegengebracht werden, welche theoretisch das gesamte Netzwerk nach Belieben steuern können. Aktuelle Iterationen von Masternodes und vollständig anonymen Blockchains (ZK-Snarks, RingCT mit voller Verschleierung) weichen vom "vertrauenswürdigen" Status öffentlicher Blockchains ab.

Viele nicht anonyme Kryptowährungen ignorieren diese Verwaltungsstrukturen völlig. Diese Tatsache widerspricht der ursprünglichen Vision von dezentraler Organisation, weil es eine oder wenige Autorität/en im Netzwerk besteht/en. Das ist gefährlich für die Blockchain-Industrie als Ganzes und verzerrt die Prinzipien von Satoshi. Keine von Menschen gemachte schriftliche Verfassung, Vereinbarung oder Abmachung kann jemals so sicher sein wie die Grundlage eines von Dritten gesicherten Blockchain-Ledgers.
Wie werden wir diese Probleme lösen? Mit dem Proof-Of-Audit wird absolutes Vertrauen in die Systematik anonymer Kryprowährungen eingeführt. Dies ermöglicht die Bereitstellung von vollständig anonymen Blockchains mit derzeit verfügbaren Tools und kann auf viele vorhandene Netzwerke ausgedehnt werden.

Was zeichnet uns aus?

Die Idee des Proof-Of-Audit und die Implementierung des DAPS-Protokolls heißt HARPOCRATES Protokoll und wird sich zu einem neuen Industriestandard entwickeln.
Folgende Schlüsseltechnologien finden dabei Verwendung:

- **Ring CT**
- **Bulletproofs**
- **Stealth Addresses**
- **Stealth Transactions**
- **Proof of Audit**

Wir bewirken eine vollständige Verschlüsselung aller Benutzer und Transaktionen. Dieser Funktionsmix mit Proof-of-Audit - welches wir "The Harpocrates Protocol" nennen - schafft ein absolut vertrauenswürdiges, anonymes Blockchain-Netzwerk.

DAPS Übersicht

DAPS ist ein hybrides PoW-PoS-PoA (Proof-of-Audit) Blockchain-System, das sich auf die Privatsphäre seiner Nutzer konzentriert und folgende, einzigartige Eigenschaften bietet:
1. Ein datenschutzorientiertes Blockchain-System, welches sicherstellt, dass jede Benutzertransaktion im Netzwerk privat bleibt. Das bedeutet, dass, obwohl alle Benutzertransaktionen vollständig an die Blockchain übermittelt werden, niemand außer dem Sender und dem Empfänger der Transaktion, die Detailinformationen einsehen kann.
Insbesondere folgende Informationen werden im DAPS-System vertraulich behandelt:
- Sender: Der Absender der Transaktion ist vollständig verborgen
- Empfänger: einmalig generierte öffentliche Schlüssel in der Transaktion können nicht von Dritten zur Identitätsfeststellung des Transaktionsempfängers bzw. zur Offenlegung der Beziehung zwischen dem öffentlichen Schlüssel und des Empfängers herangezogen werden
- Der Transaktionsbetrag ist so verschlüsselt, dass kein Dritter die Transaktionsdetails offenlegen kann
2. Ein hybrides System, welches aus unterschiedlichen Block Typen auf einer Blockchain zusammengeführt wird.
- Die ersten 500 Blöcke sind vom Typ PoW und werden durch die DAPS Stiftung zur Sicherstellung der Erstversorgung geschürft
- Ab dem 501 Block wandelt sich die DAPS-Blockchain in einen Hybrid aus PoS und PoA um
- Um Transaktionen von Benutzern der DAPS-Blockchain zu erleichtern, werden durch kontinuierlich erzeugte PoS-Blöcke Stakes geprägt und damit der Betrieb der Nodes vergütet. Jede Minute wird ein PoS-Block erstellt
- PoA Blöcke haben eine Dauer von einer Stunde. Sie werden durch externe Akteure geschürft und stellen die Funktionstüchtigkeit des Systems durch Auditierung sicher.

DAPS COIN KONSENS MECHANISMEN: MASTERNODES, STAKING-NODES UND PROOF-OF-AUDIT

DAPS-Masternodes müssen über 1.000.000 DAPS als Sicherheit verfügen und eine dedizierte IP-Adresse bereitstellen. Sie müssen 24 Stunden am Tag, mit einer maximalen Ausfallzeit von einer Stunde, laufen können. Wie im nächsten Abschnitt beschrieben, werden Masternodes anhand der „See-saw“ Methode vergütet. Für ihren Dienst für das Netzwerk erhalten Masternodes einen Teil der Blockbelohnungen, um das Ökosystem aufrechtzuerhalten. Diese Zahlung erfolgt in DAPS und dient den Masternode-Besitzern als passives Einkommen.

Das DAPS-Masternode-System ist dem PIVX-Masternode-System nachempfunden. Damit sind viele Vorteile verbunden, einschließlich der Verhinderung eines 51% Angriffs, sofern nicht sowohl „Proof of Stake“ als auch „Masternode-Layer“ gleichzeitig kompromittiert werden.

Das SBRS-System (See-Saw Balance Reward System) hat eine 60/40 MN / PoS Belohnungsaufteilung mit einem Maximum von 40/60 MN / PoS. Dies ist eine angemessene Belohnung für Teilnehmer.

Die Blockchain Verifizierung wird mit Proof of Audit, Masternodes und Proof of Stake (v3) durchgeführt. Dieses Verfahren gibt dem DAPS Netzwerk Widerstandsfähigkeit gegenüber den meisten bekannten Angriffen und gewährleistet Sicherheit, während es öffentlich überprüft werden kann.

Obwohl DAPS vertrauenswürdig ist, braucht es dennoch ein zusätzliches Vertrauenselement. Masternodes werden auf jeder Masternode Chain als Vertrauensinstanz betrachtet. Das liegt unter anderem daran, dass eine Sicherheit für den Betrieb einer Masternode hinterlegt werden muss. Weil DAPS standardmäßig anonym und mit verschleierten Transaktionen ausgestattet ist, kommt es an der Stelle zu einem Problem, wie diese hinterlegte Sicherheit nachgewiesen bzw. bestätigt werden kann.

Aus diesem Grund ist jede Transaktion, die als hinterlegte Sicherheit dienen soll, weder verschleiert, noch Bulletproofed, noch Teil einer Ring Signatur.

Sobald die hinterlegte Sicherheit eines Masternodes aufgelöst bzw. bewegt wird, entsteht eine normale Transaktion zur entsprechenden Wallet.

OBLIGATORISCHE VERSCHLEIERUNG

DAPS hat eine eingebaute Verschleierung des Adresssystems und alle transferierten Beträge sind verschlüsselt. Während eine Transaktion erzeugt wird, generiert der Sender einen öffentlichen Schlüssel über die UTXO. Dieser wird dann für die Erstellung eines einmalig verwendbaren öffentlichen Schlüssels herangezogen (entsprechend einer Bitcoin Adresse). Der private Schlüssel des letzteren wird anschließend durch den Empfänger der Transaktion abgeleitet, welcher die privaten Ausgaben-/ und Betrachtungsschlüssel besitzt. (Darauf wird noch näher eingegangen)
Transaktionsbeträge werden mit einem symmetrischen Verschlüsselungsschema kodiert, das eine elliptische Kurve Diffie Hellman ECDH zur Verschlüsselung verwendet. Die Entschlüsselung kann nur durch Sender und Empfänger der Transaktion erfolgen. Der öffentliche Transaktionsschlüssel erlaubt es dem Empfänger (Erzeuger des privaten Schlüssels) den Betrag dieser Transaktion zu kennen. Die vergebenen Schlüssel sind einmalig und gebunden an eine spezifische Transaktion.

EMISSIONEN

Die DAPS Coin Emissionen werden 1050 DAPS pro Block betragen. Es wird eine Gebühr von 50 DAPS pro Block (Gründergebühr) dem DAPS Entwicklungsfond zur Verfügung gestellt, welcher zur Weiterentwicklung und langfristigen Unterstützung des Projekts verwendet wird.
Gebührenstruktur im Detail:

1050 Emissionen pro PoS Block
50 Gründergebühr
900 Aufteilung zwischen Staking Nodes und Masternodes (60/40 = 540/360)
100 reserviert für PoA Miner

Das “See-Saw Balance Reward System” ist eine geeignete Methode um die Netzwerk Balance zwischen Stacking-Nodes und Masternodes abzubilden und die Entlohnung entsprechend zu verteilen. 1000 MN und 1000 Staking-Nodes werden vom System als gleichwertig angesehen und das 60/40 See-Saw-System angewendet. Die höhere Gewichtung des Masternodes ist durch die hinterlegte Sicherheit von 1 Million DAPS begründet.
Wenn die Anzahl der Masternodes im Verhältnis zu den Staking Nodes deutlich ansteigt, wird die Gleichung zu Gunsten der Staking Nodes (max. 40/60) angepasst.
Indem der Anreiz gesteuert wird, balanciert dieses System den Betrieb von Masternodes und Staking Nodes aus und trägt damit zur langfristigen Stabilität des Netzwerks bei.

DAPS TOKEN SPEZIFIKATIONEN

ERC-20 Token
Max. Umlauf (Supply): 60,000,000,000 DAPS
Verteilung (Contribution): über AIRDROP

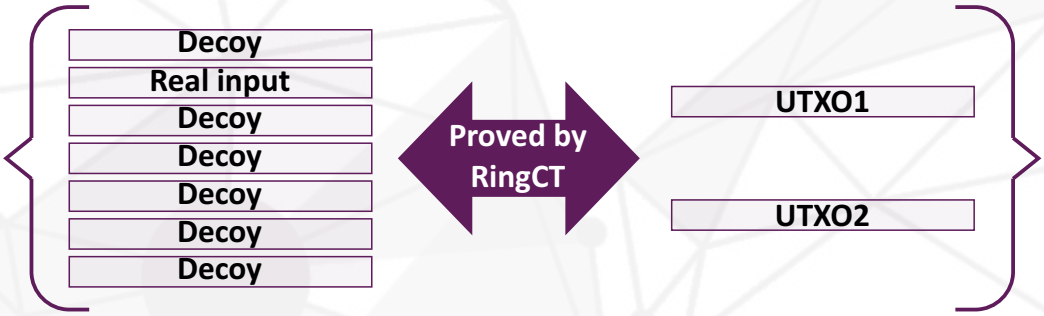
DAPS COIN SPEZIFIKATIONEN

Ursprünglicher Umlauf (Initial supply): 60,000,000,000 DAPS
Kapitalisierung des Umlaufs (supply cap): 60,000,000,000 [initial]+10,000,000,000 [block reward] DAPS
Consensus: Proof-Of-Audit, Proof-Of-Stake v3, Masternodes (See-saw rewards)
Datenschutz-Technologien (Privacy Techniques): Secp256k1-based Ring Signature, RingCT, and range proof Bulletproof
Blockzeit (Block time): 1 Minute
Blockbelohnung (Block reward): vgl. Emissionen
Notwendige Bestätigungen (Confirms required to spend): 4 blocks
Stake Reifedauer (Stake maturation): 100 blocks
Erwartete Emissionen (Approximate emissions): ~551 Millionen DAPS pro Jahr, bis 10 Milliarden DAPS emittiert wurden

DAPS CHAIN SPEZIFIKATIONEN:

RINGCT

RingCT „Ring Confidential Transaction“ bietet die Möglichkeit des „mixing“. Dies geschieht mit einer vorgegebenen Anzahl von „fake Transaktionen“, während einer tatsächlichen Transaktion. Dabei legt die Ringgröße die Anzahl der hinzugefügten „fake Transaktionen“ fest.
Der transferierte Betrag ist wesentlich schwerer zu erkennen, sobald die tatsächliche Transaktion in einer Gruppe von „fake Transaktionen“ versteckt ist.
Während Monero mit einer vorgegebenen Ring Größe (derzeit 11) arbeitet, wird die Ring Größe bei jeder DAPS Transaktion zufällig generiert (6-12). Dieses Vorgehen bewirkt zusätzliche Sicherheit, weil die Rückverfolgbarkeit durch Benutzergewohnheiten stark eingeschränkt wird.
Die Ring-Signatur versteckt die echten UTXO's und erkennt gleichzeitig Mehrfachausgaben, wodurch Nodes prüfen und nachweisen können, dass die ein- und ausgegangenen Summen übereinstimmen. Das ist von enormer Bedeutung für DAPS, weil alle Transaktionsbeträge standardmäßig verschleiert sind. Sie existieren lediglich als „Pederson commitments“ und in verschlüsselter Form. Eine Entschlüsselung ist an dieser Stelle nicht notwendig.



DAPS CHAIN SPEZIFIKATIONEN:

BULLETPROOFS

Bulletproofs sind kurze, lineare „zero-knowledge proofs", die keine besonders gesicherte Umgebung voraussetzen. Bulletproofs können zur Überprüfung des richtigen Aufbaus von verschlüsseltem Klartext herangezogen werden. Beispielsweise kann nachgewiesen werden, dass sich eine verschlüsselte Zahl in einem bestimmten Bereich befindet. Im Vergleich zu SNARKs benötigen Bulletproofs keine vertrauenswürdige Umgebung. Die Verifizierung eines Bulletproofs ist jedoch zeitaufwendiger als die eines SNARK-Proofs.
Bulletproofs wurden entwickelt, um effiziente anonymisierte Transaktionen in Bitcoin und anderen Kryptowährungen zu ermöglichen. Vertrauliche Transaktionen verschleiern den Transaktionsbetrag. Jede dieser verschleierten Transaktionen enthält einen kryptografischen Nachweis, dass sie valide ist. Bulletproofs reduzieren die Größe des kryptografischen Proofs von über 10kB auf weniger als 1kB. Darüber hinaus unterstützen Bulletproofs die Bündelung von Nachweisen. Es tragen nur gültige zusätzliche Elemente zur Größe eines einzelnen Nachweises bei. Wenn alle Bitcoin Transaktionen durch Bulletproofs verschleiert wären, hätte die Blockchain eine ungefähre Größe von 17 GB, im Vergleich zu über 160 GB durch aktuell genutzte Verfahren.

DAPS nutzt die Eigenschaft von Bulletproofs um festzustellen ob der gesendete Betrag positiv ist. Das ist entscheidend, weil secp256k1 mit „circle space number" arbeitet und ein Netzknoten keine Möglichkeit hat, einen verschlüsselten Betrag als positiv zu bestätigen. Wenn diese Überprüfung durch Bulletproofs nicht stattfindet, ist die Blockchain angreifbar. Theoretisch kann dann ein Angreifer eine Transaktion mithilfe der UTXO generieren, welche einen großen positiven Betrag aufweist, während die andere UTXO einen negativen Betrag darstellt. Die Differenz dieser beiden Beträge plus Transaktionsgebühren entspräche dann der Summe der Eingänge. Als Resultat würde die RingCT Prüfung umgangen.

DAPS CHAIN SPEZIFIKATIONEN:

MASKIERTE ADRESSEN

„Maskierte Adressen“ gehört genauso wie maskierte Transaktionen zu den tragenden Säulen der DAPS Blockchain.

Normale Adressen sind relativ leicht zu lesen und zu identifizieren; z.B.
3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy
Maskierte Adressen von DAPS sind außergewöhnlich. So sieht ein Beispiel einer öffentlichen DAPS Adresse aus:
41k8JcYj2EG4eDHbpPNneDdKvFqHFpQNMMGykRUorNnihiY4RaRNdLiUUfThfzugo5auHkq
ThwQgZ3EixmxyoDkj17c7Qy6BVWP
Wir bezeichnen sie als „Private Benutzerkonten“.
Manch einer könnte argumentieren:
Wie wird Anonymität garantiert, wenn die Adresse öffentlich ist?
Auf der DAPS Blockchain wird die öffentliche Adresse des Empfängers genutzt, um öffentliche Einwegadressen bzw. Schlüssel zu generieren. Diese basieren auf dem öffentlichen Schlüssel der durch den Sender ausgelösten Transaktion.
Die Besonderheit dieses Schemas besteht darin, dass der Absender beim Erzeugen dieses einmalig generierten öffentlichen Schlüssels keine Möglichkeit hat, den entsprechenden privaten Schlüssel anzufertigen, um diesen später zu verwenden. Ein solcher privater Schlüssel kann nur vom Besitzer der öffentlichen Adresse abgeleitet werden, der beide privaten Schlüsselpaare in unserem „Dual-Key-System“ hat (siehe unten).

ÖFFENTLICHE DAPS ADRESSEN MIT DUAL-KEY SYSTEM

DAPS verwendet ein Dual-Key-System, um maskierte Adressen bereitzustellen, welche die eigentlichen Adressen verschleiern. Eine öffentliche Adresse wird aus einem Schlüsselpaar der anonymen Ansicht abgeleitet. Eine öffentliche Adresse kann optional eine Zahlungskennung enthalten, die normalerweise von Börsen verwendet wird.
DAPS verwendet die EC secp256k1 Kurve, um öffentliche Schlüssel aus entsprechenden privaten Schlüsseln abzuleiten.

Field	Description
Header	1-byte length. Header = 19 if it is an integrated address, otherwise Header=18
Public spend key	Public spend key in compressed form, whose length is 33 bytes.
Public view key	Public view key in compressed form, whose length is 33 bytes.
paymentID	8-byte field used by exchanges for recognizing transactions from different users
Checksum	4 first bytes of the hash of the above fields

DAPS CHAIN SPEZIFIKATIONEN:

Die öffentliche Adresse wird im base58 Format für jeden 8-Byte Block der öffentlichen Adresse folgendermaßen kodiert:
- Normale öffentliche Adressen: 71 Bytes, aufgeteilt in acht 8-Byte Blöcke und einen einzelnen 7-Byte Block. Jeder Adressblock ist im base58 Format kodiert, was zu 11 base58 Zeichen pro Adressblock führt -> 99 base58 Zeichen
- Integrierte Adresse: 79 Bytes, aufgeteilt in neun 8-Byte Blöcke und einen einzelnen 7-Byte Block, was zu 110 base58 Zeichen führt

MASKIERTE TRANSAKTIONEN

Um eine vollständig anonyme Transaktion durchführen zu können, sollte die öffentliche Empfänger Adresse an den Absender übermittelt werden. Dessen Wallet führt dann folgende Schritte durch:

- Um die „public view key Pv“, „public spend key Ps“, und „payment ID“ (optional) zu extrahieren, wird die öffentliche Adresse analysiert
- Es wird geprüft, ob diese Adresse ausreichend Guthaben zum Versenden aufweist
- Für die Empfänger Adresse wird ein öffentlicher Einweg-Schlüssel generiert
  - Erzeugung eines privaten Transaktionsschlüssels Ts und des dazugehörigen öffentlichen Transaktionsschlüssels Tp
  - P = H(Ts*Pv) * G + Ps wobei
    - H eine Hash Funktion darstellt
    - * und + sind die Multiplikation und Addition in der secp256k1-Kurve
    - G ist der Ausgangspunkt in der secp256k1-Kurve
  - Pro Transaktionsvorfall wird ein öffentlicher Einweg- und ein privater Schlüssel generiert, um Schwierigkeiten mit Ring Signaturen zu vermeiden (siehe unten)
- Die Sender Wallet erzeugt einen Transaktionsvorfall an das identische, oben genannte Ziel des öffentlichen Einweg-Schlüssels inklusive dem angemeldeten Betrag
  - Erstellung eines Pederson-Commitments für den Transaktionsvorfall
  - Generierung einer elliptischen Kurve Diffie Hellman mit ECDHS secret
  - Verschlüsselung des Transaktionsausgangsbetrages mit diesem ECDHS secret
  - Erzeugung eines Bulletproofs für den Transaktionsausgangsbetrag
- Auswahl eines Satzes von verfügbaren UTXO als Transaktionseingaben
  - Berechnung der zu erwartenden Transaktionsgebühr
  - Berechnung der Änderung = Summe der Transaktionseingaben - gesendeter Betrag – Transaktionsgebühr
  - Festlegung der tatsächlichen Transaktionsgebühr
  - Erzeugung von Schlüsselabbildungen und Integration in die Transaktionseingabe
- Erstellung Ring Signatur
  - Erzeugung der zufälligen Anzahl von Ringen (Ringgröße 6-12)
  - Auswahl von Ringgrößen Attrappen für jeden Transaktionseingang
  - Berechnung der Multikey-Ringsignatur basierend auf RingCT und Ringsignatur

DAPS MASTERNODES UND STAKING

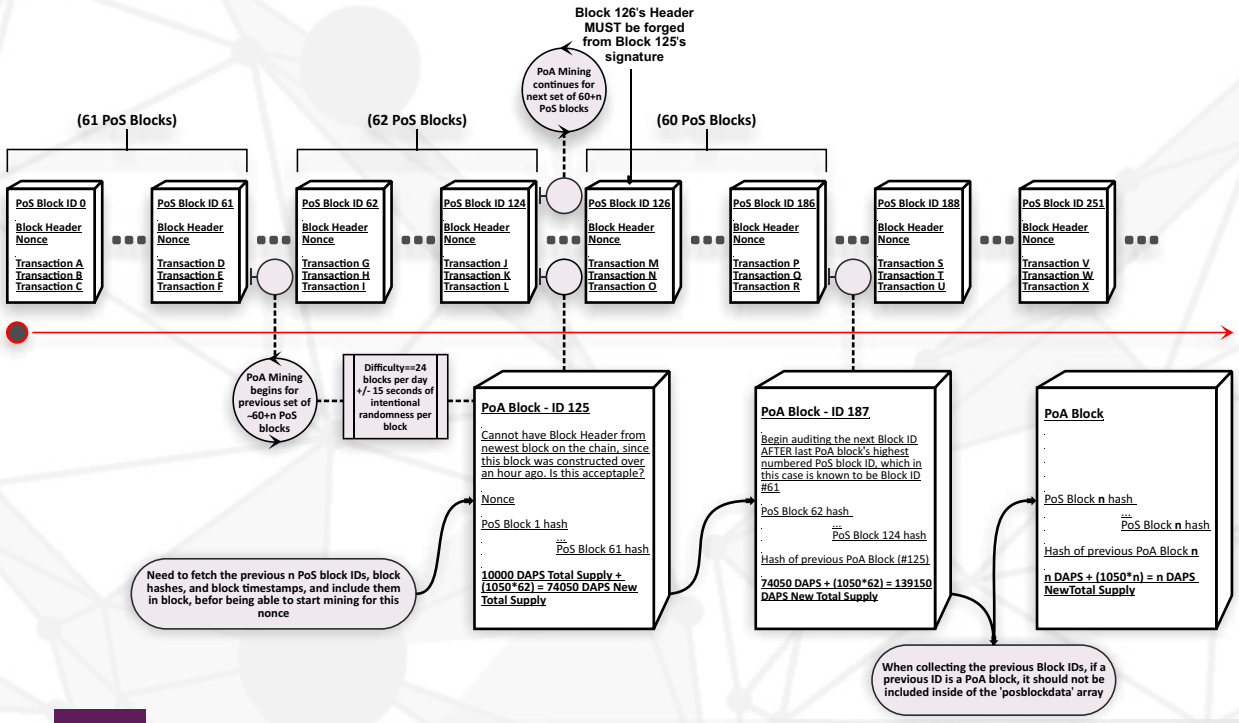
In Systemen wie PIVX werden Masternodes für die Bereitstellung zusätzlicher Dienste wie "Instant Send" entlohnt, indem die Vergütung der Adresse zugutekommt, welche die hinterlegten Coins (collateral) enthält. Ein solcher Mechanismus würde bei DAPS zum Verlust der Masternode Vergütung führen, weil die Transaktion aufgrund der zwei unterschiedlichen UTXOs von einer identischen Adresse durch Ring Signaturen als Doppelausgabe gewertet wird. Das bedeutet, dass nur eine der Masternode UTXO-Belohnungen eingelöst werden kann, sofern sie an die gleiche Adresse gesendet werden.
Der DAPS Anreizmechanismus für den Betrieb von Masternodes ist so konzipiert, dass für jede Entlohnung eine neue Adresse / ein öffentlicher Schlüssel generiert wird. Dies gelingt DAPS, indem es von den Benutzern verlangt, die öffentliche Adresse (die lange Adresse) bei der Sicherung (collateral transaction) zu hinterlegen. Die öffentliche Adresse des Masternodes wird in die Zahlungswarteschleife eingereiht. Während ein PoS-Block erstellt wird, nimmt eine Staking-Node eine der öffentlichen Adressen aus der Warteschlange und führt mithilfe eines einmalig erzeugten öffentlichen Schlüssels die Masternode Zahlung (Entlohnung) durch. Dadurch wird sichergestellt, dass alle Masternode UTXO-Belohnungen ausgeführt werden können.
Dieser Mechanismus kommt auch bei den Staking-Nodes zum Tragen. Während der Erzeugung von PoS-Blöcken, wird sichergestellt, dass alle Staking-Belohnungen über unterschiedliche öffentliche Schlüssel gesendet werden.

POA UND POS CONSENS MECHANISMUS DETAILS

1. Kein PoA-Block darf in die Kette aufgenommen werden, es sei denn, seit dem Zeitstempel des zuvor angenommenen PoA-Blocks sind mindestens 59-60 Minuten vergangen. Dadurch soll sichergestellt werden, dass ausgeschlossene PoA Blöcke keines Falls auf die Blockchain gelangen und diese unendlich fortschreiben.
2. Ein PoA-Block muss den Hash des vorherigen PoA-Blocks enthalten und bildet so eine durchgehend verbundene Kette von PoA-Blöcken.
3. Ein PoA-Block darf keinen PoA-Hash, die Höhe oder den Zeitstempel eines anderen PoA-Blocks in seinem eigenen „posblocksaudited“ Bereich aufnehmen.
4. Jeder Block-Hash, der in „posblocksaudited“ aufgenommen wird, muss aus einem gültigen PoS-Block stammen, welcher derzeit auf der Chain zu sehen ist.
5. Jeder Block-Zeitstempel, der in „posblocksaudited“ aufgenommen wird, muss aus einer Zeit stammen, die vor dem eigenen Zeitstempel des PoA-Blocks liegt. Kein PoA-Block darf zukünftige PoS-Blöcke auditieren.
6. Ein PoA-Block darf keinen PoS-Block-Hash auditieren, den ein anderer PoA-Block bereits auditiert hat.

Ein PoA-Block kann der Blockchain allzeit hinzugefügt werden. Dies ermöglicht den PoS-Blöcken eine ungehinderte Prozessfortführung und ein PoA-Block muss eine bestimmte Anzahl von existierenden fortlaufenden PoS-Blöcken auditieren. Dabei werden die PoS Block IDs + Block Hashes + Zeitstempel relational aufgezeichnet und nach Block-ID sortiert. Sobald sich der PoA-Block selbst der Blockchain hinzugefügt hat, ist der Prozess abgeschlossen und beginnt von vorn.

Zu erstellende PoA-Blöcke suchen nach der letzten PoA-Block-ID und darin nach der höchsten PoS-Block-ID. Anschließend beginnt der Auditprozess, wobei zu berücksichtigen ist, dass PoA-Block-IDs ignoriert werden.



«Privatsphäre ist ein Recht, kein Privileg»

TOR/OBFS4

In früheren Versionen dieses Whitepapers wurde die Verwendung von TOR und OBFS4 erwähnt. Nach eingehender Untersuchung wurde beschlossen, diese vorerst aus dem Technologie Paket auszuschließen. Die Gründe dafür sind einfach und doch maßgeblich.
TOR wird von vielen ISP's (Internetprovider) weltweit blockiert, was umfangreiche Einstellungen erfordert, um die Kommunikation zu "überbrücken". Das kann dazu führen, dass aufgrund einer zu hohen technischen Barriere viele Menschen DAPS nicht nutzen wollen oder können.
Eine weitere Problematik ist, dass einige dieser Provider bei Nutzung von TOR (unabhängig vom Hintergrund) - entweder die Person warnen, dies zu unterlassen, anderenfalls könnte ihr Konto geschlossen werden, oder einfach nur das Konto ohne Vorwarnung schließen. So oder so ist das schlecht und kann manchmal sogar mit einem Besuch von Strafverfolgungsbehörden enden. Das wollen wir unseren Nutzern nicht zumuten.
Wir beobachten TOR weiterhin aktiv und sind uns einig, dass die Technologie in einer zukünftigen Version "optional" implementierbar sein könnte.
Da „nur“ periphere Systeme TOR nutzen würden, muss die Kette dafür nicht zurückgesetzt, geteilt oder gespalten werden.

WEITERE EIGENSCHAFTEN

- Statische Emissionen: Keine ausgefallenen Inflationsmodelle, flache Emissionen
- Blockgröße bis zu 2MB
- Masternodes: Incentivierte 24/7 Nodes, welche erweiterte Funktionen zulassen
- Multinodes: Mehrere Masternodes pro Instanz. Kein Server-Spam mehr!

Mit den oben genannten Funktionalitäten erwarten wir, Transaktionen, Adressen, Salden und Nodes /IP Adressen vollständig verschleiern zu können. Mit einem integrierten Auditsystem „on chain“ wird das System „vertrauenslos“. Damit werden Probleme von anderen anonymen Coins vermieden. Diese einzigartige Verknüpfung von Eigenschaften (die auf einem Staking-Netzwerk basieren), wird als Harpocrates Protokoll bezeichnet und unserer Meinung nach, einen neuen Standard für Datenschutz setzen.
Darüber hinaus sind wir überzeugt, dass Proof-Of-Audit andere zeitgemäße Protokolle ergänzen und verbessern kann, sodass die Mission unseres Projekts für die gesamte Branche von Vorteil ist.

- DAPS Ökosystem & Welt: Es werden Initiativen ergriffen, um DAPS einer breiten realen Nutzung zu zuführen

ANMERKUNGEN:

Das vorliegende Dokument ist kein Prospekt. Es wurde 2019 zusammengestellt, um über das DAPS Projekt zu informieren. Beachten Sie, dass kein Kauf erforderlich ist. Es steht Jedem frei, an dem Projekt teilzunehmen oder nicht. Es liegt in Ihrer Verantwortung, die in Ihrem Land geltenden Gesetze zu überprüfen, bevor Sie DAPS kaufen oder anderweitig unterstützen. Sie müssen die Bedingungen dieses Dokuments lesen, verstehen und akzeptieren, bevor Sie sich in das Projekt einbringen.
Technische Daten und Informationen können sich ändern.
DAPS hat im ersten Halbjahr 2019 zwei erfolgreiche Testläufe durchgeführt.
DAPS wird vor dem Mainnet-Release einer Code-Überprüfung durch red4sec unterzogen.
Diese Übersetzung ins Deutsche ist nach bestem Wissen und Gewissen erfolgt. Maßgeblich ist das Original in englischer Ausführung.

DOKUMENTATION:

Bitcoin trustless

Z-cash Trust Problem

Libzerocoin Protocol

DAP Protocol, by Sasson et al

Masternodes

Masternodes

See-saw reward scheme

Posv3

Ring CT

Bulletproofs

Stealth Addresses