Loki

Transacciones privadas, comunicación descentralizada.

Kee Jefferys, Simon Harman, Johnathan Ross, Paul McLean

Versión 3

13 de julio de 2018

Resumen

Un sistema híbrido de prueba de trabajo / prueba de servicio ofrece una manera única de incentivar financieramente la operación de nodos completos (full nodes). Loki utiliza estos nodos incentivados para crear una capa de enrutamiento privada secundaria. La funcionalidad con el mínimo de nodos en la segunda capa es monitoreada y ejecutada por un método innovador llamado marcado de enjambre (swarm flagging). Loki está basado en una versión modificada del código fuente de Monero, asegurando que todas las transacciones alcancen un alto grado de privacidad.

Este documento técnico describe la tecnología usada en Loki. Anticipamos que cambios a esta tecnología van a ocurrir mientras Loki continúa siendo desarrollado. Nuevas versiones de este documento técnico se publicarán para reflejar cualquier cambio sustancial, o actualizaciones futuras.

1. Introducción

La demanda de privacidad en las comunicaciones y transacciones digitales está creciendo continuamente. Datos de los usuarios son recolectados, procesados e intercambiados a niveles nunca antes vistos. Cualquier cosa desde datos de navegación y contenido de emails de usuarios, hasta la calificación crediticia y hábitos de compra, son recolectados y vendidos entre las mayores empresas del mundo y actores a nivel estatal. Loki aspira a ofrecer un paquete de herramientas resistentes a la censura que van a permitir a los usuarios operar y comunicarse en forma privada.

Bitcoin surgió con la promesa de la privacidad, pero ha resultado tener mayor rastreabilidad a la alguna vez esperada. Empresas como Chainanalysis y BlockSeer tomaron ventaja de la arquitectura transparente de Blockchain para rastrear y seguir transacciones específicas [1]. Loki se basa en Monero, una criptomoneda que se ha establecido a sí misma como una de las redes de transacciones más seguras y privadas hasta la fecha [2]. Sin embargo, reconocemos que Monero tiene desventajas inherentes. Las transacciones de Monero son movimientos de

mayor magnitud que las transacciones de Bitcoin, con importantes requerimientos de ancho de banda, procesamiento, y espacio en disco. Conforme la red crece, esto resulta en una mayor carga sobre los operadores de nodos de Monero y no ofrece ningún incentivo o beneficio a sus contribuciones a la red. Esto hace que correr nodos sea costoso y, con frecuencia, un ejercicio ingrato. La introducción de un esquema de compensación de nodos, llamado Nodos de Servicio, mitiga esta situación, al proveer incentivos económicos a los operadores de los mismos.

Los Nodos de Servicio también pueden ser usados para ofrecer otro rango de funciones centradas en la privacidad si están adecuadamente incentivados. Primeramente, la red de Nodos de Servicio va a permitir a los usuarios transmitir y recibir paquetes de datos anónimamente. Esta comunicación privada es facilitada por cada Nodo de Servicio actuando como un relevo en una original red mixta resistente a ataques de tipo Sybil, presentando propiedades similares a las de Tor y I2P [3][4]. Más aún, esta red de comunicaciones emergente podrá ser usada como la columna vertebral de un servicio de mensajería descentralizado y encriptado de principio a fin, llamado Loki Messenger, que va a permitir a los usuarios comunicarse directamente, sin depender de una tercera parte confiable y sin el requerimiento de que ambas partes estén al mismo tiempo en línea.

Loki no sólo es un medio de intercambio privado resistente, sino también una plataforma de servicios de internet descentralizados y anónimos.

2. Parámetros Básicos

Objetivo de Dificultad Loki (Tiempo de bloque)	120 segundos
Algoritmo de dificultad	Zawy LWMA [5]
Algoritmo de hasheo	CryptoNight Heavy
Curva elíptica	Curve25519 [6]

3. Elementos CryptoNote

Aunque se podría implementar un esquema de incentivos de nodo completo sobre cualquier criptomoneda, Loki usa el código fuente de Monero debido al alto nivel de privacidad con el que le permite transaccionar. Monero es una evolución del protocolo CryptoNote, que utiliza firmas de círculo, direcciones ocultas y RingCT, dando a los usuarios la capacidad de firmar transacciones y ocultar las cantidades mientras mantiene una negación plausible [7].

Para que el ecosistema de Loki mantenga privacidad, es importante no solo proporcionar un medio de intercambio que respalde la economía interna, sino también minimizar el riesgo de análisis temporal cuando se producen interacciones a través de las capas independientes de Loki. Por ejemplo, cuando se emplea en servicios transaccionales de primera capa, los usuarios no deberían perder las garantías de privacidad que reciben de la segunda capa y viceversa.

3.1. Firmas de Círculo

Las firmas de círculo funcionan al construir un conjunto de posibles firmantes para una transacción donde solo uno de los firmantes es el signatario real. Loki hace uso de las firmas de círculo para ocultar lo que ocurrió con las transacciones de salida. Las firmas de círculo serán obligatorias para todas las transacciones de Loki (excluidas las transacciones de recompensas de bloque) y, de manera única, se aplicará un tamaño de círculo fijo de diez en la cadena de bloques. Esto significa que cada entrada se gastará de una de las diez salidas posibles, incluyendo la salida verdadera (ver 6.3).

3.2. Direcciones Ocultas

Loki hace uso de direcciones ocultas para garantizar que la verdadera clave pública del receptor nunca sea asociada a su transacción. Cada vez que se envía una transacción de Loki, una única dirección oculta se crea y los fondos se envían a dicha dirección. Usando un intercambio de claves Diffie-Hellman, el receptor de una transacción puede calcular una clave de gasto privada para la dirección oculta, tomando de esta forma la propiedad de los fondos sin tener que revelar su verdadera dirección pública [8]. Las direcciones ocultas brindan protección a los receptores de transacciones y son un pilar funcional fundamental en la privacidad de Loki.

3.3. RingCT

RingCT fue propuesto por primera vez por el equipo de investigación de Monero (Monero Research Lab) como una forma de ocultar las cantidades de las transacciones [9]. Implementaciones actuales de RingCT usan pruebas de rango, que utilizan cometidos de Pedersen (Pedersen commitments) para demostrar que el monto de la transacción enviada está entre 0 y 2^{64}. Este rango garantiza que solo se envíen cantidades de moneda no negativas, sin revelar la cantidad real enviada en la transacción. Recientemente, varias criptomonedas han propuesto implementar "bulletproofs" como reemplazo de las pruebas de rango tradicionales en RingCT debido a que brindan una reducción significativa en el tamaño de la transacción [10]. Loki utilizará "bulletproofs" para reducir la información que los nodos deben almacenar y retransmitir, mejorando así la escalabilidad.

4. Nodos de Servicio

Aunque Loki implementa cambios novedosos sobre el protocolo CryptoNote (ver 7), gran parte de la funcionalidad y escalabilidad de red de Loki es habilitada por un conjunto de nodos incentivados llamados nodos de servicio. Para operar un Nodo de Servicio, un operador debe bloquear por un tiempo una cantidad significativa de Loki y proporcionar un nivel mínimo de ancho de banda y almacenamiento a la red. A cambio de sus servicios, los operadores de Nodo de Servicio de Loki reciben una parte de la recompensa de bloque de cada bloque.

La red resultante proporciona resistencia basada en el mercado a ataques de tipo Sybil, abordando una gama de problemas de las redes mixtas existentes y los servicios centrados en la privacidad. Esta resistencia se basa en interacciones de oferta y demanda que ayudan

a prevenir que un único actor tenga una participación lo suficientemente grande en Loki como para ocasionar un impacto negativo en los servicios de privacidad que Loki brinda en la segunda capa. DASH teorizó en primera instancia que redes resistentes a ataques de tipo Sybil pueden ser derivadas de la criptoeconomía [11]. A medida que un atacante acumula Loki, la oferta circulante disminuye, a su vez ejerciendo presión del lado de la demanda, llevando el precio de Loki a subir. Mientras esto continúa, se hace cada vez más costoso comprar más unidades de Loki, generando que el ataque sea prohibitivamente caro.

Para alcanzar esta protección económica, Loki estimula la supresión activa de la oferta circulante. En particular, la curva de emisiones y requerimientos de garantía deben ser designados para asegurar que suficiente oferta circulante esté bloqueada y que los operadores reciban retornos razonables para asegurar resistencia a ataques de tipo Sybil.

4.1. Recompensa de bloque

La distribución de las recompensas de bloque en Loki es conducida a través de un sistema de prueba de trabajo, un sistema robusto y bien estudiado para la creación de bloques y los pedidos de transacciones. Los mineros colectan y escriben las transacciones en bloques y reciben pagos por hacerlo. Como una regla de consenso en Loki, cada bloque contiene múltiples emisiones de recompensas, de las cuales sólo una es dirigida al minero.

Recompensa de minería:
Además de recibir pagos de las transacciones, 45 % de la recompensa de bloque es entregada al minero que construye el bloque.

Recompensa de Nodo de Servicio:
El segundo producto de cada bloque (50 % de la recompensa total) va a un Nodo de Servicio, o dos Nodos de Servicio si un relevo es utilizado (ver 6.3). Los Nodos de Servicio son recompensados en base al tiempo desde que recibieron por última vez una recompensa (o el tiempo desde que se registraron), con una preferencia por los nodos que han estado esperando más tiempo. Cada vez que un Nodo de Servicio se registra en la red asume la última posición en la cola. Si el Nodo de Servicio ofrece un buen servicio y por ende no es expulsado de la cola por una bandera de enjambre (ver 7.3), va migrando lentamente a posiciones más altas en la misma. Los nodos al frente de la cola, o cerca de él, son elegibles para una recompensa, y una vez recompensados, el nodo de nuevo cae a la última posición en la cola y empieza lentamente a hacer su camino hacia arriba de nuevo.

Recompensa de gobierno:
El 5 % final de la recompensa de bloque es distribuida hacia operaciones de gobierno (ver 9); 3,75 % es enviado a la dirección de las bases de Loki, que es derivada deterministicamente de cada bloque, y el 1,25 % restante es reservado para las emisiones de un bloque de financiamiento (ver 9.2.3).

4.2. Garantización verificable

Los Nodos de Servicio deben probar a la red que están manteniendo las garantías requeridas. Los rasgos de privacidad inherentes al diseño de Loki hacen esto difícil, específicamente la imposibilidad de auditar balances de dirección pública o de usar “viewkeys” para ver las transacciones salientes.

Loki hace un uso novedoso de emisiones "time-locked", que permiten a las monedas de Loki ser "time-locked" hasta que la cadena de bloques alcanza una altura de bloque definida. Hasta esta altura definida, la red de Loki invalidará los intentos de gastar estas emisiones "time-locked". Loki utiliza este proceso para probar que una cantidad está siendo mantenida por un Nodo de Servicio específico, previniendo que las garantías se mezclen.

Para registrarse como un Nodo de Servicio, un operador crea una emisión de la cantidad requerida bloqueada por tiempo, que se desbloquea después de que un mínimo de 21.600 bloques haya transcurrido (aproximadamente treinta días). En el campo extra de la transacción, el operador del Nodo de Servicio incluye la dirección de Loki en la que quiere recibir las recompensas de Nodo de Servicio. Esta dirección también será usada como la llave pública para las operaciones del Nodo de Servicio tales como votaciones de enjambre. Los monederos podrán evitar usar estas transacciones de registro de Nodo de Servicio como redes mixtas, dado que sus verdaderas cantidades y destinos son de acceso público, por lo cual no son útiles en proveer mayor anonimidad a una transacción.

Antes de que cada nodo se una a la red de Nodos de Servicio, otros nodos deben validar individualmente que el desembolso de las garantías de los nodos indicadas se corresponda con la cantidad requerida, como también el requerimiento de garantía decreciente. Aunque las transacciones garantizadas expiran luego de treinta días, el monedero tendrá una función opcional para renovar la garantía automáticamente.

5. Lokinet

Los protocolos de ruteo Onion permiten a los usuarios formar túneles o caminos a través de una red distribuida, usando múltiples nodos como saltos para ofuscar el destino y el origen de los paquetes de datos. Los Nodos de Servicio en la red de Loki operarán un protocolo de ruteo Onion de baja latencia, formando una red superpuesta completamente descentralizada, llamada Lokinet. La red no depende de autoridades de confianza y su estado es totalmente derivado a partir de la cadena de bloques. Los usuarios pueden conectarse a Nodos de Servicio individuales y crear trayectorias bidireccionales para que los paquetes sean transportados a través de ellas. La red puede ser usada para acceder a servicios brindados internamente llamados SNApps (ver 6.2). Asimismo, los usuarios pueden utilizar la funcionalidad de salida de Nodo de Servicio para explorar la internet externa sin que su dirección IP sea expuesta (ver 6.3).

5.1. Protocolo de Ruteo Anónimo de Baja Latencia (LLARP)

Subyacente a todas las aplicaciones para Nodos de Servicio está un protocolo de ruteo anónimo, que define el modo en que cada Nodo de Servicio se comunica con sus pares. Loki propone un nuevo protocolo de ruteo llamado LLARP [12], el cual está diseñado como un híbrido entre Tor y I2P para proveer de propiedades adicionales deseables para cualquier protocolo de ruteo existente. LLARP es construido específicamente para correr sobre la red de Nodos de Servicio Loki y todas las optimizaciones de LLARP consideran esta arquitectura. Para entender los avances de LLARP, lo mejor es conducir un análisis de los protocolos de ruteo existentes y considerar cómo LLARP los supera.

El enrutador Onion (Tor)

En años recientes, Tor ha sido la red mixta anónima más popular. La red Tor mantiene un alto nivel de resistencia a la censura y ha probado ser una herramienta valiosa para preservar la privacidad en internet. Aun así, Tor no es tanto una red descentralizada como una jerárquica. Tor depende de un grupo de autoridades del directorio, las cuales son servidores centralizados operados por un grupo de voluntarios cercanos a la Fundación Tor [13]. Estas autoridades del directorio cumplen dos funciones principales. En primer lugar, actúan como reporteros de confianza sobre el estado de los nodos en la red. Cuando un usuario Tor (o relevo) se conecta a la red por primera vez, se pueden conectar con una de diez autoridades del directorio "hard-coded". Estas autoridades del directorio proveen al usuario o al relevo con un archivo llamado consenso. Este archivo provee una lista de todos los relevos, nodos guardianes, y nodos de salida actualmente en operación (excluyendo puentes) en la red Tor. En segundo lugar, las autoridades del directorio también miden el ancho de banda que cada relevo puede proveer a la red. Usan esta información para clasificar a los relevos en categorías, decidiendo si los nodos pueden operar como relevos, nodos guardianes, o nodos de salida.

Este alto nivel de centralización crea puntos débiles que hacen a Tor vulnerable. En 2014, Tor recibió información sobre una amenaza creíble de derribar a los servidores de autoridad del directorio [14]. Si las autoridades del directorio en Estados Unidos y de Alemania u Holanda fueran apartadas, eso sería suficiente para remover a cinco de diez servidores de autoridad del directorio. Esto resultaría en una altamente inestable red Tor, con nuevos relevos siendo disminuidos en gran manera en su habilidad para interactuar con la red.

Los métodos de comunicación en Tor son también limitados, ya que Tor sólo permite comunicación a través de TCP. IP a través Tor es posible, pero falta apoyo para protocolos basados en UDP (tales como VoIP).

Proyecto de Internet Invisible (I2P)

I2P toma un enfoque diferente de la arquitectura de redes mixtas (mixnet), manteniendo un nivel más alto de confianza al referirse a una Tabla de Hasheo Distribuida (DHT) para determinar el estado de la red en lugar de utilizar autoridades de directorio de confianza [15]. I2P también permite el tráfico TCP y UDP, lo que permite un mayor alcance de las interacciones de protocolo. Sin embargo, I2P no ha tenido un proceso de desarrollo estable y con el tiempo ha acumulado algunas deficiencias, específicamente en su uso de criptografía. I2P usa 2048 bit ElGamal, lo que hace que el cifrado y descifrado sean lentos en comparación con las operaciones de curva elíptica. Existen planes en la hoja de ruta para migrar lejos de ElGamal, el progreso ha sido lento.

Además, I2P carece de soporte formal para los nodos de salida, lo que significa que la mayoría del tráfico en la red está accediendo a sitios web alojados internamente llamados Eepsites. Esto ha reducido en gran medida la capacidad de la red I2P para llegar a los usuarios cuyo principal objetivo para el uso de redes anónimas es acceder a Internet en general.

Adicionalmente, la forma en que se construye I2P significa que la mayoría de los usuarios que se conectan a la red también se convierten en enrutadores, lo cual es problemático ya que la red resultante carece de ancho de banda suficiente para poder establecer rutas rápidas (fast paths). Las velocidades de red en las redes mixtas están embotelladas por el nodo menos capaz en cada circuito, y por ende cada usuario enrutador de bajo rendimiento enlentece la red general.

Por último, I2P difiere de Tor ya que ofrece una red de conmutación de paquetes (en lugar de conmutación de circuitos). En vez de establecer un único túnel por el cual todo el tráfico es direccionado, I2P establece múltiples rutas donde cada paquete que se comunica puede

utilizar una ruta distinta a través de la red. Esto le da a I2P la capacidad de evitar de forma transparente la congestión de la red y las fallas de los nodos.

Tanto I2P como Tor no han mitigado completamente los ataques de Sybil. Un atacante lo suficientemente motivado, que tenga tiempo suficiente y capital para comprar grandes cantidades de repetidores puede realizar un análisis temporal puede poner en riesgo la privacidad de los usuarios. La efectividad de este análisis aumenta con la cantidad de nodos de salida, enrutadores y nodos de guardia opera el atacante [16]. Tor e I2P son operados completamente por voluntarios que donan tiempo y dinero para que los nodos operen. Suponemos que una red construida a partir de incentivos financieros en lugar de altruismo puede lograr una mayor resiliencia contra los ataques y a la vez proporcionar un servicio más confiable.

LLARP

LLARP opera sin la necesidad de hacer uso de las autoridades de directorio y, en cambio, depende de un DHT creado a partir de las transacciones de "staking" en la cadena de bloques que permite que los Nodos de Servicio actúen como enrutadores en la red. El ancho de banda no se monitorea ni registra en el DHT. En cambio, se utilizan las lecturas del ancho de banda y la selección de enjambres (ver 6.1.1) que son las que evalúan cada nodo y juzgan la capacidad de los nodos para proporcionar el ancho de banda apropiado para la red.

En el modelo de Interconexión de sistemas abiertos (modelo OSI), LLARP solo intenta proporcionar una capa de red anónima. Esto significa que es compatible con una gama más amplia de protocolos de Internet y que también minimiza la carga para almacenar descriptores de archivos en caso de que los nodos de salida atraviesen el tráfico del Protocolo de datagramas de usuario (UDP) [17]. Además, LLARP opta por el enrutamiento basado en paquetes conmutados en lugar del enrutamiento basado en túneles, lo que permite un mejor equilibrio de carga y redundancia en toda la red.

No se espera (ni se permite) que los usuarios finales de Lokinet enruten paquetes, lo que significa que Lokinet se expone a una superficie de ataque mucho más baja para un ataque Sybil ya que la inversión en capital requerida para conseguir un Nodo de Servicio es importante.

6. Servicios de Loki

De forma similar a la inversión que hacen los mineros en hardware, cada operador de Nodo de Servicio deberá congelar Loki para comenzar a operar un Nodo de Servicio. Este capital congelado tiene dos propósitos.

1. Cada operador de Nodo de Servicio tendrá un interés lo suficientemente grande en el éxito de la red. Si un operador de Nodo de Servicio proporciona un rendimiento deficiente a la red o actúa de manera deshonesta, socava y arriesga la devaluación de su propia participación en la red.

2. Brinda una oportunidad para aplicar una seguridad más firme; si la red es capaz de limitar la cantidad de nodos deshonestos que reciben recompensas entonces, los nodos deshonestos deberán asumir el costo de oportunidad tanto de la pérdida de la recompensa como del tiempo de inmovilización restante de su garantía.

Si consideramos que los puntos anteriores son ciertos, y podemos aplicar castigos agresivos con los nodos deshonestos (ver 7.3), entonces podemos crear grupos de Nodos de Servicio que puedan consultarse para llegar a un consenso sobre el estado de la cadena de bloques o

para hacer cumplir el comportamiento correcto de un nodo fuera de la cadena (ver enjambres 6.1.1). En Loki, este comportamiento se relaciona con las actividades de red y almacenamiento. Estas actividades fuera de cadena se combinan para ser el back-end de las aplicaciones orientadas al usuario que utilizan estas propiedades, que son conocidos como servicios de Loki.

6.1. Loki Messenger

El primer servicio de Loki que se desarrollará y desplegará en la red Loki será una aplicación de mensajería privada descentralizada y encriptada de extremo a extremo que se llamará Loki Messenger.

Las aplicaciones de mensajería cifradas de extremo a extremo que proporcionan una plataforma para que los usuarios envíen mensajes sin revelar sus contenidos ya existen, aunque dependen de servidores centralizados que pueden ser atacados, bloqueados y cerrados [18][19]. Estos modelos de negocio centralizados presentan un alto riesgo para el anonimato de las partes que se comunican, ya que a menudo requieren que el usuario registre un número de teléfono u otra información de identificación y se conecte directamente a través de la dirección IP del mismo. Esta información podría extraerse de los servidores a través de filtraciones de datos o procesos legales y usarse contra el usuario. Utilizando la arquitectura de Nodos de Servicio en la red Loki, podemos ofrecer un servicio similar al de las populares aplicaciones de mensajería cifradas y centralizadas, como Signal, pero con un mayor grado de privacidad y resistencia a la censura.

6.1.1. Enrutamiento de los mensajes

El enrutamiento de mensajes en la red Loki cambia dependiendo de si el usuario receptor está en línea o fuera de línea. Cuando ambos usuarios están en línea, se pueden utilizar comunicaciones de mayor ancho de banda debido a que los mensajes no necesitan almacenarse en los Nodos de Servicio.

En Loki, una clave pública actúa como clave de cifrado a largo plazo y una dirección de enrutamiento. En el caso más simple, esta clave debe intercambiarse fuera de banda para garantizar la protección contra un ataque de intermediario (man-in-the-middle) Tal intercambio debe realizarse en persona o mediante otro modo de intercambio seguro (ver 6.1.2).

Mensajería en línea

Una vez que Alice conoce la clave pública de Bob, ella asume que el está en línea e intenta crear una ruta con el. Alice hace esto consultando el DHT de cualquier Nodo de Servicio y obtiene cualquier conjunto de introducción que se corresponda con la clave pública de Bob. En LLARP, los conjuntos de introducción enumeran los presentadores que cada usuario mantiene. Es a través de estos presentadores que se pueden establecer caminos. Con el introductor de Bob, Alice ahora elige tres Nodos de Servicio aleatorios para actuar como saltos intermedios entre su origen y su destino (introductor de Bob). Ahora se ha establecido un camino por el cual Alice y Bob pueden transmitir mensajes. Si se autentica correctamente y utiliza OTR (ver 6.1.2), Alice y Bob pueden comunicarse manteniendo un alto nivel de privacidad.

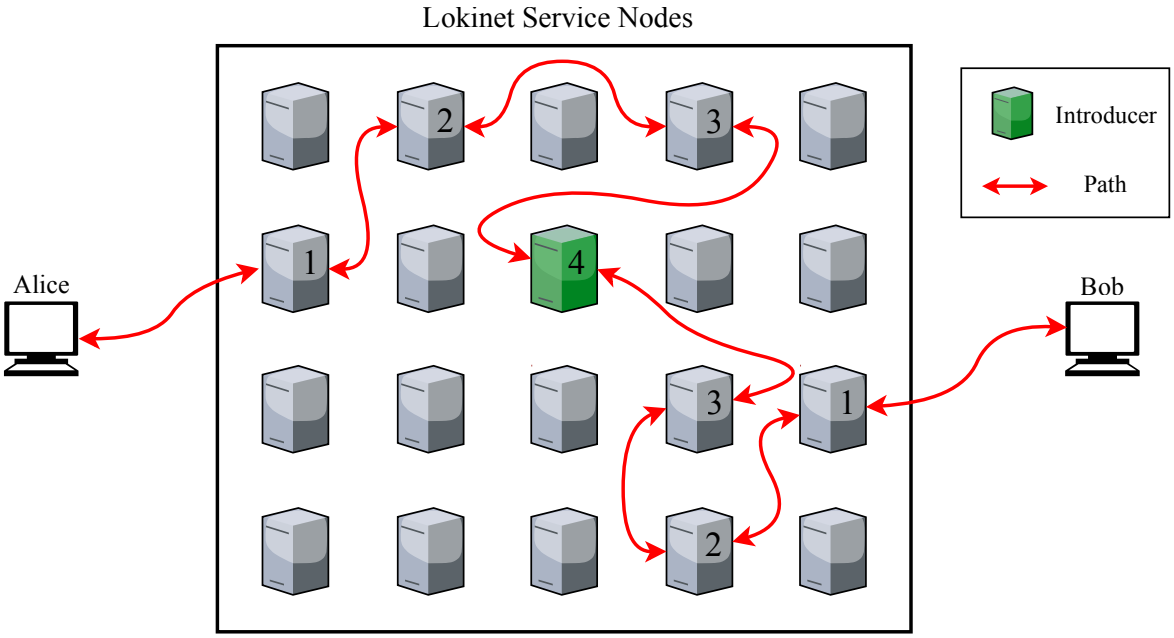

Figura 1: *Versión simplificada del enrutamiento online donde Alice se comunica con Bob, utilizado un Nodo de Servicio aleatorio estableciendo un camino en la red.*

Mensajería fuera de línea

Si Alice no recibe una respuesta de Bob, puede iniciar el proceso de mensajería sin conexión. El enrutamiento fuera de línea usa una versión modificada de Postal Services over Swarm (PSS) [20]. Los enjambres son agrupaciones lógicas de Nodos de Servicio, basadas tanto en sus claves públicas como en el hash del bloque en el que apareció por primera vez la transacción. Cada enjambre tiene un swarmID y consta de nueve nodos. Para enviar un mensaje a Bob, Alice puede usar su clave pública para calcular a qué enjambre pertenece Bob. Con esta información, Alice puede enrutar de forma anónima un mensaje a través de la red a un Nodo de Servicio aleatorio en dicho enjambre. Cuando un Nodo de Servicio recibe un mensaje único destinado a su enjambre, debe distribuir dicho mensaje a los otros ocho nodos en el enjambre. Todos los nodos se requieren adicionalmente para almacenar mensajes para su Time-to-live (TTL) asignado (ver 8.3). Cuando Bob entra en línea, puede consultar dos nodos en su enjambre para buscar mensajes que pueda descifrar. Los mensajes sin conexión están protegidos contra el correo no deseado con una pequeña prueba de trabajo adjunta a cada mensaje (ver 7.2).

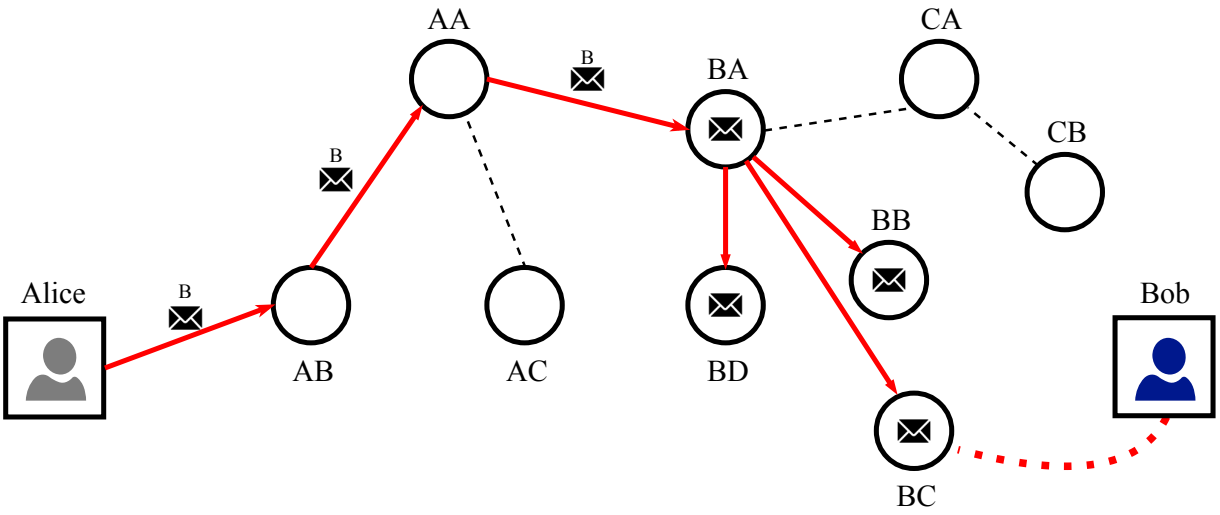

Figura 2: *Alice envía un mensaje a Bob, el enjambre asignado a Bob es B. Cuando Bob está en línea, solicita un nodo aleatorio en su enjambre y recibe el mensaje de Alice.*

6.1.2. Encriptación y autenticación de Mensajería

Una vez que se establece una cadena de mensajes, Loki Messenger aplica Perfect Forward Secrecy (PFS) y Deniable Authentication (DA). PFS y DA son conceptos clave del protocolo de mensajes Off The Record (OTR) [21]. Los servicios centralizados, como Signal y WhatsApp, usan funciones de encriptación que mantienen las protecciones OTR. Loki modela su implementación OTR del protocolo Tox existente, que es un protocolo de mensajería instantánea peer-to-peer distribuido que utiliza la biblioteca NaCl altamente auditada [22].

PFS permite resistir a los ataques donde se expone una clave por un largo período de tiempo. Se usa una nueva clave de cifrado compartida para cada sesión, de modo que si se revela una sola clave de sesión, no se compromete toda la cadena de mensajes. Si un tercero desea romper el cifrado de una cadena de mensajes, necesitaría obtener las claves para cada sesión individual. PFS garantiza que Loki Messenger es extremadamente difícil de comprometer en comparación con los métodos existentes, como el cifrado Pretty Good Privacy (PGP), donde solo se requiere un par de claves a largo plazo para comprometer toda la cadena de mensajes.

DA se refiere a la habilidad para las dos partes de probarse entre sí que son los emisores de cada nuevo mensaje. Aun así, un tercero no puede determinar quién es el verdadero emisor de un mensaje. Cuando se usa DA, Códigos de Autenticación de Mensajes (MACs) son publicados después de cada sesión, permitiendo a terceras partes crear mensajes creíbles que aparezcan como si se originaron en la dirección pública de los emisores. Cuando es correctamente implementado, es imposible para cualquier tercera parte el probar que el emisor de un mensaje específico era el verdadero emisor.

Autenticación del usuario

La autenticación de los usuarios es importante para asegurar protección contra ataques de intermediario. Por ejemplo, si Bob está esperando un mensaje de parte de Alice, pero todavía no sabe cuál es su dirección pública, entonces una tercera parte (Eve), podría enviar un mensaje a Bob pretendiendo ser Alice. Esta es la razón por la que los usuarios deberían identificarse a sí mismos antes de compartir información personal.

Al igual que Pidgin y otros servicios de mensajería OTR, Loki Messenger usa la autenticación

de clave precompartida (PSK). Los usuarios tienen múltiples opciones para el establecimiento de un PSK. Pueden establecer una clave fuera de banda, o alternativamente, pueden acordar una PSK sobre Loki Messenger haciéndole una pregunta al otro, que ningún tercero sabría la respuesta. Loki implementará la autenticación PSK basada en una versión modificada del complemento de autenticación de cifrado Pidgin [23].

6.2. SNApps (Aplicaciones de Nodo de Servicio)

La función de SNApps es similar a la de los llamados servicios ocultos en Tor, que han florecido. Proporcionan a los usuarios una forma de interactuar completamente dentro del entorno de mixnet, proporcionando un grado de anonimato incluso mayor que el que se puede lograr al acceder al contenido alojado externamente. SNApps permite a los usuarios configurar y hospedar mercados, foros, sitios web de denuncias, redes sociales y la mayoría de las demás aplicaciones de Internet en sus propias máquinas o servidores, manteniendo el anonimato del servidor y del lado del usuario. Esto amplía enormemente el alcance de la red y permite a los usuarios construir comunidades significativas dentro de Lokinet.

Los operadores de SNApp utilizan el modelo tradicional de servidor-cliente con la diferencia clave de que los Nodos de Servicio serán intermediarios en la conexión de un usuario a través de Lokinet. Cuando un SNApp desea registrarse en la red, debe actualizar el DHT con su descriptor. Este descriptor contiene varios introductores, que son Nodos de Servicio específicos que los usuarios pueden contactar para formar una ruta al SNApp. Cuando se establecen estas rutas, los usuarios pueden conectarse al SNApp sin que ninguna de las partes sepa dónde se encuentra el otro en la red.

6.3. Nodos de salida

Los nodos de salida permiten a los usuarios realizar solicitudes la internet más amplia y responder esas solicitudes a través de una red mixta. Si se usan correctamente, los nodos de salida permiten a los usuarios navegar por internet de forma privada y sin que la dirección IP del usuario quede expuesta al servidor.

Aunque la operación de los nodos de salida es esencial para la utilidad extendida de Loki, forzar a todos los operadores del Nodo de Servicio a actuar como nodos de salida podría ser perjudicial. Actuar como un nodo de salida puede exponer al operador a riesgos legales, ya que los usuarios del nodo de salida pueden realizar actividades maliciosas mientras lo utilizan como un proxy. Como los nodos de salida simplemente retransmiten el tráfico desde Internet al usuario final, los nodos de salida a menudo reciben demandas de la Ley de Derechos de Autor del Milenio Digital (DMCA) o se supone a menudo que son la fuente de los ataques de hackeo. Aunque en la mayoría de las jurisdicciones las leyes de refugio seguro pueden proteger a los operadores de nodos de salida, los proveedores de servicios de Internet que llevan tráfico de Nodo de Servicio en sus servidores pueden temer riesgos legales y a menudo cortar el servicio al nodo de salida.

Al inicio, se le asigna un indicador de retransmisión a un Nodo de Servicio y está restringido a los paquetes de enrutamiento dentro de la Lokinet, pero nunca realiza solicitudes al Internet más amplio. Un operador debe optar si desea convertirse en un nodo de salida. Al hacerlo, demuestra una comprensión de los riesgos adicionales mientras se someten a pruebas adicionales de Swarm (ver 8.3.1).

Optar por un nodo de salida permite que un operador duplique la recompensa de un relevo normal cuando se lo selecciona para una recompensa de bloque. Este incentivo se proporciona para garantizar que los operadores de nodo de salida tengan suficientes incentivos financieros para operar los nodos de salida, colaborando en la protección contra ataques de Sybil específicamente dirigidos a hacerse cargo de la red de nodos de salida. Esta es una vulnerabilidad que Tor sufre debido a su baja proporción de nodos de salida a retransmisores.

6.4. Nodos remotos

En cualquier red de criptomoneda dada, almacenar una copia completa de la cadena de bloques no es posible ni práctico para muchos usuarios. En Bitcoin y Ethereum, los usuarios pueden optar por conectarse a un nodo público completo que contiene una copia de la cadena de bloques y puede consultar y enviar transacciones a la red. Esto funciona porque los nodos completos de Bitcoin y Ethereum pueden buscar eficientemente el blockchain para las transacciones que tienen como objetivo la clave pública del usuario.

Debido a la construcción de las monedas de CryptoNote, los nodos completos públicos (llamados nodos remotos) sufren mucho más estrés. Cuando un usuario se conecta a un nodo remoto, deben temporalmente descargar cada bloque (en la creación del monedero o desde el último bloque verificado) a su máquina local y verifique cada transacción para una clave de transacción pública que se puede generar desde la clave de vista privada del usuario. Este proceso puede causar un impacto significativo en el rendimiento de los nodos remotos. Teniendo en cuenta que no hay recompensa por este servicio, puede disuadir a los usuarios de que operen servicios de sincronización para clientes ligeros. Los monederos móviles de CryptoNote a menudo no son confiables y algunas veces tienen que cambiar entre nodos remotos varias veces antes de establecer una conexión confiable para escanear el blockchain o enviar una transacción.

Además, los operadores de nodos remotos maliciosos que ejecutan uno de los pocos nodos populares pueden registrar la dirección IP de los usuarios mientras transmiten transacciones específicas. Aunque este ataque no revela ninguna información sobre la transacción real, las direcciones IP específicas pueden vincularse con transacciones que luego pueden usarse para establecer un enlace a una identidad del mundo real, comprometiendo la privacidad.

Loki elude estos problemas al requerir que cada Nodo de Servicio actúe como un nodo remoto que puede ser utilizado por usuarios generales. Los Nodos de Servicio se prestan naturalmente a este trabajo, ya que ya tienen una copia completa de la cadena de bloques y forman una red ampliamente distribuida de nodos de gran ancho de banda. Al usar Nodos de Servicio como nodos remotos, existe una limitación financiera inherente en cuanto a la cantidad de la red de nodos remotos que cada parte puede poseer y, por lo tanto, la cantidad de datos que puede recopilar un operador de nodo malicioso.

6.5. Blink

En un sistema de cadena de bloques típico, el tiempo de confirmación para cualquier transacción dada es el tiempo que tarda una transacción en ser incluida en un bloque. Debido a la competencia de los mineros, los bloques retenidos y los ataques de Finney, los destinatarios generalmente requieren que se creen varios bloques adicionales posteriores al que contiene una transacción antes de que se considere completa [24]. Dependiendo de una multitud de

factores específicos de cada cadena de bloques, este proceso a menudo puede demorar de 10 a 60 minutos, lo que es inconveniente para los comerciantes y clientes que deben esperar las confirmaciones antes de liberar productos o comenzar servicios.

Debido a la arquitectura del Nodo de Servicio de Loki, son posibles transacciones casi instantáneas. Blink permite que se confirmen las mismas transacciones que ocurrirían en la cadena principal de Loki antes de ser incluidas en un bloque, asegurando tanto al emisor como al receptor la validez de la transacción y protegiendo al receptor contra un gasto doble.

Blink funciona de manera similar a InstantSend de DASH. En cada bloque, un enjambre de Nodo de Servicio se determina de forma determinística para actuar como un conjunto de testigos que confirman la validez de una transacción y bloquean la misma para que no se gaste dos veces. En lugar de que las salidas no utilizadas en la transacción estén bloqueadas (como en DASH), las imágenes clave se bloquean. Las imágenes clave son claves únicas que se adjuntan a cada salida no utilizada en una firma de círculo. Para proporcionar confirmaciones inmediatas, Blink le da autoridad al enjambre seleccionado para indicar a la red que una imagen clave asociada con una salida debe estar bloqueada hasta que la transacción se incluya en un bloque. Si se intenta gastar dos veces la misma salida que aún no fue gastada, se produce una imagen clave idéntica, que sería rechazada por el enjambre y, por lo tanto, la red como un todo.

Los usuarios tendrán la posibilidad de pagar una tarifa más alta para enviar una transacción de Blink que se confirmará en segundos en lugar de en minutos. Esto abre una gama de nuevos casos de uso para Loki, donde los pagos cara a cara se vuelven cada vez más prácticos y los pagos en línea se vuelven más fáciles de integrar. Todas las características de privacidad inherentes a Loki son inflexibles a lo largo de este proceso.

7. Alteraciones de CryptoNote

Como una criptomoneda, Loki es funcionalmente similar al resto de las monedas CryptoNote. Sin embargo, existen algunas diferencias clave más allá de la adición de Nodos de Servicio y la funcionalidad asociada que viene con ellos.

7.1. Resistencia a ASICs

Un circuito integrado de aplicación específica (ASIC por sus siglas en inglés) es un chip de computadora que está diseñado específicamente para realizar una única función. En el contexto de la minería, los ASICs se usan para calcular algoritmos de hasheo específicos. Presentan un riesgo para la descentralización porque superan a todos los demás métodos de minería, son fabricados por empresas específicas, tienen canales de distribución muy limitados debido a la naturaleza especializada del hardware, y requieren costos de capital significativos para desarrollarse y operar de forma rentable. Existen beneficios potenciales para los ASICs, como los requisitos de costos de capital que los mineros deben asumir para invertir en hardware específico para algoritmos, lo que hace menos probable que se comporten de una manera que atente contra su propia inversión al actuar de manera deshonesta. Sin embargo, la distribución y fabricación de chips ASIC, con algoritmos de hasheo maduros, aún se centraliza en unas pocas grandes empresas. Estas compañías pueden rechazar el envío a ciertas áreas, decidir qué regiones y clientes obtienen los ASICs de mejor rendimiento y pueden estructurar partidas limitadas y manipular los precios.

Para evitar que los mineros de ASIC monopolicen el hash de la red, muchas criptomonedas desarrollaron algoritmos de hash resistentes a ASICs, como Scrypt y Ethash [25][26]. Hasta hace poco, Monero usaba el algoritmo CryptoNight, que requiere grandes cantidades de caché L3 para operar. En teoría, esto debería haber dificultado la producción de un chip ASIC debido a los grandes requisitos de memoria. Sin embargo, en 2018, Bitmain lanzó el X3, un ASIC específico de CryptoNight que podría minar con eficacia diez veces la velocidad de una unidad de procesamiento de gráficos (GPU) [27]. Otros algoritmos de hasheo han sufrido destinos similares, como Scrypt, Ethash y Equihash ahora todos minados por ASICs.

Para combatir el uso de ASIC, Monero propuso una estrategia de bifurcación dura (hardfork) cada 3-6 meses para cambiar ligeramente el algoritmo de hash CrytpoNight (la primera bifurcación fue a CryptoNightV7) [28]. El capital y el tiempo requeridos para construir un ASIC es significativo, y con diseños de hardware altamente específicos, pequeños ajustes en un algoritmo de hash deben invalidar el diseño del chip, desperdiciando el tiempo y la inversión de capital de los fabricantes de ASIC. Sin embargo, este enfoque introduce sus propios problemas. Si los cambios realizados en el algoritmo son insuficientes para evitar que se reprogramen los ASIC, entonces la red puede volverse vulnerable a la centralización del hashrate hasta que otro hardfork sea posible. Las Field Programmable Gate Arrays (FPGA) también se deben considerar en las estrategias de resistencia de ASIC, donde cambios poco frecuentes en los algoritmos hash se pueden reprogramar fácilmente para los FPGA. Otra preocupación es que los cambios regulares a los mecanismos de consenso básicos introducen la posibilidad de errores no deseados y generalmente centralizan el desarrollo de dichos cambios en torno al equipo central de desarrolladores.

Se han propuesto una serie de algoritmos de prueba de trabajo alternativos para combatir la necesidad de bifurcación dura con regularidad, incluidos algoritmos de hash intensivos en memoria como Argon2, Ballon hash y algoritmos hash polimórficos como ProgPoW y RandProg [29][30][31][32]. El equipo de Loki publicará investigaciones adicionales sobre los algoritmos antes mencionados para desarrollar una solución a largo plazo para la resistencia ASIC.

Mientras se lleva a cabo este trabajo, Loki incorporará una versión de CryptoNight llamada CryptoNight-Heavy, que mantiene la resistencia de ASIC contra los mineros CryptoNight ASIC. CryptoNight-Heavy difiere de CryptoNightV7 en varias formas: proporciona un aumento en el tamaño del scratchpad a 4mb, y se cambia la forma en la que se manejan las implosiones y explosiones [33]. Estos cambios lo diferencian del mayor objetivo para los mineros de ASIC, que es CryptoNightV7 de Monero, y también proporcionan una protección más robusta contra el desarrollo de ASIC hasta que se proponga una solución permanente.

7.2. Tamaño de Bloque Dinámico

Al igual que otras monedas de CryptoNote, Loki no tiene un tamaño de bloque fijo. En cambio, el tamaño de bloque cambia con el tiempo, creciendo para incluir más transacciones a medida que la red alcanza un mayor rendimiento de transacción. El tamaño del bloque Loki escala al observar el tamaño mediano del bloque en los últimos 100 bloques y lentamente retarda el tamaño máximo de cualquier nuevo bloque en consecuencia.

La preocupación de largo plazo en otras criptomonedas es que los tamaños de bloques grandes son una carga para los nodos que almacenan y verifican las transacciones. A medida que crecen los tamaños de los bloques, los nodos que se ejecutan en hardware no preparado no pueden procesar y propagar nuevos bloques, lo que lleva a la centralización de la red de nodos

entre los que tienen interés comercial por mantener los mismos. Esto puede ser preocupante porque la distribución de la cadena de bloques a través de muchos nodos permite que se confirme el estado de la cadena entre muchas partes diferentes, lo que aumenta su validez y resistencia a la censura.

En Loki, una parte de la recompensa del bloque se otorga a los Nodos de Servicio que procesan y propagan bloques, como los nodos completos. Debido a que los Nodos de Servicio con ancho de banda y rendimiento insuficientes se eliminan de la red de Nodos de Servicio (ver 7.3), el conjunto de recompensas requiere cumplir con un rendimiento mínimo. Esta estructura de incentivos no solo asegura que la cantidad de nodos sea significativa, sino que dichos nodos tienen un nivel de rendimiento suficiente para propagar con éxito los datos de blockchain en la red, independientemente de cuánto crezca la cadena de bloques o cuán exigentes sean los requisitos de ancho de banda. Aun así, se requieren optimizaciones del tamaño de las transacciones para garantizar que la red pueda escalar de manera eficiente a fin de mantener bajos los costos operativos del Nodo de Servicio, de modo que más participantes puedan operar uno a largo plazo.

7.3. Tamaño de Firmas de Círculo

Las firmas de círculo se usan para ocultar salidas reales entre otras en cualquier transacción dada. El tamaño de una firma de círculo se refiere a cuántas firmas se utilizan para construir el círculo. Actualmente, Monero tiene un tamaño de firma de círculo mínimo obligatorio de siete, con seis firmas junto con la salida real no utilizada en una transacción.

El efecto de tamaños de círculo más grandes ha sido escasamente estudiado, sin embargo, en el artículo 0001 (publicado por Monero Research Lab), se analizó el efecto de diferentes tamaños de círculo frente a un atacante que poseía una gran cantidad de resultados en la blockchain [34]. Se descubrió que los tamaños de círculo más altos reducen el marco temporal en el que un atacante malintencionado que posee una gran cantidad de transacciones no utilizados podría realizar un análisis efectivo de las mismas. Obligar a tamaños de círculo más grandes también protege contra un ataque teórico conocido como ataque EABE/Knacc [35], donde un tercero (por ejemplo, un intercambio) puede realizar un análisis temporal limitado de las transacciones entre dos usuarios.

Además, Monero no tiene un tamaño de círculo máximo impuesto por las reglas de consenso de la red. Muchos monederos, como el monedero GUI de Monero, tienen un tamaño de círculo igual a 26. Sin embargo, un usuario puede crear una transacción de forma manual con el tamaño de círculo que desee, siempre que esté por encima de un tamaño mínimo de círculo de siete. Esto es problemático ya que la mayoría de los monederos el tamaño mínimo predeterminado de siete. Por ende, aumentar el tamaño de círculo de transacciones por encima de siete hace que la transacción se destaque (Figura 4). Además, si las transacciones de un individuo debieran usar siempre un tamaño de círculo no estándar en Monero (diez por ejemplo), un tercero pasivo podría analizar el blockchain e inferir patrones usando el análisis temporal.

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

Figura 3: *xmrchain.net (Explorador de bloque Monero) muestra cómo resaltan los tamaños de círculo no estándar*

Loki mejora estos dos problemas al imponer el tamaño de los círculos y establece el tamaño del mismo en diez. Establecer estáticamente el tamaño máximo de círculo protege a los usuarios que construyen círculos con más de nueve transacciones y a su vez previene que un atacante que posee un gran número de salidas pueda discernir los resultados reales gastados en una firma de círculo. Los tamaños de círculo más grandes también aumentan la eficacia de la ofuscación predeterminada de forma no lineal, volviéndose más efectivos a medida que crecen los tamaños de estos.

En el esquema de transacción actual, aumentar el tamaño del círculo a 10 daría lugar a un aumento del 2,6 % en el tamaño de la transacción. Sin embargo, cuando se implementan Bulletproofs, representará aproximadamente un 8 - 13 % de aumento en el tamaño de una transacción. Esto se debe a la reducción general en el tamaño de la transacción causada por Bulletproofs. Aumentar el tamaño mínimo del círculo puede presentar un problema en una red que carece de arquitectura para admitir transacciones de mayor tamaño, debido al aumento de la carga. Sin embargo, con Loki, esta carga puede ser soportada por los Nodos de Servicio que están incentivados para operar y proporcionar suficiente ancho de banda.

8. Prevención de ataques

8.1. IP y bloqueo de paquetes

Aunque la red de Nodo de Servicio no tiene puntos centrales de falla, la red enfrenta dos amenazas de censura significativas; concretamente ataques de recolección e inspección profunda de paquetes [36][37]. Los ataques de recolección buscarían reunir las direcciones IP de todos los Nodos de Servicio operativos en la red y usar los cortafuegos de nivel de ISP para bloquear las conexiones con esas direcciones particulares. Este tipo de censura se realiza regularmente en la red Tor en China [38]. La inspección profunda de paquetes (DPI) tiene como objetivo investigar la estructuración de cada paquete individual que pasa a través de un cortafuegos y, de forma selectiva, eliminar o bloquear paquetes que parecen estar relacionados con un servicio en particular. Nuevamente, el DPI ha sido utilizado ampliamente por actores estatales [39].

Se ha trabajado mucho para diseñar sistemas que evadan DPI. Los usuarios pueden aprovechar tipos de transportes conectables que alteran la firma de cada paquete con el objetivo de aparecer como tráfico desbloqueado normal. El bloqueo de IP generalmente se evita ejecutando puentes de fachada de dominio que encriptan el tráfico como solicitudes HTTPS a servicios desbloqueados como Azure o Cloudflare. Una vez que lleguen al servicio desbloqueado, el puente reenviará la solicitud a la ubicación deseada. En el caso de la fachada de

un dominio, se vuelve difícil para un actor a nivel estatal evitar el paso de todos los puentes populares sin causar una alteración significativa en el uso general de Internet.

Los mecanismos de gobernanza integrados en Loki (ver 9) pueden ser usados para operar puentes de fachada de dominio para que los usuarios puedan acceder a los servicios de Loki en países donde las políticas de censura de Internet a gran escala están activas. Además, el soporte de transporte conectable OBFS4 se incluirá con la emisión del Nodo de Servicio del monedero Loki para contribuir en mayor medida en la protección contra DPI [40].

8.2. Ataques de denegación de servicio

Los usuarios de cadenas de bloques descentralizadas no están obligados a proporcionar identificadores digitales o físicos. Esto puede ser beneficioso para los usuarios que carecen de identidad o que son perseguidos por ello. Sin embargo, los sistemas que no requieren identificación se vuelven vulnerables a los ataques de Sybil, donde un actor maligno produce numerosas identidades falsas (en el caso de Loki, numerosos pares de claves público-privadas) y utiliza estas identidades para enviar solicitudes a la red.

Muchas criptomonedas han tenido problemas con esto y se ven obligadas a implementar un modelo de tarifa por servicio o un modelo de prueba de trabajo. En los modelos de tarifa por servicio como Siacoin, los usuarios pagan por los servicios que utilizan. En el caso de Siacoin, el costo se determina por TB de almacenamiento por mes [41]. Los modelos de tarifa por servicio son eficaces para reducir los ataques de Sybil, sin embargo, alejan a muchos usuarios del sistema, especialmente cuando hay servicios similares disponibles de forma gratuita (como Google Drive y Onedrive en el caso de Siacoin). Los sistemas de prueba de trabajo como los utilizados en Hashcash y Nano requieren que los usuarios calculen una pequeña prueba de trabajo antes de enviar un mensaje o una transacción [42][43]. Estos pequeños sistemas de prueba de trabajo son posiblemente más igualitarios que el modelo de pago por servicio, pero pueden ser presa de los atacantes que poseen grandes cantidades de poder de cómputo.

Loki propone un esquema de prueba de trabajo modificado para abordar las dos superficies de ataque más grandes de Sybil en el sistema Loki; mensajes fuera de línea y creación de rutas. Los mensajes fuera de línea presentan un objetivo potencial porque cada mensaje debe ser almacenado por un enjambre de nueve nodos. El Abuso potencial podría surgir cuando un usuario malicioso sobrecarga un enjambre particular con un gran volumen de mensajes que tendría que almacenar. En los ataques de creación de ruta, el atacante busca involucrarse en el proceso de creación de ruta con tantos nodos como sea posible, tomando recursos de ancho de banda y denegando el servicio a los usuarios que crean rutas a través de la red para fines legítimos.

Para evitar ambos ataques, la red Loki requiere que se adjunte una prueba de trabajo corta cuando se crean ambos mensajes y rutas. Para los mensajes, esta prueba de trabajo se calcula como un hash Blake2b del mensaje. Para la creación de ruta, la prueba de trabajo se envía junto con la solicitud de que se incluya un nodo en el proceso de creación de ruta. Para garantizar la escalabilidad y la accesibilidad para los usuarios móviles, el requerimiento de dificultad de prueba de trabajo es establecido en base en el Tiempo de Vida (TTL) del mensaje o de la ruta, y no en base a la actividad de la red global.

8.3. Marcado de enjambre

Cuando los nodos operan en un entorno de desconfianza, sin un líder centralizado que imponga las reglas generales, mantener el comportamiento adecuado de los nodos en la red se vuelve difícil. Aunque los Nodos de Servicio en Loki deben tener el requisito de garantía correcto, pueden optar por no enrutar el tráfico o almacenar datos en sus pools de memoria. Debido a que esta opción es financieramente beneficiosa (utilizando menos ancho de banda / ciclos de CPU / almacenamiento), se debe proponer un sistema de marcado distribuido para eliminar los nodos con bajo rendimiento.

Para Loki, dicha marcación distribuida enfrenta importantes problemas de implementación. Fundamentalmente, cada Nodo de Servicio está incentivado financieramente a marcar a algunos Nodos de Servicio como un mal actor. Esto se debe a que, cuando un Nodo de Servicio es marcado, enfrentará la eliminación de la "staking pool" y, por lo tanto, crecerá la probabilidad de que los marcadores ganen una recompensa. Un posible método de marcado distribuido es aquel en el que se proporciona evidencia cuando ocurre un evento de marcado; sin embargo, esta solución cae presa de los nodos que fabrican evidencia a su favor. Por el contrario, marcar sin restricciones permite a nodos individuales o grupos de nodos colaborativos marcar intencionalmente nodos honestos con el fin de mejorar sus posibilidades de ganar recompensas de bloque. Para eludir estos problemas, Loki propone el marcado de enjambre.

El marcado de enjambre funciona utilizando los enjambres existentes (ver 6.1.1) para elegir los miembros que participarán en cada ronda de prueba. Cada Nodo de Servicio contiene una copia de la cadena de bloques, y cada bloque creado por un minero seleccionará deterministicamente una cantidad de enjambres de prueba. Por bloque, el 1 % de los enjambres de redes son seleccionados para participar en un enjambre de prueba. Para calcular los enjambres participantes, el hash de los cinco bloques previos se usa para sembrar una función Mersenne Twister que luego selecciona los enjambres por orden de su posición en la lista determinística.

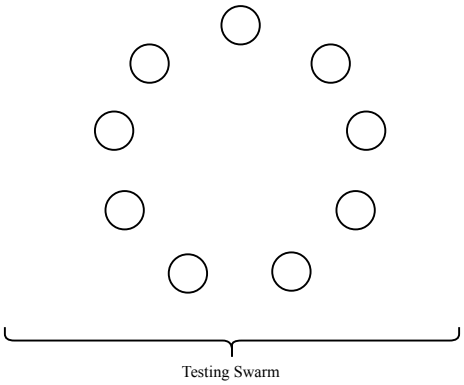

Figura 4: *Un enjambre de prueba es un enjambre seleccionado de 9 nodos*

Cuando se ha seleccionado un enjambre para participar, se espera que cada nodo en ese enjambre realice una serie de pruebas en cada otro nodo en el enjambre. Estas no son pruebas activas; más bien, cada nodo almacena información histórica sobre sus interacciones con todos los demás nodos dentro de su enjambre. La información sobre el ancho de banda, el almacenamiento de mensajes, las solicitudes de cadena de bloque y la funcionalidad del nodo de salida se recopilan y conservan a lo largo del tiempo. Los nuevos participantes de enjambres que todavía tienen que recopilar esta información pueden consultar Nodos de

Servicio fuera de su enjambre inmediato para recopilar datos en cada uno de los Nodos de Servicio que prueban.

Cada Nodo de Servicio decide cómo votar sobre cada uno de los otros miembros del enjambre. Una vez que ha tomado su decisión en base a las pruebas mencionadas anteriormente, recopila y difunde sus votos al enjambre. Cada nodo en el enjambre ahora puede verificar los votos de todos los miembros. Si un nodo individual en el enjambre tiene más del 50 % de los nodos votando en su contra, cualquier miembro del enjambre tiene la información requerida para construir una transacción de eliminación de registro. Una vez que esta transacción se valida e incluye en un bloque, todos los Nodos de Servicio actualizan su DHT, purgando los nodos que fueron votados negativamente.

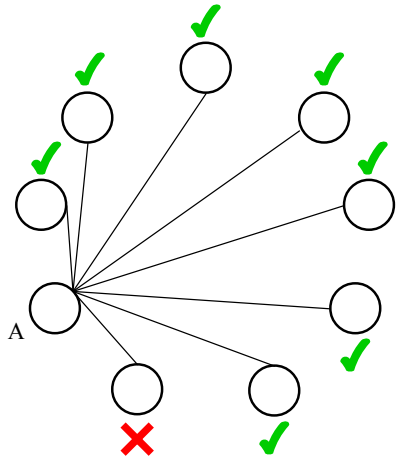

Figura 5: *El nodo deshonesto es testeado por el nodo A y falla el test. El nodo A llega a la comprensión local de qué nodos están perdiendo o pasando las pruebas.*

8.3.1. Paquete de prueba

Con el fin de permitir a la red aplicar por sí misma los estándares de rendimiento, los Nodos de Servicio deben estar equipados con las herramientas necesarias para probar otros Nodos de Servicio. Estas pruebas deben cubrir el alcance de todas las funcionalidades proporcionadas por los Nodos de Servicio para evitar ataques perezosos de masternode [44]. En este diseño inicial, se proponen cuatro pruebas fundamentales. Se pueden agregar más pruebas al paquete de prueba a medida que se expanda la función de los Nodos de Servicio.

Cuando un operador ejecuta por primera vez el software del Nodo de Servicio, se asigna un archivo vacío con un tamaño predeterminado en el disco para garantizar que haya espacio para las tareas que requieren almacenamiento. A continuación, se realiza una prueba de ancho de banda simple entre el Nodo de Servicio y un conjunto de servidores de prueba geográficamente distribuidos administrados por la Fundación Loki. Estas comprobaciones son opcionales y los Nodos de Servicio pueden saltarlas, ignorarlas o fallarlas, y unirse al "pool" de Nodos de Servicio No confiables. Sin embargo, ejecutar y pasar estas pruebas proporciona un buen indicador para cualquier potencial operador de Nodo de Servicio en cuanto a si deben arriesgarse a bloquear las garantías en un nodo que no cumpla con los requisitos mínimos. Una vez que un Nodo de Servicio se une a la "pool" de Nodo de Servicio que no son de confianza, su garantía es bloqueada y son testeados por el próximo enjambre elegido. Las pruebas de enjambre se hacen cumplir por consenso y los nuevos participantes en la red del Nodo de Servicio no pueden evadir estas pruebas. Si un nodo supera todas las

pruebas de enjambre, recibe el distintivo de nodo de confianza y puede comenzar a enrutar paquetes. Si esto falla, se elimina de la red y su garantía permanece congelada durante 30 días.

Prueba de ancho de banda

La prueba de ancho de banda forma la columna vertebral del paquete de pruebas de la red Loki. Si un nodo supera esta prueba, se supone que enruta honestamente paquetes por encima del umbral mínimo.

Cada vez que un nodo interactúa con otro Nodo de Servicio, creará y conservará un registro del ancho de banda entrante provisto. Con el tiempo, los nodos serán incluidos en miles de rutas y enrutan millones de mensajes. Estas interacciones formarán la base de cada tabla de ancho de banda de nodos. Desde esta tabla, un nodo puede responder a las pruebas de ancho de banda sobre los Nodos de Servicio dentro de su enjambre.

También se espera que todos los nodos respondan a las consultas de sus propias tablas de ancho de banda desde otros nodos. Esto significa que incluso los nodos que se han unido recientemente a la red pueden consultar la red más amplia para obtener información sobre cualquier nodo específico en su enjambre.

Prueba de almacenamiento de mensajes

El almacenamiento de mensajes es esencial para la funcionalidad de mensajería sin conexión para los usuarios de Loki Messenger. Los Nodos de Servicio deben ser testeados en su capacidad de almacenar en caché los mensajes y entregarlos a los usuarios en el transcurso del Tiempo de Vida del mensaje (TTL).

Los usuarios que envían mensajes sin conexión seleccionan al azar un Nodo de Servicio dentro del enjambre de usuarios de destino. Este nodo debe distribuir una copia del mensaje entre el resto del enjambre. Dependiendo de la prueba de trabajo adjunta al encabezado del mensaje, los Nodos de Servicio que reciben una copia almacenan los datos para el TTL. A medida que el TTL en el mensaje original alcanza la finalidad, el nodo de distribución envía un "nonce" a todos los otros miembros del enjambre. El enjambre usa el nonce agregándolo al mensaje, para entonces realizar un hasheo al resultado y luego enviarlo de regreso al nodo de distribución. Esta prueba asegura que los Nodos de Servicio retienen mensajes hasta la TTL, y se enfrentan a la expulsión si no pueden producir el resumen del mensaje correcto. Como el muestreo del nodo de distribución es aleatorio, con el tiempo cada Nodo de Servicio podrá recopilar datos de rendimiento en sus compañeros de enjambre.

Prueba de almacenamiento de cadena de bloques

Se espera que los Nodos de Servicio tengan una copia completa de la cadena de bloques Loki. Al mantener una copia completa de la cadena de bloques, los Nodos de Servicio pueden realizar una serie de tareas que son esenciales para los usuarios de la red, que incluyen actuar como un nodo remoto, validar transacciones y bloquear transacciones en Blink.

Como los nodos honestos también contienen una copia de la cadena de bloques, un nodo deshonesto podría evitar tener una copia completa simplemente solicitando bloques de un nodo honesto cuando se pruebe. Para evitar este resultado, la prueba de almacenamiento de cadena de bloques está diseñada para que los nodos honestos que contienen una copia de la cadena de bloques puedan pasar esta prueba, mientras que los nodos deshonestos no.

Para lograr esto, el nodo de prueba solicita a cada nodo testeado que realice una selección de K transacciones aleatorias dentro de la historia de la cadena de bloques que luego se

concatenan y hashean. Este hash luego se devuelve al nodo de prueba. Al medir la latencia de esta solicitud, el nodo de prueba puede comparar la latencia con el tiempo esperado de retorno T. El valor exacto para T se establecerá para diferenciar con precisión la latencia esperada entre la carga desde el disco y la descarga de bloques desde la red. Para cualquier atacante, no debería ser posible descargar y hacer hash de bloques K dentro de T, y así los ataques piggybacking se vuelven difíciles.

Prueba de nodo de salida

Los Nodos de Servicio que optan por actuar como nodos de salida reciben recompensas adicionales, por lo que se requieren pruebas funcionales para garantizar que no se abuse de esta recompensa adicional.

Para que se produzca una prueba de salida funcional, un Nodo de Servicio debe ser capaz de emular el comportamiento de búsqueda natural de un ser humano. Si un Nodo de Servicio puede detectar que está siendo testeado, puede responder sólo a las pruebas y descartar las solicitudes legítimas de los usuarios. Emular el comportamiento de solicitud de página natural es difícil, sin embargo, las pruebas de salida pueden diseñarse de manera tal que la tarea de ordenar entre solicitudes y pruebas legítimas sea lo suficientemente difícil para que la diferencia en el costo de ancho de banda entre ejecutar un nodo legítimo y un nodo malicioso sea negable.

Los Nodos de Servicio usan una lista de motores de búsqueda, mantenidos localmente, combinados con un diccionario para construir términos de búsqueda natural pseudoaleatorios. Los términos de búsqueda se envían a los motores de búsqueda y las páginas web se eligen al azar a partir de los resultados. El Nodo de Servicio ahora puede construir una ruta con nodos aleatorios que actúen como relevos y el nodo que se está probando como nodo de salida. Desde esta salida, el Nodo de Servicio solicita el resultado de la página web generado a partir de su búsqueda pseudoaleatoria. Si el resultado devuelto por el nodo de salida coincide con el resultado generado por el Nodo de Servicio, entonces se considera que el nodo de salida ha pasado la prueba.

9. Gobernanza, Financiamiento y Votación

La gobernanza es una parte esencial del diseño de criptomonedas y debe ser respaldado a nivel de protocolo. El riesgo de una gobernanza débil e informalmente definida se ha estudiado ampliamente a lo largo de la historia de la tecnología de cadena de bloques. Bitcoin y Ethereum experimentaron bifurcaciones duras contenciosas que dividieron el enfoque y los esfuerzos de sus respectivas comunidades. Aunque las bifurcaciones duras se pueden utilizar como una estrategia de gobierno, siempre se deben considerar como un último recurso en lugar de la solución a cada problema polémico. El sistema de gobernanza de Loki está diseñado para resolver problemas potenciales al proporcionar un entorno estructurado para el discurso y la representación, y también para obtener fondos para el desarrollo de Loki sin depender de la influencia externa o el altruismo.

Más allá de la prevención de las bifurcaciones duras, las estructuras de gobernanza deberían crear los medios para financiar internamente nuevos proyectos que mejoren el ecosistema de Loki. Los proyectos de financiación interna pueden evitar la formación de grupos de interés especiales que no necesariamente tengan motivos que estén en línea con los usuarios, los mineros o los Nodos de Servicio. Hemos visto esto en Bitcoin y en varias bifurcaciones de

Bitcoin con la formación de compañías con fines de lucro, como Blockstream, Bitcoin ABC y Bitcoin Unlimited, que han sido acusadas frecuentemente de contratar desarrolladores para realizar cambios específicos de protocolo en Bitcoin y Bitcoin Cash para promover sus propios objetivos comerciales o seguir su ideología específica.

Es por esta razón que en cada bloque de Loki, el 5 % de la recompensa se asigna con el propósito de la gobernanza de la red. Esto proporciona un flujo constante de Loki que se distribuirá entre proyectos comunitarios, desarrolladores de software y equipos de integración. De esta recompensa del bloque del 5 %, el 3.75 % es controlado por la Fundación Loki y el 1.25 % es controlado por los Nodos de Servicio a través del Sistema de Financiamiento Loki, lo cual fomenta una representación justa de los Nodos de Servicio y permite propuestas de financiamiento comunitario que pueden ocurrir fuera del control directo de la Fundación Loki.

9.1. La Fundación Loki

La Fundación Loki es una organización registrada sin fines de lucro con sede en Australia. Esta entidad legal central existe para permitir que el Proyecto Loki opere dentro de un marco legal bien definido y para brindar a quienes trabajan en el proyecto protecciones y obligaciones legales. La Fundación Loki fue incorporada en Australia en 2018 y utiliza la misma constitución que el ejemplo proporcionado por la Comisión Australiana de Organizaciones benéficas y sin fines de lucro (ACNC) [45]. Esta constitución otorga a la Fundación la misma estructura de gobernanza corporativa que muchas otras organizaciones sin fines de lucro, donde la compañía no tiene accionistas o beneficiarios, los miembros de la junta directiva tienen asientos con límites de mandato y llevan a cabo acciones votando las resoluciones presentadas por los otros miembros. La Fundación Loki está estructurada para lograr el estatus de organización benéfica registrada en Australia.

Esta organización está constitucionalmente obligada a gastar cualquier ingreso (incluida la recompensa del bloque de gobernanza) en la promoción del proyecto y las iniciativas alineadas. Como organización auditada externamente, la transparencia es fundamental para mantener cualquier estatus de organización benéfica registrado que reciba la Fundación Loki, y para asegurarle al público general que la Fundación Loki sigue siendo honesta y sigue gastando dentro de límites razonables. La Fundación Loki es responsable tanto ante la comunidad como ante sus auditores. Si este sistema finalmente no sirve a Loki y sus proyectos circundantes, existen protecciones duras. En caso de que surja una bifurcación dura con suficiente consenso de red, existe la posibilidad de eliminar o reemplazar a la Fundación Loki como receptora de esta recompensa por bloque.

9.2. El sistema de financiación Loki

Aunque la Fundación Loki está hecha de un grupo diverso de personas que representan el Proyecto Loki, la Fundación está sujeta tanto a su propia constitución de gobernanza como a las leyes de Australia. Esto podría ser un factor limitante en el rango de decisiones que la Fundación puede tomar. El Sistema de Financiamiento Loki permite que una porción de la recompensa de bloque sea efectuada simplemente por un voto de los Nodos de Servicio. Los Nodos de Servicio representan entidades de todo el mundo y no están obligados a recibir aportaciones del equipo o la fundación del proyecto Loki. Esto les permite alcanzar un nuevo nivel de autonomía en las decisiones que pueden tomar. Los Nodos de Servicio son los

participantes más comprometidos en la red y están incentivados financieramente para tomar decisiones que aumenten el valor de Loki.

9.2.1. Propuestas

Cada propuesta que es presentada ante los Nodos de Servicio se publica en la cadena de bloques Loki. Si una parte determinada desea presentar una propuesta a los Nodos de Servicio, la parte debe construir una propuesta de transacción. Debido a que los contenidos de las propuestas de transacción deben ser legibles y los resultados deben ser destruidos, renuncian a las características de privacidad de las transacciones típicas de Loki.

Los bloques de financiamiento se crean cada 43.000 bloques (aproximadamente 60 días). Los líderes de propuestas pueden enviar sus propuestas en cualquier momento durante este período. Sin embargo, se debe considerar que cuanto más se acerquen al inicio de cada fase de propuesta, más tiempo tendrán para obtener votos de cada Nodo de Servicio.

Junto con cada transacción hay un campo adicional que contiene la información que cada Nodo de Servicio necesita comprender para votar sobre la propuesta. Esta información incluye: un título de propuesta, una URL que enlaza con una explicación detallada de la propuesta, la cantidad de Loki que busca la propuesta, una dirección de pago y un agente de custodia si se elige.

A la espera de la aprobación de parte de la Fundación Loki, los usuarios que hagan propuestas también pueden elegir que la Fundación Loki o cualquier otro tercero actúe como agente de custodia, liberando fondos a medida que se alcanzan los objetivos. Además, para fomentar un alto nivel de propuestas y evitar el spamming de estas transacciones, cada propuesta de transacción debe grabar una cantidad no trivial de Loki.

9.2.2. Votación

Cada Nodo de Servicio tiene una clave específica para votar. Esta clave se puede exportar y utilizar para votar en nombre de un Nodo de Servicio sin tener que iniciar sesión en el servidor donde está alojado.

La votación no ocurre en cadena, más bien, cada Nodo de Servicio señala su apoyo, desacuerdo o abstención para cada propuesta activa en la cadena de bloques. Los Nodos de Servicio pueden votar sobre las propuestas tan pronto como estén destinadas a la cadena de bloques hasta el próximo bloque de financiamiento bimensual. Poco antes de la creación del siguiente bloque de financiación, se elige un enjambre para recopilar un recuento de todos los votos emitidos. Este recuento se envía luego al mempool de nodos y permanece allí hasta que un minero alcanza el bloque de financiación. Esta información luego se usa para construir el bloque que asigna una recompensa a las propuestas ganadoras. Las propuestas solo se pasan cuando el resultado de los votos afirmativos menos los no votos equivalen al 15 % del recuento de nodos en la red del Nodo de Servicio.

9.2.3. Distribución de fondos

Todos los ingresos del Sistema de Financiación Loki se pagan a través de bloques de financiación. Las recompensas de los bloques de financiación funcionan de forma similar a las

tradicionales recompensas de bloque, como una forma totalmente no custodiada de distribuir Loki. Cada 43.000 bloques (aproximadamente 60 días) un bloque de financiamiento es construido por mineros. Este bloque contiene el 1,25 % de la recompensa total del bloque para todo el período del bloque de financiación.

Para construir un bloque de financiación válido, los mineros deben poder evaluar las propuestas que hayan alcanzado el porcentaje requerido de votos. Esto se hace utilizando la información que los Nodos de Servicio envían a la cadena de bloques, que contiene tanto las direcciones a las que pagar como el estado de todos los votos. Todos los Nodos de Servicio validarán el bloque de financiación de los mineros y descartarán cualquier bloque de financiación que pague a direcciones no válidas.

A menudo, la suma de Loki requerida por las propuestas aprobadas excederá o disminuirá por debajo de la cantidad total acumulada en ese período de 60 días. Si la suma total de las propuestas aprobadas excede la que está disponible en el bloque de financiación, el minero construirá el bloque de financiación priorizando las propuestas que se enviaron a la cadena de bloques anteriormente. Las propuestas aprobadas restantes seguirán asignadas al blockchain hasta el próximo bloque de financiación.

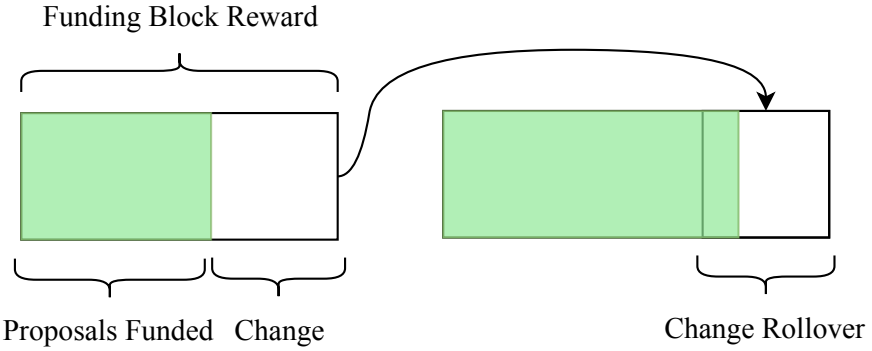

Figura 6: *Los fondos que quedan sin usar crean cambio que aumenta la recompensa del siguiente bloque de financiación*

10. Conclusión

Loki propone un modelo para transacciones anónimas y comunicación descentralizada construida en una red de nodos incentivados económicamente. Loki utiliza las bases del protocolo CryptoNote para garantizar privacidad e implementar un sistema de nodos garantizados para mejorar la flexibilidad y la funcionalidad de la red.

Además, Loki propone mejoras en investigaciones previas y proyectos de código abierto y presenta un nuevo protocolo de enrutamiento anónimo que ofrece ventajas significativas sobre los protocolos existentes. La combinación de una arquitectura única y un diseño de protocolo crea una red con resistencia Sybil basada en el mercado, disminuyendo la eficacia del análisis temporal y brindando a los usuarios un alto grado de privacidad digital.

Referencias

[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.