Loki

Private Transaktionen, dezentrale Kommunikation.

Kee Jefferys, Simon Harman, Johnathan Ross, Paul McLean

Version 3

July 13th 2018

Abstract

Loki ist ein hybrides Proof-of-Work / Proof-of-Service System und bietet dadurch eine einzigartige Möglichkeit, den Betrieb von Full-Nodes mit einem finanziellen Anreiz zu versehen (Incentivierung). Loki nutzt diese incentivierten Nodes, um auf einer zweiten Ebene eine private Routing Funktion zu erstellen und zu etablieren. Die minimale Node Funktionalität auf dieser zweiten Ebene wird durch eine neuartige Methode überwacht, die Schwarm Markierung genannt wird. Loki basiert auf einer modifizierten Version des Monero Quellcodes und stellt sicher, dass alle Transaktionen einen hohen Grad an Privatsphäre erreichen.

Dieses Whitepaper beschreibt die in Loki verwendete Technologie. Wir gehen davon aus, dass sich weitere Änderungen an dieser Technologie ergeben werden wenn Loki weiterentwickelt wird. Neue Versionen dieses Whitepapers werden zukünftig veröffentlicht, um wesentliche Änderungen und Aktualisierungen widerzuspiegeln.

1 Einleitung

Die Nachfrage nach Privatsphäre bei digitaler Kommunikation und Finanztransaktionen nimmt weltweit ständig zu, da Benutzerdaten gesammelt, verarbeitet und auf beispiellosem Niveau weiterverarbeitet werden. Nahezu sämtliche Daten eines Benutzer, wie personenbezogene Daten und E-Mail Inhalte die durchsucht werden, bis hin zu Kredit Score Werten und Ausgabengewohnheiten, werden gesammelt und zwischen den weltweit größten Unternehmen und staatlichen Akteuren verkauft. Loki's Ziel ist es, ein zensurresistentes Angebot von Tools und Werkzeugen zur Verfügung zu stellen, die es Benutzern ermöglichen privat zu handeln und zu kommunizieren.

Bitcoin wurde mit dem Versprechen einer hohen Privatsphäre lanciert, aber was daraus resultierte, ist eine höhere Rückverfolgbarkeit als jemals zuvor. Unternehmen wie Chainalysis und

BlockSeer nutzen Bitcoins transparente Blockchain Architektur, um bestimmte Transaktionen nachverfolgen zu können [1]. Loki wurde auf Basis von Monero heraus entwickelt, einer Kryptowährung, die sich bis heute als eines der sichersten privaten Transaktionsnetzwerke etabliert hat [2]. Jedoch hat Monero auch Nachteile. Monero Transaktionen sind erheblich größer als Bitcoin Transaktionen und unterliegen erheblichen Anforderungen an Bandbreite, Verarbeitung und Speicherplatz. Wenn das Netzwerk wächst, führt dies zu einer erheblichen Belastung für die Betreiber von Monero Nodes und bietet keinen finanziellen Anreiz zum Betrieb oder Ausbau dieser. Dies macht den Betrieb zu einer kostspieligen und oft undankbaren Aufgabe. Die Einführung eines ökonomischen Anreizes zum Betrieb eines Nodes, hier Service-Nodes genannt, wird dies ändern.

Service-Nodes können auch verwendet werden, um eine Vielzahl unterschiedlicher datenschutzbasierter Funktionen bereitzustellen, wenn sie angemessen ökonomisch vergütet werden. In erster Linie ermöglicht das Service-Node Netzwerk Benutzern, Datenpakete anonym zu übertragen und zu empfangen. Diese private Kommunikation wird erleichtert, indem jeder Service-Node als Relais in einem neuartigen Sybil Attacke resistenten Mixnet arbeitet, der ähnliche Eigenschaften wie Tor und I2P [3][4] aufweist. Darüber hinaus soll dieses Kommunikationsnetzwerk als Rückgrat für einen dezentralen und Ende-zu-Ende verschlüsselten Messaging Dienst mit dem Namen Loki Messenger dienen, der es Benutzern ermöglicht, direkt und ohne Vertrauen auf in dritte Partei zu kommunizieren. Voraussetzung hierfür ist, dass beide Parteien gleichzeitig online sind.

Loki ist nicht nur eine Plattform für den privaten Austausch von Nachrichten, sondern ebenso eine Plattform für dezentrale und anonyme Internetdienste.

2 Grundparameter

Loki difficulty target (blocktime)	120 Seconds
Difficulty algorithm	Zawy LWMA [5]
Hashing algorithm	CryptoNight Heavy
Elliptic curve	Curve25519 [6]

3 CryptoNote Elemente

Obwohl bei allen Kryptowährungen ein finanzielles Anreizsystem zum Betrieb von Full-Nodes implementiert werden könnte, verwendet Loki den Monero Quellcode wegen seines hohen Grades an Datenschutz, der den Transaktionen zur Verfügung steht. Monero ist eine Weiterentwicklung des CryptoNote Protokolls, das Ring-Signaturen, Stealth Adressen und RingCT verwendet und Benutzern die Möglichkeit gibt, Transaktionen zu signieren und zu verschleiern, während die Plausibilität beibehalten wird [7].

Damit das Loki Ökosystem die Privatsphäre ebenso wahren kann, ist es wichtig, nicht nur ein Austauschmedium zu schaffen, das die interne Ökonomie unterstützt, sondern auch das Risiko zeitlicher Analysen zu minimieren, wenn Interaktionen auf Loki's unabhängiger Ebene stattfinden. Wenn Sie beispielsweise mit Transaktionsdiensten der ersten Ebene arbeiten, sollten Benutzer niemals die Garantie auf Datenschutz verlieren, die sie von der zweiten Eben erhalten und umgekehrt.

3.1 Ringsignaturen

Ringsignaturen arbeiten so, dass sie einen Ring von möglichen Unterzeichnern für eine Transaktion konstruieren, bei der nur einer der Unterzeichner der tatsächliche Absender ist. Loki verwendet Ring Signaturen, um die wahre Historie der Transaktions Outputs zu verschleiern. Ring Signaturen sind für alle Loki Transaktionen obligatorisch (mit Ausnahme der Block Reward Transaktionen). Auf der Loki Blockchain wird eine feste Ringgröße von zehn erzwungen. Dies bedeutet, dass jede Eingabe von einer von zehn möglichen Outputs ausgegeben werden könnte, einschließlich der tatsächlichen Ausgabe (siehe 6.3).

3.2 Stealth Adressen

Loki verwendet Stealth Adressen, um sicherzustellen, dass der wahre öffentliche Schlüssel des Empfängers niemals mit seiner Transaktion verknüpft ist. Jedes Mal, wenn eine Loki Transaktion gesendet wird, wird eine einmalige Stealth Adresse erstellt und das Geld an diese Adresse gesendet. Unter Verwendung des Diffie-Hellman Schlüsselaustausches kann der Empfänger der Transaktion einen privaten Ausgabeschlüssel für diese Stealth Adresse berechnen und dadurch das Eigentum an den Geldern übernehmen, ohne seine wahre öffentliche Adresse preisgeben zu müssen [8]. Stealth Adressen bieten Empfängern von Transaktionen Schutz und sind ein zentrales Datenschutzmerkmal in Loki.

3.3 RingCT

RingCT wurde zuerst vom Monero Research Lab als eine Möglichkeit vorgeschlagen, Transaktionsbeträge zu verschleiern [9]. Aktuelle Implementierungen von RingCT verwenden rangeproofs, die Pedersen-commitments nutzen, um zu beweisen, dass der Betrag einer gesendeten Transaktion zwischen 0 und 2^{64} liegt. Ebenso wird sichergestellt, dass keine negativen Beträge der Währung gesendet werden, ohne den tatsächlich gesendeten Betrag der Transaktion anzuzeigen. In letzter Zeit wurde von einer Reihe von Kryptowährungen vorgeschlagen, Bulletproofs als Ersatz für traditionelle range-proofs in RingCT einzuführen, da die Transaktionsgröße erheblich reduziert würde [10]. Loki wird Bulletproofs verwenden, um die Informationen zu reduzieren, die Nodes speichern und weiterleiten müssen, um die Skalierbarkeit zu verbessern.

4 Service Nodes

Obwohl Loki eine Vielzahl von Optimierungen zusätzlich zum CryptoNote Protokoll implementiert (siehe 7) hat, wird ein großer Teil der Netzwerkfunktionalität und Skalierbarkeit von Loki durch eine Reihe von Nodes mit finanziellem Anreiz, so genannte Service-Nodes, ermöglicht. Um einen Service-Node zu betreiben, sperrt ein Betreiber eine signifikante Menge von Loki Coins für eine bestimmte Zeit und stellt dem Netzwerk ein Mindestmaß an Bandbreite und Speicher zur Verfügung. Als Gegenleistung für diesen Dienst erhalten Betreiber von Loki Service-Nodes einen Teil des Block Rewards von jedem gefundenen Block.

Das entstehende Netzwerk bietet marktbasierte Resistenz von Sybil Attacken um eine Reihe von Problemen mit bestehenden Mixnets und datenschutzorientierten Diensten zu lösen. Diese Widerstandsfähigkeit basiert auf Interaktionen zwischen Angebot und Nachfrage, die

dazu beitragen zu verhindern, dass einzelne Akteure einen ausreichend großen Anteil an Loki haben, um eine negative Auswirkung auf die Datenschutzdienste der zweiten Ebene, die Loki bietet, zu haben. Die Kryptowährung DASH stellte zunächst die Theorie auf, dass Sybil Attacke resistente Netzwerke aus der Crypto Ökonomie abgeleitet werden können [11]. Wenn ein Angreifer Loki akkumuliert, verringert sich das frei verfügbare Angebot, was wiederum Druck auf die Nachfrageseite ausübt und den Preis von Loki erhöht. Wenn dies fortgeführt wird, wird es immer teurer, zusätzliche Loki Coins zu kaufen, was den Angriff zu teuer macht.

Um diesen marktbasierten, wirtschaftlichen Schutz zu erreichen, fördert Loki die aktive Festsetzung des zirkulierenden Angebots. Insbesondere müssen die Emissionskurve und die Anforderungen an das Mindestkapital so gestaltet sein, das sichergestellt ist, dass das zirkulierende Angebot reduziert ist und angemessene Renditen für die Betrieb der Service-Nodes bereitgestellt werden, um Sybil Angriffe abwehren zu können.

4.1 Block Reward

Die Verteilung des Block Rewards in Loki erfolgt durch Proof-of-Work, ein sicheres und etabliertes System für die Erstellung von Blöcken und die Verarbeitung von Transaktionen. Miner sammeln und schreiben Transaktionen in Blöcke und erhalten dafür Transaktionsgebühren. Als eine Konsens Regel in Loki enthält jeder Block mehrere Rewards, von denen nur einer an den Miner geht.

Mining Reward:
Zusätzlich zu den Transaktionsgebühren, werden 45% des Block Rewards an den Miner vergeben der den Block erstellt.

Service Node Reward:

Der zweite Teil in jedem Block, 50% des Block Rewards, wird an einen oder zwei Service-Nodes gesendet, wenn dieser als Relais betrieben wird (siehe 6.3). Service-Nodes werden zeitbasiert vergütet. Dies bedeutet, dass derjenige Service-Node, der die längste Zeit keine Vergütung erhalten hat, den nächsten Reward am wahrscheinlichsten erhält. Jedes Mal, wenn sich ein Service-Node im Netzwerk registriert, übernimmt er die letzte Position in der Warteschlange. Wenn der Service-Node einen guten Service bereitstellt und nicht durch die Schwarm Markierung aus der Warteschlange geworfen wird (siehe 7.3), klettert dieser langsam zu den höheren Positionen in der Warteschlange herauf. Nodes, die durch ihre hohe Position vergütet wurden, fallen anschließend wieder auf die letzte Position zurück und durchlaufen den beschrieben Prozess erneut.

Governance Reward:
Der letzte 5% Anteil des Block Rewards verteilt sich auf Governance Operationen (siehe 9); 3,75% wird an die Adresse der Loki Stiftung gesendet, die deterministisch aus jedem Block abgeleitet werden und die verbleibenden 1,25% gehen an den „funding block“ (siehe 9.2.3).

4.2 Verifizierbare Kapitalanforderung

Service-Nodes müssen dem Netzwerk beweisen, dass sie das erforderliche Mindestkapital besitzen. Datenschutzmerkmale die dem Design von Loki innewohnen machen dies schwierig,

insbesondere weil es nicht möglich ist, dass Guthaben einer öffentlichen Adressen zu prüfen oder mit ViewKeys zu verifizieren.

Loki nutzt neuartige zeitgesteuerte Outputs, mit denen Loki Coins zeitlich fixiert bzw. festgesetzt werden können, bis die Blockchain eine vorher definierte Blockhöhe erreicht hat. Bis zu dieser definierten Höhe macht das Loki Netzwerk Versuche unmöglich, diese zeitverriegelten Outputs auszugeben. Loki verwendet diesen Prozess um sicherzustellen, dass ein bestimmter Service-Node tatsächlich das verlangte Mindestkapital hinterlegt hat und dieser nicht für andere Service-Nodes verwendet werden kann.

Um sich als Service-Node zu registrieren, erstellt der Betreiber einen zeitgesteuerte Output der erforderlichen Menge and Coins, die nach Ablauf von mindestens 21.600 Blöcken (etwa 30 Tagen) wieder entsperrt werden. Ein zusätzliches Feld in der Transaktion enthält die Adresse des Service-Node Betreibers, der den Service-Node Reward erhalten soll. Diese Adresse wird auch als öffentlicher Schlüssel für den Betrieb des Service-Node verwendet, der auch der Schwarm Markierung unterliegt. Wallets verwenden hier nicht die Ausführung der Transaktion als Mixins, da ihre tatsächlichen Beträge und ihr Ziel offengelegt werden und es nicht erforderlich ist, diese Transaktionen anonym zu halten.

Bevor ein Node dem Service-Node Netzwerk beitritt, müssen andere Nodes einzeln validieren, dass das hinterlegte Kapital der Mindestsumme gemäß der Anforderungen entspricht. Da die Kapitalanforderungen nach 30 Tagen ablaufen und ein neues Staking erfolgen kann, verfügt die Wallet über eine automatische Wiederholung für diese Staking Transaktion.

5 Lokinet

Das Onion-routing-Protocol ermöglicht es Benutzern, Tunnel oder Pfade durch ein verteiltes Netzwerk zu bilden, wobei mehrere Nodes als mögliche Absprünge verwendet werden können, um das Ziel und den Ursprung von Datenpaketen zu verschleiern. Service-Nodes im Loki Netzwerk arbeiten mit einem On-Board-Routing-Protokoll mit niedriger Latenz und bilden ein vollständig dezentrales Netzwerk mit dem Namen Lokinet. Das Netzwerk ist nicht auf vertrauenswürdige Institutionen angewiesen und sein Status ist vollständig von der Blockchain abgeleitet. Benutzer können sich mit einzelnen Service-Nodes verbinden und bidirektionale Pfade für Datenpakete erstellen, die durchgeleitet werden sollen. Das Netzwerk kann für den Zugriff auf intern gehostete Dienste mit dem Namen SNApps verwendet werden (siehe 6.2). Ebenso können Benutzer die Service-Node-Exit-Funktionalität verwenden, um das externe Internet zu durchsuchen, ohne dass ihre IP-Adresse offengelegt wird (siehe 6.3).

5.1 Low Latency Anonymous Routing Protocol (LLARP)

Allen Anwendungen für Service-Nodes liegt ein anonymes Routing Protokoll zugrunde, das definiert, wie jeder Service-Node mit seinen Partnern kommuniziert. Loki schlägt ein neues Routing Protokoll namens LLARP [12] vor, dass als Hybrid zwischen Tor und I2P entworfen wurde, um zusätzliche wichtige und wünschenswerte Eigenschaften gegenüber jedem bisher existierenden Routing Protokoll bereitzustellen. LLARP wurde speziell dafür entwickelt, auf dem Loki Service-Nodes Netzwerk zu laufen und alle LLARP Optimierungen berücksichtigen diese Architektur. Um die Ziele von LLARP zu verstehen, ist es am besten, eine Analyse bestehender Routing Protokolle durchzuführen und darzulegen, wie LLARP diese verbessert.

The Onion Router (Tor)

In den letzten Jahren war Tor das beliebteste anonyme Mixnet. Das Tor Netzwerk hat einen hohen Zensurwiderstand und hat sich als wertvolles Instrument zur Wahrung der Privatsphäre im Internet erwiesen. Tor ist jedoch kein dezentrales, sondern ein hierarchisches Netzwerk. Tor ist auf eine Gruppe von Verzeichnissen angewiesen, bei denen es sich um zentralisierte Server handelt, die von einer Gruppe von freiwilligen die der Tor Stiftung nahestehen betrieben werden [13]. Diese autoritären Verzeichnisse führen zwei Hauptfunktionen aus. Erstens fungieren sie als vertrauensvolle Reporte für den Status von Nodes im Netzwerk. Wenn ein Tor-Benutzer (oder Relais) sich zum ersten Mal mit dem Netzwerk verbindet, kann er sich mit einem von zehn fest codierten autoritären Verzeichnissen verbinden. Diese stellen dem Benutzer oder Relais eine Datei zur Verfügung, die als Konsens bezeichnet wird. Diese Datei enthält eine Liste aller zurzeit im Tor Netzwerk vorhandenen Relais, überwachende Nodes und Exit Nodes (mit Ausnahme von Brücken). Zweitens messen die autoritären Verzeichnisse auch die Bandbreite, die jedes Relais dem Netzwerk bereitstellen kann. Sie verwenden diese Informationen, um Relais in Kategorien einzuteilen und zu entscheiden, ob Nodes als Relais, Security Nodes oder Exit Node agieren können.

Diese hohe Zentralisierung führt zu Schwachstellen, die Tor verwundbar machen. Im Jahr 2014 erhielt Tor Informationen über eine glaubwürdige Bedrohung, die zum Ausschalten einer signifikanten Menge von Verzeichnisservern führen könnte[14]. Würden die Verzeichnisserver in den Vereinigten Staaten und entweder in Deutschland oder in den Niederlanden abgeschaltet, würde das ausreichen, um fünf der zehn Verzeichnisserver herunterzufahren. Dies würde zu einem sehr instabilen Tor Netzwerk führen, wobei neue Relais stark in ihrer Fähigkeit beeinträchtigt werden, mit dem Netzwerk zu interagieren.

Die Kommunikationsmöglichkeiten in Tor sind ebenfalls begrenzt, da Tor nur die Kommunikation über TCP erlaubt. IP über Tor ist möglich, aber es fehlt eine Unterstützung für UDP-basierte Protokolle (z. B. VoIP).

Invisible Internet Project (I2P)

I2P verfolgt eine andere Herangehensweise an die Mixnet Architektur, indem es sich auf eine Distributed Hashing Table (DHT) bezieht, um den Netzwerkzustand anstelle der Verzeichnisserver zu ermitteln [15]. I2P ermöglicht auch sowohl TCP als auch UDP-Datenverkehr und unterstützt einen größeren Bereich von Protokollinteraktionen. I2P hatte jedoch keinen stetigen Entwicklungsprozess und im Laufe der Zeit haben sich technische Versäumnisse aufsummiert, insbesondere in seiner kryptografischen Nutzung. I2P verwendet 2048 Bit ElGamal, was die Verschlüsselung und Entschlüsselung im Gegensatz zu elliptischen Kurven verlangsamt. Während in der I2P Roadmap Pläne zur Abkehr von ElGamal existieren, sind hier Fortschritte nur langsam vorangeschritten.

Darüber hinaus fehlt I2P die formale Unterstützung für Exit-Nodes, was bedeutet, dass der Großteil des Datenverkehrs im Netzwerk auf intern gehostete Websites namens Eepsites zugreift. Dies hat die Fähigkeit des I2P-Netzwerks reduziert, Benutzer anzusprechen, deren Hauptzweck die Verwendung von anonymisierten Netzwerken ist, um auf das breite Internet zuzugreifen.

Darüber hinaus bedeutet die Art und Weise, in der I2P aufgebaut wird, dass die Mehrheit der Benutzer, die sich mit dem Netzwerk verbinden, auch Router werden, was problematisch ist, da das Netzwerk oft nicht genügend Bandbreite hat um schnelle Pfade bauen zu können. Netzwerkgeschwindigkeiten in Mixnets werden durch den schwächsten teilnehmenden Node in jeder Schaltung vermindert. Als Ergebnis daraus, dass Benutzer mit niedriger Leistung

zu Relais in I2P werden, verringert sich wiederum die Gesamtleistung.

Schließlich unterscheidet sich I2P von Tor darin, dass es ein paketvermitteltes (statt leitungsvermitteltes) Netzwerk anbietet. Anstatt einen einzigen längerfristigen Tunnel einzurichten durch den der gesamte Verkehr verläuft, baut I2P mehrere Pfade auf, die jedes übertragene Paket verwenden kann, um eine andere Route durch das Netzwerk zu nehmen. Dies gibt I2P die Möglichkeit, Netzwerkstaus und Ausfälle von Nodes transparent umzuleiten.

Sowohl I2P als auch Tor können Sybil Attacken nicht vollständig mildern. Ein ausreichend motivierter Angreifer, der genug Zeit und Kapital hat um große Mengen an Relais zu kaufen, kann eine zeitliche Analyse durchführen, die die Privatsphäre der Benutzer untergräbt. Die Effektivität dieser Analyse erhöht sich, je mehr Exit-Nodes, Relais und Schutz-Nodes der Angreifer betreibt [16]. Tor und I2P werden ausschließlich von freiwilligen betrieben, die sowohl Zeit als auch Geld für den Betrieb von Nodes spenden. Wir nehmen an, dass ein Netzwerk, das aus finanziellen Anreizen und incentivierten Nodes besteht und nicht aus Altruismus heraus betrieben wird, eine größere Widerstandsfähigkeit gegen Angriffe erreichen und gleichzeitig einen zuverlässigeren Dienst bieten kann.

LLARP

LLARP arbeitet ohne die Verwendung von Verzeichnisservern und stützt sich stattdessen auf einen DHT, der aus Blockchain Staking Transaktionen aufgebaut ist, wodurch Service-Nodes als Router im Netzwerk fungieren können. Die Bandbreite wird im DHT nicht überwacht oder aufgezeichnet. Stattdessen resultieren Messungen zur Bandbreite und Triage aus Schwärmen (siehe 6.1.1), die jeden Node bewerten und eine Beurteilung vornehmen, ob Nodes dem Netzwerk eine ausreichende Bandbreite bereitstellen.

Im Open-Systems-Interconnection-Model (OSI-Modell) versucht LLARP nur, eine anonyme Netzwerk Ebene bereitzustellen. Dies bedeutet, dass es eine größere Auswahl an Internetprotokollen unterstützt und auch den Aufwand für das Speichern von Datei Deskriptoren minimiert, wenn Exit-Nodes den UDP-Datenverkehr (User-Datagram-Protocol) durchlaufen [17]. Darüber hinaus entscheidet sich LLARP für paketvermitteltes Routing anstelle von tunnelbasiertem Routing und ermöglicht so eine bessere Lastenverteilung und Redundanz im Netzwerk.

Von einem Endanwender von Lokinet wird nicht erwartet und es ist auch nicht erlaubt, selbst Datenpakte zu routen. Das bedeutet, dass Lokinet aufgrund des erheblichen Kapitalaufwands, der für den Start eines Service-Nodes erforderlich ist, einer wesentlich geringeren Angriffsfläche für eine Sybil Attacke ausgesetzt ist.

6 Loki Services

Ähnlich wie bei der Investition die Miner in Hardware tätigen, friert jeder Service-Node Betreiber Loki Coins als Mindestkapital zeitlich ein, sobald sie mit dem Betrieb eines Service-Nodes beginnen. Dieses festgelegte Kapital dient zwei Zwecken:

1. Jeder Service-Node Betreiber hat einen ausreichend großen Anteil am Erfolg des Netzwerks.Sollte ein Betreiber eines Service-Nodes dem Netzwerk eine schlechte Performance liefern oder unehrlich handeln, untergräbt und riskiert er eine Abwertung seines eigenen Anteils innerhalb des Netzwerks.

2. Es bietet die Möglichkeit einer aggressiveren Durchsetzung; Wenn das Netzwerk in der Lage ist, unehrliche Nodes wirksam daran zu hindern, ein Reward zu erhalten, müssen unehrliche Nodes die Opportunitätskosten sowohl des Verlustes des Rewards als auch der verbleibenden Sperrzeit für ihre Sicherheit tragen.

Setzen wir die oben genannten Annahmen als gegeben voraus und können wir aggressive Strafen für schlecht handelnde Nodes erzwingen (siehe 7.3), so können wir Gruppen von Service-Nodes erstellen die abgefragt werden, um über den Zustand der Blockchain zu einem Konsens zu kommen oder sie durch ein spezielles off-Chain Nodes Verhalten durchzusetzen (siehe Schwärme 6.1.1). In Loki bezieht sich dieses Verhalten sowohl auf Netzwerk- als auch auf Speicheraktivitäten. Loki Services kombinieren diese off-chain Aktivitäten, um das Back-End von Anwendungen für Benutzer zu sein, die diese Eigenschaften nutzen.

6.1 Loki Messenger

Der erste Loki Service, der im Loki Netzwerk entwickelt und implementiert wird, ist eine dezentralisierte, Ende-zu-Ende verschlüsselte Anwendung für private Nachrichtenübermittlung namens Loki Messenger.

End-to-End Anwendungen für verschlüsselte Nachrichten, die eine Plattform für Benutzer zum Senden von Nachrichten ohne deren Inhalt bereitstellen, sind bereits vorhanden. Sie basieren jedoch auf zentralisierten Servern, die gezielt gesteuert, blockiert und heruntergefahren werden können [18][19]. Diese zentralisierten Dienstmodelle stellen ein hohes Risiko für die Anonymität der kommunizierenden Parteien dar, da sie häufig erfordern, dass der Benutzer eine Telefonnummer oder andere identifizierende Informationen registriert und sich direkt über die IP-Adresse des Benutzers verbindet. Diese Information könnte von Servern durch Datenlecks oder legale Prozesse extrahiert und gegen den Benutzer verwendet werden. Durch die Nutzung der Service-Node Architektur im Loki-Netzwerk können wir einen Service anbieten, der gängige zentralisierte und verschlüsselten Messaging Apps wie Signal mit einem höheren Maß an Datenschutz- und Zensurresistenz bietet.

6.1.1 Messenger Routing

Das Nachrichtenrouting im Loki Netzwerk ändert sich je nachdem, ob der empfangende Benutzer online oder offline ist. Wenn beide Benutzer online sind, kann eine Kommunikation mit höherer Bandbreite stattfinden, da Nachrichten nicht auf den Service-Nodes gespeichert werden müssen.

In Loki agiert ein öffentlicher Schlüssel sowohl als langfristiger Schlüssel zur Verschlüsselung, als auch als Routing Adresse. Im einfachsten Fall sollte dieser Schlüssel out-of-band ausgetauscht werden, um einen Schutz vor einem Man-in-the-Middle Angriff zu gewährleisten. Ein solcher Austausch sollte entweder persönlich oder durch eine andere sichere Art des Austausches erfolgen (siehe 6.1.2).

Online Messaging

Sobald Alice Bobs öffentlichen Schlüssel kennt, geht sie davon aus, dass er online ist und versucht, einen Pfad zu ihm zu erstellen. Alice tut dies, indem sie den DHT eines beliebigen Service-Nodes abfragt und ein introduction set erhält, das dem öffentlichen Schlüssel von Bob entspricht. In LLARP führen introduction sets die introducer auf, die jeder Benutzer

führt. Durch diese introducer können Pfade eingerichtet werden. Mit dem introducer von Bob wählt Alice nun drei zufällige Service-Nodes aus, die als intermediary hops zwischen ihrer Herkunft und ihrem Ziel dienen (introducer von Bob). Es wurde nun ein Pfad festgelegt, über den Alice und Bob Nachrichten senden können. Wenn sie korrekt authentifiziert sind und OTR verwenden (siehe 6.1.2), können Alice und Bob nun kommunizieren, während sie ein hohes Maß an Privatsphäre genießen.

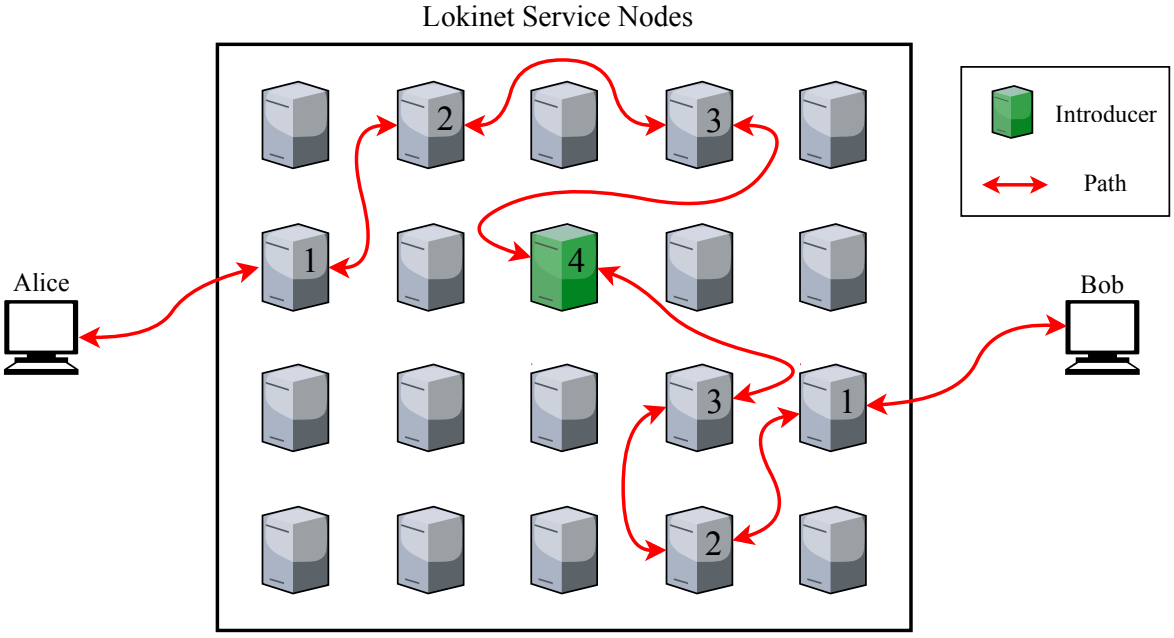

Abbildung 1: *Vereinfachte Darstellung des online Routing, in der Alice mit Bob unter Verwendung von zufälligen Service-Nodes Pfaden durch das Netzwerk kommuniziert.*

Offline Messaging

Wenn Alice keine Antwort von Bob erhält, kann sie den Offline-Messaging Prozess initiieren. Offline Routing verwendet eine modifizierte Version von Postal Services over Swarm (PSS) [20]. Schwärme sind logische Gruppierungen von Service-Nodes, die sowohl auf ihren öffentlichen Schlüsseln als auch auf dem Hash des Blocks beruhen, in dem ihre Staking Transaktion gültig wurde. Jeder Schwarm hat eine SchwarmID und besteht aus neun Nodes. Um eine Nachricht an Bob zu senden, kann Alice mit seinem öffentlichen Schlüssel berechnen, zu welchem Schwarm Bob gehört. Mit diesen Informationen kann Alice anonym eine Nachricht durch das Netzwerk an einen zufälligen Service-Node in diesem Schwarm weiterleiten. Wenn ein Service-Node eine eindeutige Nachricht empfängt, die für seinen Schwarm bestimmt ist, muss er diese Nachricht an die anderen acht Nodes im Schwarm verteilen. Alle Nodes müssen zusätzlich Nachrichten für ihre zugewiesene „Time-to-live“ (TTL) speichern (siehe 8.3). Wenn Bob online ist, kann er zwei beliebige Nodes in seinem Schwarm nach Nachrichten abfragen, die er entschlüsseln kann. Offline-Messaging ist vor Spamming mit einem kleinen Proof-of-Work geschützt, der jeder Nachricht angehängt ist (siehe 7.2).

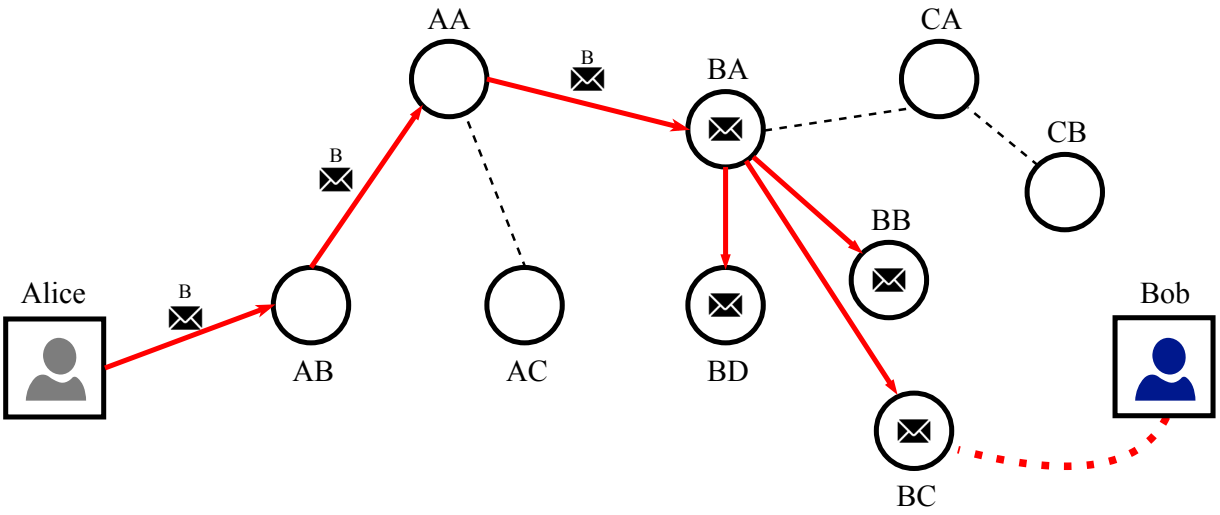

Abbildung 2: *Alice sendet eine Nachricht an Bob, Bobs zugehöriger Schwarm ist B. Wenn Bob wieder online ist, fragt er einen zufälligen Node in seinem Schwarm an und erhält Alices Nachricht*

6.1.2 Messenger Verschlüsselung und Authentifizierung

Sobald eine Nachrichtenkette eingerichtet ist, erzwingt der Loki Messenger Perfect Forward Secrecy (PFS) und Deniable Authentication (DA). PFS und DA sind Schlüsselkonzepte des OTR-Nachrichtenprotokolls [21]. Zentralisierte Dienste wie Signal und WhatsApp verwenden Verschlüsselungsfunktionen, die OTR-Schutz aufrechterhalten. Loki basiert seine OTR-Implementierung aus dem bestehenden Tox-Protokoll, einem verteilten Peer-to-Peer-Instant-Messaging-Protokoll, das die bereits of auditierte NaCl-Bibliothek verwendet [22].

PFS ermöglicht die Abwehr von Angriffen, bei denen ein Langzeitschlüssel verfügbar ist. Ein neuer gemeinsamer Schlüssel zur Verschlüsselung wird für jede Sitzung verwendet. Wenn also ein einzelner Sitzungsschlüssel offengelegt wird, wird nicht die gesamte Nachrichtenkette kompromittiert. Wenn ein Drittanbieter die Verschlüsselung einer Nachrichtenkette unterbrechen wollte, müsste er die Schlüssel für jede einzelne Sitzung in Erfahrung bringen. PFS stellt sicher, dass Loki Messenger im Vergleich zu bestehenden Methoden wie der Pretty Good Privacy (PGP) Verschlüsselung, bei der nur ein langfristiges Schlüsselpaar erforderlich ist um die gesamte Nachrichtenkette zu kompromittieren, äußerst sicher ist.

DA bezieht sich auf die Fähigkeit von zwei Parteien, sich gegenseitig zu beweisen, dass sie der tatsächliche Absender jeder neuen Nachricht sind. Ein Dritter kann jedoch nicht feststellen, wer der wahre Absender einer Nachricht ist. Bei Verwendung von DA werden nach jeder Sitzung Codes für die Authentifizierung von Nachrichten (MACs) veröffentlicht, so dass Dritte plausibel Nachrichten erstellen können, die so aussehen, als ob sie von der öffentlichen Adresse des Absenders stammen. Bei korrekter Implementierung ist es für Dritte damit nicht möglich zu beweisen, dass ein Absender einer bestimmten Nachricht der eigentliche Absender war.

Benutzer Authentifizierung

Die Authentifizierung von Benutzern ist wichtig, um einen Schutz vor Man-in-the-Middle-Angriffen zu gewährleisten. Wenn Bob beispielsweise eine Nachricht von Alice erwartet, aber noch nicht weiß, welches ihr öffentlicher Schlüssel ist, könnte eine Drittpartei (Eve) eine

Nachricht an Bob senden, der vorgibt, Alice zu sein. Aus diesem Grund sollten sich Benutzer gegenseitig authentifizieren, bevor sie persönliche Informationen weitergeben.

Wie Pidgin und andere OTR-Messaging-Dienste verwendet der Loki Messenger die Pre-Shared Key (PSK) Authentifizierung. Benutzer haben mehrere Optionen für die Einrichtung eines PSK. Sie können einen Out-of-Band-Schlüssel einrichten, oder alternativ sich auf einen PSK über Loki Messenger einigen. Möglich wird das über eine Frage, die kein Dritter kennt. Loki wird die PSK Authentifizierung basierend auf einer modifizierten Version des Pidgin Verfahrens zur verschlüsselten Authentifizierung implementieren [23].

6.2 SNApps (Service-Node Anwendungen)

Die Funktion von SNApps ähnelt den sogenannten versteckten Diensten in Tor. Sie bieten Benutzern die Möglichkeit, vollständig in der Mixnet Umgebung zu interagieren, was zu einer noch höheren Anonymität führt als beim Zugriff auf extern gehostete Inhalte. SNApps ermöglichen es Benutzern, Marktplätze, Foren, Whistleblowing Websites, soziale Medien und viele andere Internet Anwendungen auf ihren eigenen Computern oder Servern einzurichten und zu hosten, während die Anonymität auf der Server- und Benutzerseite erhalten bleibt. Dies erweitert den Umfang des Netzwerks erheblich und ermöglicht Benutzern, innerhalb von Lokinet sinnvolle Gemeinschaften zu bilden.

SNApp Betreiber verwenden das traditionelle Server-Client-Modell, wobei der Hauptunterschied darin besteht, dass Service-Nodes bei einer Benutzerverbindung über Lokinet als Vermittler fungieren. Wenn sich ein SNApp im Netzwerk registrieren möchte, muss es den DHT mit seinem Deskriptor aktualisieren. Dieser Deskriptor enthält verschiedene Introducer, bei denen es sich um spezielle Service-Nodes handelt, die Benutzer kontaktieren können, um einen Pfad zur SNApp zu erstellen. Wenn diese Pfade eingerichtet sind, können Benutzer sich mit der SNApp verbinden, ohne dass einer der Teilnehmer weiß, wo sich der andere im Netzwerk befindet.

6.3 Exit-Node

Exit-Nodes ermöglichen es Benutzern, Anfragen an das allgemeine Internet zu stellen und diese Anfragen über ein Mixnet zurückzugeben. Wenn sie ordnungsgemäß verwendet werden, können Benutzer über Exit-Nodes das Internet privat durchsuchen, ohne dass die IP Adresse des Benutzers dem Server zur Verfügung gestellt wird.

Obwohl der Betrieb von Exit-Nodes für den erweiterten Service von Loki sehr wichtig ist, könnte die Verpflichtung, dass jeder Service-Node als Exit-Nodes operieren muss, nachteilig sein. Die Verwendung als Exit-Node kann den Betreiber rechtlichen Risiken aussetzen, da Benutzer des Exit-Nodes bösartige Aktivitäten ausführen könnten, während sie ihn als Proxy verwenden. Da Exit-Nodes einfach Datenverkehr vom Internet an den Endbenutzer weiterleiten, erhalten Exit-Nodes häufig DMCA-Anforderungen (Digital Millennium Copyright Act) oder werden oft als die Quelle von Hacker Angriffen angesehen. Obwohl in den meisten Gerichtsständen die Betreiber von Exit-Nodes rechtlich geschützt sind, können Internet-Service-Provider, die Service-Node Datenverkehr durch ihre Server leiten, rechtliche Risiken befürchten und den Dienst für den Exit-Node sperren.

Beim Start wird einem Service-Node zunächst eine Relais Markierung zugewiesen und er ist auf das Routen von Datenpaketen innerhalb von Lokinet beschränkt. Er sendet damit

niemals Anfragen an das allgemeine Internet. Ein Exit-Node Betreiber muss sich explizit dazu verpflichten, wenn er diese Rolle einnehmen möchte. Er macht dies indem er versichert, dass er über die zusätzlichen Risiken informiert ist und sich ebenso den erweiterten Schwarm Tests unterzieht (siehe 8.3.1).

Der Betrieb des Nodes als Exit-Node ermöglicht es einem Benutzer, den Reward eines normalen Relais zu verdoppeln, wenn er für einen Block Reward ausgewählt wird. Dieser Anreiz wird geboten, um sicherzustellen, dass die Betreiber von Exit-Nodes über ausreichende finanzielle Anreize verfügen, um Exit-Nodes zu betreiben, was zum Schutz vor Sybil Angriffen beiträgt, die speziell auf die Übernahme des Exit-Node Netzwerks ausgerichtet sind. Dies ist eine Schwachstelle, an der Tor aufgrund seines niedrigen Verhältnisses von Exit-Nodes zu Relais leidet.

6.4 Remote Nodes

In jedem Kryptowährungsnetzwerk ist das Speichern einer vollständigen Kopie der Blockchain für viele Benutzer nicht möglich oder praktisch. Bei Bitcoin und Ethereum können Benutzer eine Verbindung zu einem öffentlichen Full-Node herstellen, der eine Kopie der Blockchain enthält um Transaktionen abzufragen und ebenso an das Netzwerk zu senden. Dies funktioniert, da die Full-Nodes der Bitcoin und Ethereum Blockchain effizient nach Transaktionen durchsucht werden können, die den öffentlichen Schlüssel des Benutzers als Ziel haben.

Durch die Verwendung von CryptoNote Währungen werden öffentliche Full-Nodes (sogenannte Remote-Nodes) viel stärker beansprucht. Wenn ein Benutzer eine Verbindung zu einem Remote-Node herstellt, muss er jeden Block (bei Neuerstellung einer Wallet oder seit dem letzten überprüften Block) temporär auf seinen lokalen Rechner herunterladen und jede Transaktion auf einen öffentlichen Transaktionsschlüssel prüfen, der aus dem privaten View-Key generiert werden kann. Dieser Prozess kann erhebliche Auswirkungen auf die Leistung von Remote-Nodes haben. Wenn man bedenkt, dass es für diesen Service keinen finanziellen Anreiz gibt, kann es Nutzer davon abhalten, Dienste zur Synchronisierung von Light Clients zu betreiben. Mobile CryptoNote Wallets sind oft unzuverlässig und müssen manchmal mehrmals zwischen Remote-Nodes wechseln, bevor sie eine zuverlässige Verbindung aufbauen können.

Darüber hinaus können böswillige Remote-Node Betreiber, die einen der wenigen gängigen Nodes ausführen, die IP-Adresse von Benutzern aufzeichnen, während sie bestimmte Transaktionen senden. Obwohl durch diesen Angriff keine Informationen über die tatsächliche Transaktion enthüllt werden, können bestimmte IP-Adressen mit Transaktionen verknüpft werden, die dann verwendet werden können, um eine Verbindung zu einer echten Identität herzustellen, wodurch die Privatsphäre erheblich gefährdet wird.

Loki umgeht diese Probleme, indem jeder Service-Node ebenso als Remote-Node arbeitet, der von jedem Benutzer verwendet werden kann. Service-Nodes eignen sich hervorragend für diese Arbeit, da sie bereits eine vollständige Kopie der Blockchain enthalten und ein weit verbreitetes Netzwerk von Nodes mit hoher Bandbreite bilden. Durch die Verwendung von Service-Nodes als Remote-Node gibt es finanzielle Barrieren in Bezug auf den Anteil des Remote-Node Netzwerks, über den eine böswillige Partei verfügen und damit auch darüber, wie viele Daten ein böswilliger Node Betreiber sammeln kann.

6.5 Blink

In einem typischen Blockchain System ist die Bestätigungszeit für eine Transaktion die Zeit, die für die Aufnahme einer Transaktion in einen Block benötigt wird. Aufgrund konkurrierender Miner, zurückgehaltener Blöcke und Finney Attacken benötigen die Empfänger in der Regel eine Anzahl zusätzlicher Blöcke, die nach dem Block der die aktuelle Transaktion enthält folgen, bevor diese als abgeschlossen gilt [24]. Abhängig von einer Vielzahl von Faktoren, die für jede Blockchain spezifisch sind, kann dieser Prozess oft 10-60 Minuten dauern, was für Händler und Kunden unbequem ist, die auf Bestätigungen warten müssen bevor sie Waren freigeben oder ihre Dienste beginnen.

Aufgrund der Service-Node Architektur von Loki sind nahezu sofortige Transaktionen möglich. Blink ermöglicht, dass dieselben Transaktionen, die auf der Loki Main-Chain stattfinden würden bestätigt werden, bevor sie in einen Block aufgenommen werden. Dadurch wird vom Absender als auch vom Empfänger die Gültigkeit der Transaktion sichergestellt und der Empfänger ebenso vor doppelten Outputs geschützt.

Blink funktioniert ähnlich wie DASH's InstantSend. Für jeden Block wird ein Service-Node Schwarm deterministisch ausgewählt, um als eine Gruppe von Zeugen zu agieren, die eine Transaktionsgültigkeit bestätigen und die Transaktion daran hindern, zweimal ausgegeben zu werden. Anstatt der nicht verwendeten Outputs, die mit der Transaktion verwendet werden (wie bei DASH) zu sperren, werden hier Schlüsselbilder gesperrt. Schlüsselbilder sind eindeutige Schlüssel, die an jeden nicht ausgegebenen Output in einer Ringsignatur angehängt werden, um sofort zur Verfügung zu stehen. Blink erteilt dem ausgewählten Schwarm die Berechtigung, dem Netzwerk zu signalisieren, dass ein mit einer Ausgabe verknüpftes Schlüsselbild gesperrt werden soll, bis die Transaktion in einem Block enthalten ist. Wenn ein doppelter Output desselben nicht ausgegebenen Outputs versucht wird, wird ein identisches Schlüsselbild erzeugt, das vom Schwarm und somit vom Netzwerk als Ganzes zurückgewiesen würde.

Benutzer haben die Möglichkeit, eine höhere Gebühr zu zahlen, um eine Blink Transaktion zu senden, die in Sekunden anstatt in Minuten bestätigt wird. Dies eröffnet eine Reihe neuer Anwendungsfälle für Loki, in denen persönliche Zahlungen immer praktischer werden und online Zahlungen einfacher zu integrieren sind. Alle Datenschutzfunktionen, die Loki auszeichnen, sind auch hier während des gesamten Prozesses gültig.

7 CryptoNote Änderungen

Als Kryptowährung ähnelt Loki funktionell anderen CryptoNote Währungen. Es gibt jedoch wesentliche Unterschiede, die über das Hinzufügen von Service-Nodes und die damit verbundene Funktionalität hinausgehen.

7.1 ASIC Resistance

Ein Application-Specific Integrale Circuit (ASIC) ist ein Computerchip, der speziell für eine einzelne Funktion hergestellt ist. Im Kontext des Mining werden ASICs verwendet, um spezifische Hashing-Algorithmen zu berechnen. Sie stellen ein Risiko für die Dezentralisierung dar, da sie technisch oftmals anderen Mining Verfahren überlegen sind, von nur wenigen Unternehmen hergestellt werden und aufgrund der speziellen Beschaffenheit der Hardware

nur sehr begrenzte Vertriebskanäle und erhebliche Kapitalkosten haben, um sich profitabel betreiben zu lassen. ASICs haben potenzielle Vorteile, wie z. B. die Kapitalkostenanforderungen, die Miner in algorithmespezifische Hardware investieren müssen, wodurch es weniger wahrscheinlich ist, dass sie sich in einer Weise verhalten, die ihre eigenen Investitionen untergräbt, indem sie sich unehrlich verhalten. Die Herstellung und der Vertrieb von ASIC-Chips mit ausgereiften Hashing Algorithmen ist jedoch immer noch zentralisiert und durch wenige große Unternehmen kontrolliert. Diese Unternehmen können den Versand in verschieden Regionen ablehnen und ebenso entscheiden, ob und welche Kunden und Regionen mit leistungsfähigsten ASICs beliefert werden. Ebenso können sie Preise manipulieren.

Um zu verhindern, dass ASIC-Miner die Netzwerk Hashrate monopolisieren, haben viele Kryptowährungen ASIC resistente Hash Algorithmen wie Scrypt und Ethash [25][26]. Bis vor kurzem verwendete Monero den CryptoNight Hashing Algorithmus, der große Mengen an L3-Cache benötigt, um zu funktionieren. Theoretisch hätte dies die Herstellung eines ASIC-Chips aufgrund großer Speicheranforderungen erschweren sollen. Im Jahr 2018 veröffentlichte Bitmain den X3, einen CryptoNight spezifischen ASIC, der effektiv die zehnfache Geschwindigkeit einer Graphics Processing Unit (GPU) erreichen konnte [27]. Andere Hashing Algorithmen haben ähnliche Schicksale erlebt, wobei Scrypt, Ethash und Equihash nun mit ASICs berechnet werden können.

Um die Verwendung von ASICs zu bekämpfen, schlug Monero eine Strategie vor, alle drei bis sechs Monate einen hard fork durchzuführen, um den CryptoNight Hashing Algorithmus leicht zu ändern (der erste fork führte zu einem Wechsel zu CryptoNightV7) [28]). Das Kapital und die Zeit, die zum Aufbau eines ASICs erforderlich sind, sind signifikant und bei sehr spezifischen Hardwaredesigns sollten geringfügige Optimierungen in einem Hashing Algorithmus das Chipdesign ungültig machen und den Zeit- und Kapitalaufwand der ASIC-Hersteller obsolet machen. Dieser Ansatz führt jedoch einige Probleme mit sich. Wenn an dem Algorithmus vorgenommene Änderungen nicht ausreichen, um zu verhindern, dass ASICs neu programmiert werden, dann kann das Netzwerk für eine Hash Zentralisierung anfällig werden, bis ein anderer hard fork möglich ist. Field Programmable Gate Arrays (FPGAs) sollten auch bei ASIC Resistenz Strategien berücksichtigt werden, da kleinere Änderungen am Hashing Algorithmus hier schnell umprogrammiert werden können. Ein weiteres Problem besteht darin, dass regelmäßige Änderungen an den Kernkonsensmechanismen die Möglichkeit unbeabsichtigter Fehler fördern und die Entwicklung solcher Änderungen im Allgemeinen um das Kernteam herum zentralisiert sind und Ressourcen binden.

Eine Reihe von alternativen Proof-of-Work Algorithmen wurde vorgeschlagen, um die Notwendigkeit regelmässiger hard forks unnötig zu machen, einschließlich memory-hard hashing Algorithmen wie Argon2, Balloon-Hash und polymorphe Hashing Algorithmen wie ProgPoW und RandProg [29][30][31][32]. Das Loki-Team wird zusätzliche Forschung zu den oben genannten Algorithmen veröffentlichen, um eine langfristige Lösung für die ASIC-Resistenz zu entwickeln.

Loki implementiert eine Version von CryptoNight namens CryptoNight Heavy, die die ASIC Resistenz gegen CryptoNight ASIC Miner aufrechterhält. CryptoNight Heavy unterscheidet sich von CryptoNight V7 in mehrfacher Hinsicht: Es bietet eine Erhöhung der Scratchpad-Größe auf 4 MB und eine Änderung in der Art, wie mit implodes and explodes umgegangen wird [33]. Diese Änderungen unterscheiden es von Moneros CryptoNight V7 und bieten einen robusteren Schutz gegen ASIC Weiterentwicklungen bis eine dauerhaftere Lösung gefunden und umgesetzt wird.

7.2 Dynamische Block Größe

Wie andere CryptoNote Währungen auch, hat Loki keine feste Blockgröße. Stattdessen ändert sich die Blockgröße im Laufe der Zeit, womit mehr Transaktionen berücksichtigt werden wenn das Netzwerk einen höheren Transaktionsdurchsatz erreicht. Die Loki Blockgröße skaliert im Verhältnis zur Medianblockgröße über die letzten 100 Blöcke und reorganisiert die maximale Größe neuer Blöcke langsam entsprechend neu.

Die langfristige Sorge in anderen Kryptowährungen ist, dass große Blockgrößen die Nodes, die Transaktionen speichern und verifizieren, zu stark belasten. Wenn Blockgrößen wachsen, können Nodes, die auf schwacher Hardware laufen, keine neuen Blöcke verarbeiten. Dies führt dann zu einer Zentralisierung des Node Netzwerkes unter denen mit einem kommerziellen Interesse. Dies kann insofern problematisch sein, als das die Verteilung der Blockchain auf sehr viele Nodes ermöglicht, den Zustand der Blockchain unter vielen verschiedenen Parteien zu bestätigen, was zu ihrer Validität und Zensurresistenz beiträgt.

In Loki wird ein Teil des Block Rewards an Service-Nodes vergeben, die Blöcke als Full-Nodes verarbeiten und propagieren. Da Service-Nodes mit unzureichender Bandbreite und Leistung aus dem Netzwerk der Service-Nodes fallen (siehe 7.3), erzwingt der Prämienpool selbst eine minimale Leistungsanforderung. Diese Anreizstruktur stellt nicht nur sicher, dass die Anzahl der Nodes hoch bleibt, sondern auch, dass die Nodes ein ausreichendes Leistungsniveau aufweisen, um Blockchain Daten über das Netzwerk effektiv und erfolgreich zu verteilen, unabhängig davon, wie groß die Blockchain ist oder wie anspruchsvoll die Bandbreitenanforderungen werden. Trotzdem sind Transaktionsgrößenoptimierungen immer noch erforderlich um sicherzustellen, dass das Netzwerk effizient skaliert, um die Betriebskosten der Service-Nodes niedrig zu halten. Nur so kann sichergestellt werden, dass eine hohe Anzahl von Nodes langfristig aufrechterhalten werden kann.

7.3 Größe der Ringsignaturen

Ringsignaturen werden verwendet, um reale Outputs unter anderem in einer bestimmten Transaktion zu verbergen. Die Größe einer Ringsignatur bezieht sich darauf, wie viele Mixins zum Aufbau des Rings verwendet werden. Monero verfügt derzeit über eine erzwungene Mindestring Signaturgröße von sieben, wobei sechs Mixins neben der tatsächlich nicht ausgegebenen Ausgabe in einer Transaktion verwendet werden.

Die Wirkung von größeren Ringgrößen wurde nur rudimentär untersucht,. Jedoch wurde in der Veröffentlichung 0001 (veröffentlicht vom Monero Research Lab) der Effekt unterschiedlicher Ringgrößen gegenüber einem Angreifer analysiert, der eine große Anzahl von Outputs auf der Blockchain besaß [34]. Es wurde festgestellt, dass höhere Ringgrößen den Zeitrahmen verkürzen, in dem ein böswilliger Angreifer, der eine große Anzahl nicht ausgegebener Outputs besitzt, in der Lage wäre, eine effektive Transaktionsanalyse durchzuführen. Das Verpflichten größerer Ringgrößen schützt auch vor einem theoretischen Angriff, der als EABE / Knacc-Angriff bekannt ist [35], in der eine dritte Partei (zum Beispiel eine Wechselbörse) eine begrenzte zeitliche Analyse von Transaktionen zwischen zwei Benutzern durchführen kann.

Darüber hinaus hat Monero keine maximale Ringgröße, die durch Netzwerkkonsensregeln erzwungen wird. Viele Wallets wie die Monero-GUI Wallet decken theoretisch eine Ringgröße bis 26 ab. Es ist einem Benutzer jedoch freigestellt, eine Transaktion mit der von ihnen gewünschten Ringgröße manuell zu erstellen, solange sie über einer Ringgröße von sieben liegt. Dies ist problematisch, da die meisten Wallets eine Standardgröße von sieben haben. Wenn Sie eine Transaktions Ringgröße über sieben auswählen, fällt dies auf (Abbildung 4). Wenn eine Einzeltransaktion in Monero immer eine nicht standardisierte Ringgröße verwendet (z. B. zehn), könnte ein Drittanbieter die Blockchain analysieren und Muster mithilfe der zeitlichen Analyse ableiten.

transaction hash	ring size	tx size [kB]
3feaff3f48de0bc4c92ec027236165337b64df404aca098e212c1215e9456697	7	13.47
39d484f7c0a2e8f3823a514056d7cb0bf269171cb4582e05955d4c5ee995cad0	7	13.47
e08f5a937e725011bedd44075334ae98dcca32749da231c56da1278d49c0a231	7	13.50
ab35e69d9cca39219c90df8b2b7aab4a54c82127fb1fbaae65d76357f8f76387	7	13.50
6d8ccd56dc2d3eb7de03ba767f0dbf4d5f42ae91e67f4c28f16d6f8b0229c272	10	13.87

Abbildung 3: *xmrchain.net (Monero block explorer) zeigt, wie nicht standardisierte Ringgrößen aussehen*

Loki löst diese beiden Probleme, indem es Ringgrößen statisch erzwingt und die Ringgröße auf zehn setzt. Das statische Festlegen der maximalen Ringgröße schützt Benutzer, die Ringe mit mehr als neun Mixins zu konstruieren. Ebenfalls verhindert das Festlegen des Ringgrößenminimums auf zehn effektiv, dass ein Angreifer, der eine große Anzahl von Outputs besitzt, die wahren Outputs in einer Ringsignatur erkennt. Größere Ringgrößen erhöhen auch die Standard Wirbel Effektivität nicht linear und werden mit zunehmender Größe der Ringe effektiver.

Im aktuellen Transaktionsschema würde eine Erhöhung der Ringgröße auf 10 zu einer Erhöhung der Transaktiongröße um 2,6% führen. Wenn Bulletproofs jedoch implementiert werden, wird die Transaktionsgröße um ca. 8 - 13% zunehmen. Dies liegt an der durch Bulletproofs ins-

gesamt verringerten Transaktionsgröße. Das Erhöhen der minimalen Ringgröße kann ein Problem in einem Netzwerk darstellen, das aufgrund des erhöhten Overheads keine Architektur aufweist, um größere Transaktionen zu unterstützen. Mit Loki kann diese Last jedoch von Service-Nodes getragen werden, die Anreize zum Betrieb und zur Bereitstellung ausreichender Bandbreite und Leistung erhalten.

8 Angriffsschutz

8.1 IP und Packet Blockierung

Obwohl das Service-Node Netzwerk keinen zentralen Angriffspunkten ausgesetzt ist, gibt es dennoch zwei zensurbezogene Bedrohungen. Nämlich Harvesting-Attacks und Deep Packet Inspection [36][37]. Harvesting-Attacks würden versuchen, die IP-Adressen aller in Betrieb befindlichen Serivce-Nodes im Netzwerk zu sammeln und Firewalls auf ISP-Ebene zu verwenden, um Verbindungen zu diesen bestimmten Adressen zu blockieren. Diese Art der Zensur wird regelmäßig im Tor-Netzwerk in China durchgeführt [38]. Die Deep Packet Inspection (DPI) zielt darauf ab, die Strukturierung jedes einzelnen Pakets zu untersuchen, das eine Firewall durchläuft, und selektiv Pakete zu löschen oder zu blockieren, die scheinbar auf einen bestimmten Dienst bezogen sind. Auch hier wurde DPI von staatlichen Akteuren intensiv genutzt [39].

Es wurde viel Arbeit investiert, um Systeme zu entwickeln, die DPI umgehen. Benutzer können verschiedene Arten von Pluggable-Transporten nutzen, die die Signatur jedes Pakets ändern, die als normaler nicht blockierter Verkehr erscheinen soll. IP-Blockierung wird im Allgemeinen vermieden, indem Domänenfrontbrücken ausgeführt werden, die den Datenverkehr mit Hilfe von HTTPS an nicht gesperrte Dienste wie Azure oder Cloudflare verschlüsseln. Sobald sie den nicht blockierten Dienst erreichen, leitet die Brücke die Anfrage an den gewünschten Ort weiter. Im Falle der Domänenfronten wird es für einen Akteur auf Länderebene schwierig, den Fluss des gesamten Verkehrs zu populären Brücken zu verhindern, ohne eine signifikante Störung der allgemeinen Nutzung des Internets zu verursachen.

Governance Mechanismen, die in Loki integriert sind (siehe 9), können verwendet werden, um Domänen-Frontend-Bridges zu betreiben, so dass Benutzer auf Loki Services auch aus Ländern zugreifen können, in denen groß angelegte Internet Zensur Regelungen im Spiel sind. Darüber hinaus wird die OBFS4-Unterstützung für den Transport mit der Service-Node Version der Loki Wallet gebündelt, um weiteren Schutz gegen DPI zu bieten [40].

8.2 Angriffe zur Verhinderung von Services

Benutzer von dezentralen Blockchains müssen keine digitalen oder physischen Kennungen bereitstellen. Dies kann für Benutzer hilfreich sein, denen die Identität fehlt oder die deswegen verfolgt werden. Systeme, die keine Identifizierung erfordern, sind jedoch anfällig für Sybil Attacken, bei denen ein böswilliger Akteur zahlreiche falsche Identitäten erzeugt (im Fall von Loki zahlreiche öffentlich private Schlüsselpaare) und diese Identitäten verwendet, um das Netzwerk mit Anfragen zu fluten (Spam).

Viele Kryptowährungen haben mit diesem Problem zu kämpfen und sind gezwungen, entweder ein Servicemodell gegen Entgelt oder ein Proof-of-Work-Modell zu implementieren. In

kostenpflichtigen Modellen wie Siacoin zahlen Nutzer für die von ihnen genutzten Dienste. Im Falle von Siacoin werden die Kosten pro TB Lagerung pro Monat bestimmt [41]. „Fee-for-Service-Modellereduzieren effektiv Sybil Attacken, führen jedoch viele Benutzer vom System weg, insbesondere wenn ähnliche Dienste kostenlos zur Verfügung stehen (wie beispielsweise Google Drive und Onedrive im Fall von Siacoin). Proof-of-Work-Systeme, wie sie in Hashcash und Nano verwendet werden erfordern, dass Benutzer einen kleinen Proof-of-Work Nachweis berechnen, bevor sie eine Nachricht oder Transaktion versenden können [42][43]. Diese kleinen Proof-of-Work-Systeme sind egalitärer als das „Fee-for-ServiceModell, können aber Angreifern zum Opfer fallen, die große Mengen an Rechenleistung besitzen.

Loki schlägt ein modifiziertes Proof-of-Work System vor, um mit den zwei größten Sybil Angriffsflächen im Loki System umzugehen; Offline Nachrichten und Pfaderstellung. Offline Nachrichten stellen ein potenzielles Ziel dar, da jede Nachricht von einem Schwarm von neun Nodes gespeichert werden muss. Ein potenzieller Missbrauch könnte entstehen, wenn ein böswilliger Benutzer einen bestimmten Schwarm mit einem hohen Volumen von Nachrichten flutet, die diese speichern müssten. Bei Pfaderstellungsangriffen versucht der Angreifer, den Pfaderstellungsprozess mit so vielen Nodes wie möglich durchzuführen, um Bandbreitenressourcen für legitime Zwecke von anderen Benutzern des Netzwerks zu blockieren.

Um beide Angriffe zu verhindern, erfordert das Loki Netzwerk die Erstellung eines kurzen Proof-of-Work, wenn sowohl Nachrichten als auch Pfade erstellt werden. Bei Nachrichten wird dieser Proof-of-Work als Blake2b-Hash der Nachricht berechnet. Bei der Pfaderstellung wird der Arbeitsnachweis zusammen mit der Anforderung für einen Node gesendet, der in den Pfadbildungsprozess einbezogen werden soll. Um die Skalierbarkeit und Zugänglichkeit für mobile Benutzer zu gewährleisten, wird die Schwierigkeit des Proof-of-Work basierend auf der Time-to-live (TTL) der Nachricht oder des Pfads und nicht auf der Grundlage der globalen Netzwerkaktivität festgelegt.

8.3 Schwarm Markierung

Wenn Nodes in einer vertrauensfreien Umgebung arbeiten, ohne dass eine zentrale und übergeordnete Stelle Regeln erzwingt, wird die Aufrechterhaltung eines korrekten Node Verhaltens im Netzwerk schwierig. Service-Nodes in Loki müssen zwar die erforderlichen Sicherheitsanforderungen erfüllen (Mindestkapital), sie können jedoch wählen, dass Datenverkehr nicht weitergeleitet oder Daten in ihren Speicherpools gespeichert werden. Da diese Option finanziell nachteilig ist (weniger Bandbreite, CPU Zyklen, Speicher), muss ein System mit verteilter Kennzeichnung vorgeschlagen werden, um leistungsschwache Nodes zu eliminieren.

Loki stellt eine solche verteilte Kennzeichnung vor große Probleme bei der Implementierung. Grundsätzlich ist es für jeden Service-Node finanziell attraktiv, einen anderen Service-Node als schlechten Akteur zu kennzeichnen. Dies liegt daran, dass ein markierter Node aus dem Vergütungspool entfällt, welches die Chance der restlichen Nodes erhöht eine (auch möglicherweise höhere) Vergütung zu erhalten. Um diese Probleme zu umgehen, schlägt Loki die Schwarm Markierung vor.

Die Schwarm Markierung funktioniert, indem vorhandene Schwärme verwendet werden (siehe 6.1.1), um die Mitglieder auszuwählen, die an der nächsten Testrunde teilnehmen. Jeder Service-Node enthält eine Kopie der Blockchain und jedem von einem Miner erstellte Block wird deterministisch eine Anzahl von Testschwärmen zugeordnet. Von jedem Block werden 1% der Schwärme aus dem Netzwerk für die Teilnahme an einem Testschwarm ausgewählt.

Um teilnehmende Schwärme zu berechnen, wird der Hash der fünf vorherigen Blöcke verwendet, um eine Mersenne-Twister Funktion zu erzeugen, die dann Schwärme in der Reihenfolge ihrer Position in der deterministischen Liste auswählt.

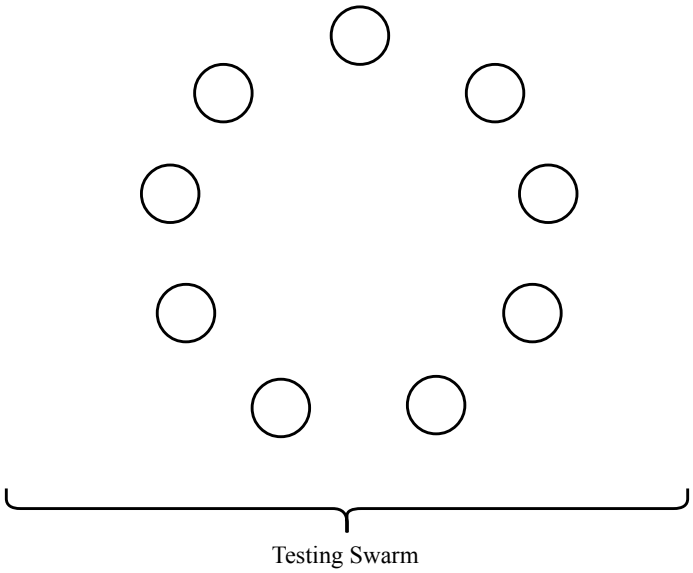

Abbildung 4: *Ein Test Schwarm besteht aus 9 ausgewählten Nodes*

Wenn ein Schwarm zur Teilnahme ausgewählt wurde, wird erwartet, dass jeder Node in diesem Schwarm eine Anzahl von Tests bei jedem anderen Node im Schwarm durchführt. Dies sind keine aktiven Tests, vielmehr speichert jeder Node historische Informationen über seine Interaktionen mit jedem anderen Node innerhalb seines Schwarms. Informationen über Bandbreite, Nachrichtenspeicher, Blockchain Anforderungen und Exit-Node Funktionalität werden gesammelt und im Laufe der Zeit beibehalten. Neue Schwarm Teilnehmer, die diese Informationen noch sammeln müssen, können Service-Nodes außerhalb ihres unmittelbaren Schwarms abfragen, um Daten zu jedem der von ihnen getesteten Service-Nodes zu sammeln.

Jeder Service-Node prüft und entscheidet autark, wie er bei jedem anderen Schwarm Mitglied abstimmen soll. Sobald er seine Entscheidung aufgrund der oben genannten Tests getroffen hat, werden diese gesammelt an den Schwarm gesendet. Jeder Node im Schwarm kann nun die Stimmen aller Mitglieder überprüfen. Wenn bei einem einzelnen Node im Schwarm mehr als 50% der Nodes negativ stimmen, verfügt jedes Schwarmmitglied über die erforderlichen Informationen, um eine Deregistrierungstransaktion zu erstellen. Sobald diese Transaktion validiert und in einen Block aufgenommen wurde, aktualisieren alle Service-Nodes ihre DHT und bereinigen alle Nodes, die abgewählt wurden.

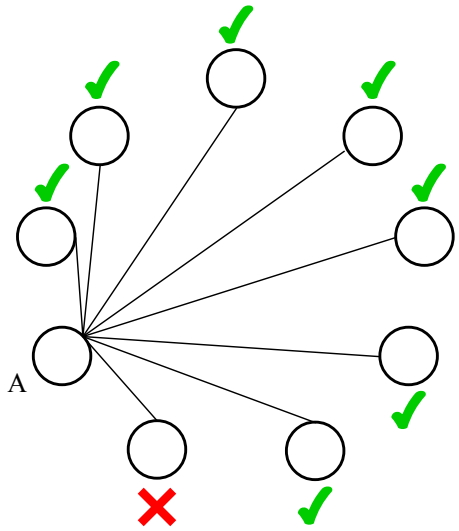

Abbildung 5: *Ein unehrlicher Node wurde durch Node A getestet und hat nicht bestanden. Node A entscheidet lokal, welche Nodes bestanden und welche nicht bestanden haben.*

8.3.1 Test Suite

Damit das Netzwerk die Leistungsstandards selbst durchsetzen und kontrollieren kann, müssen Service-Nodes mit den erforderlichen Tools ausgestattet sein, um andere Service-Nodes zu testen. Diese Tests sollten den Umfang aller von Service-Nodes bereitgestellten Funktionalitäten abdecken, um Lazy-Masternode Attacken zu verhindern [44]. In diesem anfänglichen Entwurf werden vier grundlegende Tests vorgeschlagen. Weitere Tests können zu der Testsuite jederzeit hinzugefügt werden, wenn die Funktionalitäten der Service-Nodes erweitert werden.

Wenn ein Betreiber das erste Mal seine Service-Node Software ausführt, wird eine leere Datei mit einer vorbestimmten Größe auf dem Datenträger zugewiesen, um sicherzustellen, dass ausreichend Speicherplatz für Aufgaben vorhanden ist, die Speicher benötigen. Als nächstes wird ein einfacher Bandbreitentest zwischen dem Service-Node und einem geografisch verteilten Anzahl von Test Servern durchgeführt, die von der Loki Foundation betrieben werden. Diese Überprüfungen sind optional und Service-Nodes dürfen sie überspringen, ignorieren oder verfehlen und dem Pool nicht vertrauenswürdiger Service-Nodes beitreten. Sobald ein Service-Node jedoch dem nicht vertrauenswürdigen Service-Node Pool beigetreten ist und den produktiven Betrieb aufnehmen möchte, wird sein Mindestkapital gesperrt und dieser vom nächsten ausgewählten Schwarm getestet. Schwarm Tests werden über den Konsensus erzwungen und Neueinsteiger in das Service-Node Netzwerk können diese nicht umgehen. Wenn ein Node alle Schwarmtests besteht, erhält er eine Markierung, die ihn als vertrauensvoll einstuft und kann damit beginnen, Pakete zu routen. Andernfalls wird er aus dem Netzwerk entfernt und das Mindestkapital bleibt für 30 Tage gesperrt.

Bandbreiten Test

Der Bandbreitentest bildet das Rückgrat der Loki Netzwerk Testsuite. Wenn ein Node diesen Test besteht, wird angenommen, dass er Datenpakete oberhalb des minimalen Schwellenwerts weiterleiten kann.

Jedes Mal, wenn ein Node mit einem anderen Service-Node interagiert, erstellt und speichert er eine Aufzeichnung der eingehenden Bandbreite. Im Laufe der Zeit werden Nodes mit Tau-

senden von Pfaden enthalten sein und Millionen von Nachrichten routen. Diese Interaktionen bilden die Grundlage für die Node Bandbreiten Tabellen. Aus dieser Tabelle kann ein Node auf Bandbreitentests über Service-Nodes innerhalb seines Schwarms antworten.

Von allen Nodes wird auch erwartet, dass sie auf Abfragen ihrer eigenen Bandbreitentabellen von anderen Nodes antworten. Dies bedeutet, dass sogar Nodes, die erst kürzlich dem Netzwerk beigetreten sind, das weitere Netzwerk nach Informationen über bestimmte Nodes in ihrem Schwarm abfragen können.

Test zur Nachrichtenspeicherung

Nachrichtenspeicherung ist für Offline-Messaging Funktionen für Benutzer von Loki Messenger unerlässlich. Service-Nodes müssen auf ihre Fähigkeit getestet werden, Nachrichten im Cache zu speichern und sie Benutzern im Verlauf der Time-to-Live (TTL) der Nachricht bereitzustellen.

Benutzer, die Offline-Nachrichten senden, wählen nach dem Zufallsprinzip einen Service-Node im Schwarm der Zielbenutzer aus. Dieser Node muss eine Kopie der Nachricht an den Rest des Schwarms verteilen. Abhängig von dem Proof-of-Work, der dem Header der Nachricht angehängt ist, speichern Service-Nodes, die eine Kopie erhalten, die Daten für die TTL. Wenn die TTL der ursprünglichen Nachricht ihre Ablaufzeit erreicht hat, sendet der Verteiler Node eine Nonce an alle anderen Mitglieder des Schwarms. Der Schwarm verwendet die Nonce, fügt sie der Nachricht hinzu, hasht dann das Ergebnis und sendet es schließlich an den Verteiler Node zurück. Dieser Test stellt sicher, dass Service-Nodes Nachrichten bis zur TTL Endgültigkeitsdauer speichern und eine Löschung verhindern, wenn sie nicht in der Lage sind, den korrekten Nachrichtenauszug zu erstellen. Da die Stichprobenverteilung des Verteiler Nodes zufällig ist, kann jeder Service-Node im Laufe der Zeit Leistungsdaten für seinen Schwarm sammeln.

Test zur Speicherung der Blockchain

Von Service-Nodes wird ebenso erwartet, dass sie eine vollständige Kopie der Loki Blockchain vorhalten. Durch das Halten einer vollständigen Kopie der Blockchain können Service-Nodes eine Reihe von Aufgaben ausführen, die für Benutzer des Netzwerks wichtig sind, darunter die Funktion als Remote-Node, die Validierung von Transaktionen und das Sperren von Transaktionen in Blink.

Da ehrliche Nodes auch eine Kopie der Blockchain enthalten, könnte ein unehrlicher Node es vermeiden, eine vollständige Kopie vorzuhalten, indem er beim Testen einfach Blöcke von einem ehrlichen Node anfordert. Um dieses Ergebnis zu vermeiden, ist der Blockchain Speichertest so konzipiert, dass ehrliche Nodes, die eine Kopie der Blockchain besitzen, diesen Test bestehen können, während unehrliche Node dies nicht können.

Um dies zu erreichen, fordert der Test-Node jeden getesteten Node auf, eine Auswahl von K zufälligen Transaktionen innerhalb des Verlaufs der Blockchain zu treffen, die dann verkettet und gehasht werden. Dieser Hash wird dann an den Test-Node zurückgegeben. Durch Messen der Latenz dieser Anforderung kann der Test-Node die Latenz mit der erwarteten Rückkehrzeit T vergleichen. Der genaue Wert für T wird eingestellt, um die erwartete Latenz zwischen dem Laden von der Festplatte und dem Herunterladen von Blöcken aus dem Netzwerk genau zu unterscheiden. Für jeden Angreifer sollte es unmöglich sein, K Blöcke innerhalb von T herunterzuladen und zu hashen, wodurch piggybacking Angriffe schwierig werden.

Exit Node Test

Service-Nodes, die als Exit-Node arbeiten, erhalten zusätzliche Rewards. Daher sind Funktionstests erforderlich, um sicherzustellen, dass diese zusätzliche Rewards nicht missbraucht werden.

Damit funktionale Exit Tests stattfinden können, muss ein Service-Node das natürliche Suchverhalten eines Menschen simulieren können. Wenn ein Service-Node erkennen kann, dass er getestet wird, kann er nur auf Tests reagieren und legitime Benutzeranforderungen verwerfen. Das simulieren des natürlichen Seitenanforderungsverhaltens ist schwierig, jedoch können Exit Tests so entworfen werden, dass der Aufwand für das Sortieren zwischen legitimen Anforderungen und Tests ausreichend erschwert wird, so dass der Unterschied in den Bandbreitenkosten zwischen dem Ausführen eines legitimen Nodes und eines bösartigen Nodes vernachlässigbar sind.

Service-Nodes verwenden eine lokal gehaltene Liste von Suchmaschinen, die mit einem Wörterbuch kombiniert werden, um pseudozufällige natürliche Suchbegriffe zu erstellen. Die Suchbegriffe werden dann in die Suchmaschinen eingegeben und die Webseiten werden zufällig aus den Ergebnissen ausgewählt. Der Service-Node kann nun einen Pfad mit zufälligen Nodes erstellen, die als Relais fungieren und den Node, der als Exit-Node getestet wird. Von diesem Exit fordert der Service-Node das Website Ergebnis an, das von seiner pseudozufälligen Suche erzeugt wurde. Wenn das vom Exit-Node zurückgegebene Ergebnis mit dem Ergebnis übereinstimmt, dass vom Service-Node generiert wurde, gilt der Exit-Node Test als bestanden.

9 Governance, Funding und Voting

Governance ist ein wesentlicher Bestandteil des Kryptowährungsdesigns und sollte auf Protokollebene unterstützt werden. Das Risiko einer schwachen, nur informell definierten Governance wurde in der Geschichte der Blockchain Technologie umfassend untersucht. Bitcoin und Ethereum erlebten kontroverse forks, die den Fokus und die Bemühungen ihrer jeweiligen Gemeinschaften aufteilten. Hard forks und auch Interventionen durch Governance sollten immer als letztes Mittel und nicht als Lösung für jedes strittige Thema betrachtet werden. Das Loki Governance System wurde entwickelt, um potenzielle Probleme zu lösen, indem es eine strukturierte Umgebung für Diskurs und Repräsentation bereitstellt und ebenfalls monetäre Mittel für die Weiterentwicklung von Loki zur Verfügung stellen kann, ohne auf externe Einflüsse und Geldgeber oder gar Altruismus angewiesen zu sein.

Über die Verhinderung von hard forks hinaus sollten Governance Strukturen die Mittel schaffen, um neue Projekte, die das Loki-Ökosystem verbessern, intern finanzieren zu können. Intern finanzierte Projekte können die Bildung von speziellen Interessengruppen verhindern, die nicht unbedingt Motive haben, die mit Nutzern, Minern oder Service-Nodes Betreibern übereinstimmen. Wir haben dies bei Bitcoin und verschiedenen Bitcoin forks mit der Bildung von gewinnorientierten Unternehmen wie Blockstream, Bitcoin ABC und Bitcoin Unlimited gesehen. Diese werden häufig beschuldigt, Entwickler einzustellen, um protokollspezifische Änderungen an Bitcoin und Bitcoin Cash vorzunehmen um ihre eigenen Geschäftsziele oder ihrer spezifischen Ideologien zu verfolgen.

Aus diesem Grund werden von jedem Loki Block 5% des Block Reward dem Governance Pool zugewiesen. Dies sorgt für einen stetigen Einkommensfluss, der unter Community Projekten, Softwareentwicklern und Integrationsteams verteilt wird. Von diesen 5% des Block Reward werden 3,75% von der Loki Foundation und 1,25% von den Service-Nodes über das Loki

Funding System kontrolliert. Dies fördert eine faire Vertretung der Service-Nodes Interessen und ermöglicht die Finanzierung von Vorschlägen, die außerhalb der direkten Kontrolle der Loki Foundation liegen.

9.1 Die Loki-Stiftung

Die Loki Stiftung ist eine eingetragene gemeinnützige Organisation mit Sitz in Australien. Diese zentrale rechtliche Einheit existiert, damit das Loki Projekt in einem klar definierten rechtlichen Rahmen betrieben werden kann und den Projektarbeitern rechtlichen Schutz gewährt und ebenso Verpflichtungen gewahrt werden können. Die Loki Foundation wurde 2018 in Australien gegründet und verwendet die gleiche Verfassung wie beispielsweise Australian Charities und Non-Profit-Kommission (ACNC) [45]. Diese Satzung verleiht der Stiftung die gleiche Corporate Governance Struktur wie viele andere gemeinnützige Organisationen, in denen die Gesellschaft keine Aktionäre oder Nutznießer hat, die Verwaltungsratsmitglieder jeweils Mandate mit Befristung haben und Abstimmungen für ihre Mitglieder durchgeführt werden können. Die Loki Foundation ist so strukturiert, dass sie in Australien als gemeinnützig anerkannt ist.

Diese Organisation ist satzungsrechtlich verpflichtet, jegliche Einnahmen (einschließlich der Rewards für den Governance Block) für die Weiterentwicklung des Projekts und für abgestimmte Initiativen auszugeben. Als extern auditierte Organisation ist Transparenz für die Aufrechterhaltung eines eingetragenen Charity Status für die Loki Foundation von erheblicher Bedeutung wie eben auch, die Ausgaben in vernünftigen Grenzen zu halten.

Die Loki Foundation ist sowohl gegenüber ihren Mitgliedern als auch ihren Prüfern rechenschaftspflichtig. Ist dieses System letztendlich Loki und seinen Projekten nicht dienlich, gibt es einen Schutzmechanismus. Sollte ein hard fork mit ausreichend Zustimmung der Community aufbegehren, besteht die Möglichkeit, die Loki Foundation als Empfänger dieses Block Rewards zu entfernen oder zu ersetzen.

9.2 Das Loki Finanzierungssystem

Obwohl die Loki Foundation aus einer gemischten Gruppe von Personen besteht, die das Loki Projekt repräsentieren, unterliegt die Stiftung sowohl ihrer eigenen Verfassung als auch den Gesetzen Australiens. Dies könnte sich als begrenzender Faktor für die Entscheidungen erweisen, die die Stiftung treffen kann. Das Loki Finanzierungssystem sieht vor, dass ein Teil des Block Rewards ausschließlich durch eine Abstimmung der Service-Nodes umgesetzt wird. Service-Nodes repräsentieren Organisationen aus der ganzen Welt und sind nicht verpflichtet, Beiträge vom Loki Projektteam oder von der Foundation anzunehmen. Dies ermöglicht es ihnen, ein neues Maß an Autonomie bei den Entscheidungen zu erreichen, die sie eigenständig treffen können. Service-Nodes sind die am meisten kapitalgebundenen Teilnehmer im Netzwerk und haben einen finanziellen Anreiz, Entscheidungen zu treffen, die den Wert von Loki steigern.

9.2.1 Vorschläge

Jeder Vorschlag, der von Service-Nodes eingebracht wird, wird auf der Loki Blockchain veröffentlicht. Wenn eine bestimmte Partei einem Service-Node einen Vorschlag vorlegen

möchte, muss die Partei eine Angebotstransaktion erstellen. Da die Inhalte der Angebotstransaktionen lesbar und die Outputs „verbrannt“ werden müssen, verzichten sie hier auf die Datenschutzfunktionen typischer Loki Transaktionen.

Finanzierungsblöcke werden alle 43.000 Blöcke (ca. 60 Tage) erstellt. Proposal leaders können ihre Vorschläge jederzeit während dieses Zeitraums einreichen. Es sollte jedoch bedacht werden, dass je früher sie sich in der Vorschlagsphase befinden, desto mehr Zeit haben sie um Stimmen von jedem Service-Node zu erhalten.

An jede Transaktion ist ein zusätzliches Feld angehängt, dass die Informationen enthält, die jeder Service-Node zum Abstimmen verstehen muss. Diese Information beinhaltet; ein Vorschlagstitel, eine URL, die mit einer detaillierten Erläuterung des Angebots verknüpft ist, die Menge an Loki, die der Vorschlag benötigt, eine Zahlungsadresse und ein Escrow Agent, falls ausgewählt.

Bis zur Zustimmung durch die Loki Foundation können Nutzer, die Vorschläge machen, auch die Loki Foundation oder eine andere dritte Partei als Treuhänderin auswählen, die Mittel freigibt, wenn Meilensteine erreicht werden. Um einen hohen Standard bei Vorschlägen zu gewährleisten und ein Spammen dieser Transaktionen zu verhindern, muss jede Angebotstransaktion eine nicht geringe Menge an Loki verbrennen.

9.2.2 Abstimmung

Jeder Service-Node trägt einen spezifischen Schlüssel für das Voting. Dieser Schlüssel kann exportiert und verwendet werden, um im Namen eines Service-Nodes zu wählen, ohne sich beim Server anmelden zu müssen, auf dem er gehostet wird.

Die Abstimmung findet nicht on-chain statt, vielmehr signalisiert jeder Service-Node seine Unterstützung, Ablehnung oder Abstinenz für jeden aktiven Vorschlag in der Blockchain. Service-Nodes können über Vorschläge abstimmen, sobald sie der Blockchain anhängig sind, bis zum nächsten zweimonatlichen Finanzierungsblock. Kurz vor der Schaffung des nächsten Finanzierungsblocks wird ein Schwarm ausgewählt, um die Anzahl aller abgegebenen Stimmen zu sammeln. Diese werden dann übereinstimmend in den Node mempool übertragen und dort gespeichert, bis ein Miner den Funding Block errichtet hat. Diese Information wird dann verwendet, um den Block zu konstruieren, der dem Gewinner des Vorschlags den Reward zuweist. Der Reward wird jedoch nur übergeben, wenn das Ergebnis der Ja Stimmen Minus der Nein Stimmen 15% der Node Anzahl im Service-Node Netzwerk entspricht.

9.2.3 Mittelverteilung

Alle Erlöse aus dem Loki Funding werden durch die Funding Blocks bezahlt. Blöcke für die Refinanzierung funktionieren ähnlich wie traditionelle Block Rewards, da sie Loki nicht zufällig vergüten. Alle 43.000 Blöcke (ca. 60 Tage) wird ein Funding Block von Minern erstellt. Dieser Block enthält 1,25% der gesamten Blockprämie für die gesamte Finanzierungsperiode.

Um einen gültigen Finanzierungsblock zu erstellen, müssen Miner in der Lage sein, Vorschläge zu bewerten, die den erforderlichen Stimmenanteil erreicht haben. Dies geschieht, indem Informationen verwendet werden, die die Service-Nodes der Blockchain übergeben, die sowohl die zu bezahlenden Adressen als auch den Status aller Stimmen enthält. Alle Service-Nodes

validieren den Finanzierungsblock des Miners und verwerfen alle Finanzierungsblöcke, die ungültig sind.

Oft wird die benötigte Summe aus dem genehmigten Vorschlag ober- oder unterhalb der in der Zeitperiode von 60 Tagen aufgebauten Gesamtmenge liegen. Sollte die Summe der genehmigten Vorschläge die im Finanzierungsblock verfügbare Summe übersteigen, wird der Miner den Förderblock erstellen, periodisiert mit den Vorschlägen, die früher an die Blockchain übergeben wurden. Verbleibende genehmigte Vorschläge bleiben der Blockchain bis zum nächsten Finanzierungsblock erhalten.

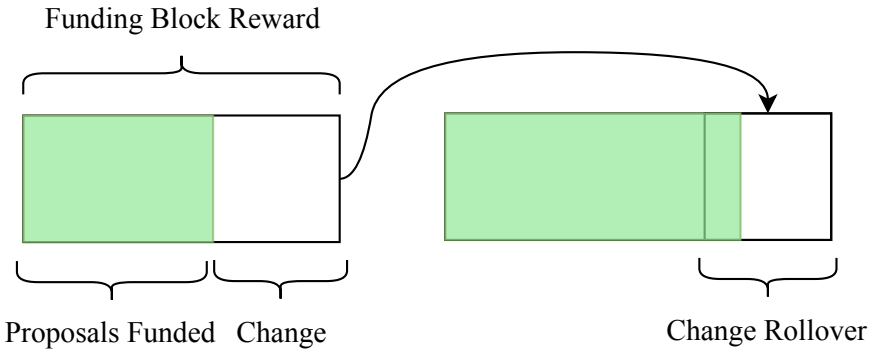

Abbildung 6: *Ungenutzte Mittel aus der aktuellen Funding Periode, erhöhen den Funding Block der nächsten Periode*

10 Fazit

Loki schlägt ein Modell für anonyme Transaktionen und dezentrale Kommunikation vor, das auf einem Netzwerk von wirtschaftlich incentivierten Nodes aufbaut. Loki nutzt die Grundlagen des CryptoNote Protokolls, um den Datenschutz zu gewährleisten und implementiert ein gesichertes System von Nodes, um die Ausfallsicherheit und Funktionalität des Netzwerks zu verbessern.

Darüber hinaus schlägt Loki Verbesserungen gegenüber früheren Forschungs- und Open Source Projekten vor und präsentiert ein neues anonymes Routing Protokoll, das deutliche Vorteile gegenüber bestehenden Protokollen bietet. Die Kombination eines einzigartigen Architektur- und Protokolldesigns schafft ein Netzwerk mit marktwirtschaftlich orientier Sybil Attacken Resistenz, verringert die Wirksamkeit der zeitlichen datenbezogener Analyse und bietet den Nutzern ein hohes Maß an digitaler Privatsphäre.

Literatur

[1] Mike Orcutt, *Criminals Thought Bitcoin Was the Perfect Hiding Place, but They Thought Wrong* (September 11, 2017), https://www.technologyreview.com/s/608763/criminals-thought-bitcoin-was-the-perfect-hiding-place-they-thought-wrong.

[2] *Monero*, https://getmonero.org.

[3] *Tor Project*, https://www.torproject.org.

[4] *I2P Anonymous Network*, https://geti2p.net/en.

[5] *LWMA Difficulty Algorithm*, https://github.com/zawy12/difficulty-algorithms/issues/3.

[6] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters, *Twisted Edwards Curves* (2008), https://eprint.iacr.org/2008/013.pdf.

[7] Nicolas van Saberhagen, *CryptoNote v 2.0* (2013), https://cryptonote.org/whitepaper.pdf.

[8] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Trans. Information Theory **IT-22** (1976), no. 6, 644–654. MR0437208

[9] Shen Noether, Adam Mackenzie, and Monero Core Team, *Ring Confidential Transactions* (2016), https://lab.getmonero.org/pubs/MRL-0005.pdf.

[10] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell, *Bulletproofs: Short Proofs for Confidential Transactions and More* (2017), https://eprint.iacr.org/2017/1066.pdf.

[11] Evan Duffield and Daniel Diaz, *Dash: A Privacy-Centric Crypto-Currency*, https://github.com/dashpay/dash/wiki/Whitepaper.

[12] *GitHub - loki-project/loki-network*, https://github.com/loki-project/loki-network.

[13] *Tor Project: Docs*, https://www.torproject.org/docs/faq#KeyManagement.

[14] *Possible upcoming attempts to disable the Tor network — Tor Blog.* (December 19, 2014), https://blog.torproject.org/possible-upcoming-attempts-disable-tor-network.

[15] Petar Maymounkov and David Mazières, *Kademlia: A Peer-to-peer Information System Based on the XOR Metric*, https://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf.

[16] Philipp Winter, Roya Ensafi, Karsten Loesing, and Nick Feamster, *Identifying and characterizing Sybils in the Tor network* (February 25, 2016), https://arxiv.org/abs/1602.07787.

[17] *OSI model - Wikipedia*, https://en.wikipedia.org/wiki/OSI_model.

[18] Farid Farid, *No Signal: Egypt blocks the encrypted messaging app as it continues its cyber crackdown* (December 26, 2016), https://techcrunch.com/2016/12/26/1431709.

[19] Matt Burgess, *Russia's Telegram block tests Putin's ability to control the web* (April 24, 2018), http://www.wired.co.uk/article/russia-google-telegram-ban-blocks-ip-address.

[20] *Go Ethereum - Postal Services over Swarm*, https://github.com/ethersphere/go-ethereum/blob/ddfc0a2a02ce574f4c252068ce81f0f5ada1c1ff/swarm/pss/README.md.

[21] Nikita Borisov, Ian Goldberg, and Eric Brewer, *Off-the-record Communication, or, Why Not to Use PGP*, Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society, 2004, pp. 77–84, DOI 10.1145/1029179.1029200.

[22] *NaCl: Networking and Cryptography library*, https://nacl.cr.yp.to.

[23] *Pidgin-Encryption - SourceForge*, http://pidgin-encrypt.sourceforge.net.

[24] *Irreversible Transactions - Bitcoin Wiki* (March 15, 2018), https://en.bitcoin.it/wiki/Irreversible_Transactions.

[25] *Scrypt - Litecoin Wiki - Litecoin.info* (February 12, 2018), https://litecoin.info/index.php/Scrypt.

[26] *Ethash · ethereum/wiki Wiki - GitHub*, https://github.com/ethereum/wiki/wiki/Ethash.

[27] *BITMAIN*, https://shop.bitmain.com/product/detail?pid=00020180314213415366s4au3Xw306A4.

[28] *Monero Cryptonight V7 - GitHub*, https://github.com/monero-project/monero/pull/3253/files/e136bc6b8a480426f7565b721ca2ccf75547af62.

[29] Alex Biryukov, Daniel Dinu, and Dmitry Khovratovich, *Argon2: the memory-hard function for password hashing and other applications* (December 26, 2015), https://password-hashing.net/argon2-specs.pdf.

[30] Dan Boneh, Henry Corrigan-Gibbs, and Stuart Schechter, *Balloon Hashing: A Memory-Hard Function Providing Provable Protection Against Sequential Attacks* (2017), https://eprint.iacr.org/2016/027.pdf.

[31] *GitHub - A Programmatic Proof-of-Work for Ethash*, https://github.com/ifdefelse/ProgPOW.

[32] *GitHub - hyc/randprog: Randomly generate a C (or javascript) program*, https://github.com/hyc/randprog.

[33] *GitHub - curie-kief/cryptonote-heavy-design: Cryptonote Heavy deign essay*, https://github.com/curie-kief/cryptonote-heavy-design.

[34] Surae Noether, Sarang Noether, and Adam Mackenzie, *A Note on Chain Reactions in Traceability in CryptoNote 2.0* (2014), https://lab.getmonero.org/pubs/MRL-0001.pdf.

[35] *Github Comment - EABE/Knacc Attack*, https://github.com/monero-project/monero/issues/1673#issuecomment-312968452.

[36] *I2P's Threat Model - I2P*, https://geti2p.net/en/docs/how/threat-model#harvesting.

[37] *Deep packet inspection - Tec Gov*, http://tec.gov.in/pdf/Studypaper/White%20paper%20on%20DPI.pdf.

[38] Philipp Winter and Stefan Lindskog, *How China Is Blocking Tor* (2012), https://arxiv.org/abs/1204.0447.

[39] *Egypt Quietly Blocks VOIP Services Skype, Whatsapp - TorGuard* (October 26, 2015), https://torguard.net/blog/egypt-quietly-blocks-voip-services-skype-whatsapp.

[40] *GitHub - Yawning/obfs4: The obfourscator (Development mirror)*, https://github.com/Yawning/obfs4.

[41] David Vorick and Luke Champine, *Sia: Simple Decentralized Storage* (2014), https://sia.tech/whitepaper.pdf.

[42] Adam Back, *Hashcash - A Denial of Service Counter-Measure* (2002), http://www.hashcash.org/papers/hashcash.pdf.

[43] Colin LeMahieu, *RaiBlocks: A Feeless Distributed Cryptocurrency Network*, https://raiblocks.net/media/RaiBlocks_Whitepaper__English.pdf.

[44] *Lazy Masternodes: do you actually have to do any work to get paid/vote?*, https://www.reddit.com/r/dashpay/comments/5t6kvc/lazy_masternodes_do_you_actually_have_to_do_any/.

[45] *ACNC template constitution for a charitable company*, https://acnc.gov.au/CMDownload.aspx?ContentKey=2efea0fa-af4f-4231-88af-5cffc11df8b7&ContentItemKey=6046cbc5-d7fd-4b6b-93ba-c8e3114b07ba.