Loki

Transactions privées, communication décentralisée.

Kee Jefferys, Simon Harman, Johnathan Ross, Paul McLean

Version 3

13 juillet 2018

Abstract

Un système hybride, basé sur la preuve de travail et la preuve de service, offre un moyen unique de développer financièrement l'exploitation de nœuds complets.Loki utilise ces nœuds pour créer une couche de routage privé secondaire.La fonctionnalité de nœud minimum sur la deuxième couche est surveillée et appliquée par une nouvelle méthode appelée swarm flagging.Loki repose sur une version modifiée du code source de Monero, cela permet d'assurer que toutes les transactions atteignent un niveau important de confidentialité.

Ce livre blanc explique la technologie et les moyens utilisés dans Loki.Nous prévoyons des changements appliqués à cette technologie au fur et à mesure du développement de Loki. Les nouvelles versions de ce livre blanc seront publiées pour prévenir de tout changement ou mise à jour importants.

1 Introduction

De nos jours, la demande sur la confidentialité dans les communications et les transactions numériques ne cesse d'augmenter. Les données des utilisateurs sont collectées, traitées et échangées à des niveaux sans précédent. Toutes nos données internet telles que nos historiques de recherches, nos mails, notre carte de crédit, etc. sont rassemblées et vendues entre les plus grandes sociétés du monde ou la censure d'un gouvernement par exemple. Loki vise à fournir une suite d'outils résistants à la censure qui permettra aux utilisateurs de traiter et de communiquer en privé sans se soucier d'une censure ou d'un blocage quel qu'il soit.

Le Bitcoin est apparu avec la promesse d'une confidentialité sûre, mais au final le Bitcoin peut-être facilement traçable.Des sociétés comme Chainalysis et BlockSeer ont profité de l'architecture de la blockchain transparente du Bitcoin pour suivre des transactions spécifiques [1]. Loki est construit à partir de Monero, une crypto-monnaie qui s'est imposée comme l'un des réseaux de transactions les plus sécurisés et privés à ce jour [2]. Cependant, nous

reconnaissons que Monero a des inconvénients.Les transactions Monero sont bien plus importantes que les transactions Bitcoin. Monero a des besoins importants en bande passante, etc... Avec le temps, le réseau se développe, les opérateurs de nœud Monero subissent une lourde charge et n'offrent aucune récompense pour leurs contributions au réseau. Cela rend l'exécution d'un nœud un exercice coûteux et souvent ingrat. Afin d'atténuer cette situation tout en offrant des avantages économiques aux opérateurs de nœuds, Loki intègre un système de récompense appelé Services Nodes ou en français nœuds de services.

Les nœuds de services peuvent également être utilisés pour d'autres fonctions centrées sur la confidentialité si elles sont correctement motivées.Principalement, le réseau de nœuds de services permettra aux utilisateurs de transmettre et de recevoir des paquets de données anonymes.Cette communication privée est facilitée par le fait que chaque nœud de service agit comme un relais dans un nouveau réseau mixte Sybil résistant, étant similaire à Tor et I2P [3][4].D'autre part, ce réseau de communication émergent sera utilisé dans le cadre d'un service de messagerie décentralisé et chiffré de bout en bout, appelé Loki Messenger, qui permettra aux utilisateurs de communiquer directement.

Loki n'est pas seulement un support permettant des échanges privés, mais une plate-forme pour les services Internet décentralisés et anonymes.

2 Basic Parameters

Loki Difficulté (Blocktime)	120 secondes
Algorithme de difficulté	Zawy LWMA [5]
Algorithme de hachage	CryptoNight Heavy
Courbe elliptique	Curve25519 [6]

3 CryptoNote Elements

Loki utilise le code source de Monero en raison du haut niveau de confidentialité qu'il offre aux transactions.Monero est une évolution du protocole CryptoNote, qui utilise des signatures en cercle, des adresses anonymes et RingCT, donnant aux utilisateurs la possibilité de signer des transactions et cacher les montants [7].

Pour préserver l'intimité de l'écosystème Loki, il est important non seulement de fournir un moyen d'échange qui prend en charge l'économie interne, mais aussi de rendre quasi nulle le risque d'analyse temporelle lorsque des interactions se produisent entre les couches indépendantes de Loki. Par exemple, lorsqu'ils s'engagent dans des services transactionnels de première couche, les utilisateurs ne doivent jamais perdre les garanties de confidentialité qu'ils reçoivent de la deuxième couche et inversement...

3.1 Ring Signatures

Les ring signatures, en français signatures de cercle fonctionnent en construisant un cercle de signataires possibles à une transaction où un seul des signataires est l'expéditeur réel. Loki utilise des signatures en cercle pour cacher l'historique réel des résultats de transaction. Les

signatures de cercle seront obligatoires pour toutes les transactions Loki (à l'exception des transactions de récompense de bloc).

3.2 Adresses furtives

Loki utilise des adresses furtives pour s'assurer que la vraie clé publique du récepteur n'est jamais liée à leur transaction. A chaque fois qu'une transaction Loki est envoyé cela résulte par la création d'une adresse furtive unique et les fonds sont donc envoyés à cette adresse. En utilisant un échange de clés Diffie-Hellman, le destinataire de la transaction est en mesure de calculer une clé de dépense privée pour cette adresse furtive, prenant ainsi possession des fonds sans avoir à révéler leur véritable adresse publique [8]. Les adresses furtives protègent les destinataires des transactions et constituent une confidentialité qui est une fonction fondamentale dans Loki.

3.3 RingCT

RingCT a été présenté par le laboratoire de recherche de Monero comme un moyen de masquer les montants des transactions[9]. Les déploiements actuels de RingCT utilisent des preuves de portée qui s'appuient sur les engagements de Pedersen pour prouver que le montant d'une transaction est compris entre 0 et 2^{64}. Cette fourchette garantit que seules les quantités non-négatives de devises sont envoyées, sans dévoiler le montant réel de la transaction. Récemment, un certain nombre de crypto-monnaies ont proposé de mettre en œuvre bulletproofs en remplacement des épreuves de portée traditionnelles dans RingCT en raison de la réduction significative de la taille des transactions[10]. Loki utilisera bulletproofs, cela permettra de réduire les informations que les nœuds doivent stocker et relayer, améliorant ainsi la scalabilité.

4 Service Nodes

Bien que Loki implémente de nouveaux changements en plus du protocole CryptoNote, une grande partie de la fonctionnalité réseau et de l'évolutivité de Loki est activée par un ensemble de nœuds incités appelé service Nods ou en français nœuds de services. Pour exploiter un nœud de service, des personnes détenant une quantité suffisante de Loki devront les verrouiller pendant un certain temps tout en fournissant un niveau minimum de bande passante et de stockage au réseau. En contrepartie de leurs services, ils recevront une partie de la récompense de bloc.

Le réseau qui en résulte fournit une résistance aux attaques Sybil basée sur le marché, couvrant une gamme de problèmes avec les mixnets existants et les services centrés sur la vie privée. Cette résistance est basée sur l'interaction entre l'offre et la demande qui empêchent les acteurs individuels d'avoir une taille suffisante de Loki qui pourrait avoir un impact négatif significatif sur les services de confidentialité de deuxième couche que Loki fournit. DASH a théorisé pour la première fois que les réseaux résistants aux attaques Sybil peuvent être dérivés de la crypto-économie [11]. Au fur et à mesure que l'attaquant accumule des Loki, l'approvisionnement en circulation diminue, face à la pression de la demande, le prix du loki augmente donc. Comme cela continue, il devient de plus en plus coûteux pour l'achat de Loki supplémentaires, rendant l'attaque prohibitive coûteuse.

Pour terminer la partie de la protection économique, Loki encourage la suppression active des tokens en circulation. De ce fait, la courbe d'émission ainsi qu'un équilibre entre le nombre les jetons en circulation et ceux bloqués doit être adaptés afin d'éviter une attaque sybil.

4.1 Récompense de bloc :

Loki distribue des récompenses de bloc, cela est réalisé à travers le proofs of work en français preuve de travail, un système solide et bien étudié pour la création de blocs et la commande de transactions. Les utilisateurs qui minent appelés « les mineurs » collectent et écrivent des transactions en blocs. La règle concernant Loki est que chaques blocs contient plusieurs niveaux de récompense dont une seule va au mineur.

Récompense minière :
Il est déterminé qu'en plus de percevoir des frais de transaction, 45% de la récompense est réservée au mineur qui construit le bloc.

Récompense du nœud de service :
(50% de la récompense totale) va à un nœud de service, ou deux nœuds de service si le choix d'un relais est sélectionné. Les nœuds de service sont récompensés par rapport au temps écoulé depuis la dernière récompense reçue (ou le temps écoulé depuis leur enregistrement), avec une préférence pour les nœuds qui ont attendu plus longtemps. Á chaque fois qu'un nœud de service s'inscrit, il se retrouve en dernière position dans la file d'attente. Si le nœud de service maintient un bon service et n'est pas éjecté de la file d'attente par un drapeau Swarm, il migre vers les positions les plus élevées de la file d'attente. Lorsque les nœuds sont ou presque à la tête de la file, ils sont éligibles pour une récompense. Une fois cette récompense attribuée, le nœud tombe de nouveau à la dernière position dans la file d'attente et recommence à remonter progressivement.

Récompense de gouvernance :
Les 5% finaux de la récompense de bloc est distribuée aux opérations de gouvernance. La distribution est répartie selon le schéma suivant : 3.75% est envoyé à l'adresse de Loki Foundations, les 1.25% restants sont réservés aux sorties d'un bloc de financement.

4.2 Collateralisation vérifiable

Pour information, nous devons savoir que les nœuds de service doivent prouver au réseau qu'ils détiennent les garanties nécessaires. Les caractéristiques de confidentialité essentielle à la conception de Loki rendent cette opération compliquée et complexe, en particulier l'incapacité à auditer les soldes d'adresses publiques ou à utiliser les touches d'affichage pour voir les transactions sortantes.

Loki utilise de manière innovante les sorties temporisées, qui permettent de verrouiller les pièces Loki jusqu'à ce que la blockchain atteigne une hauteur de bloc choisi. Jusqu'à cette hauteur définie, le réseau Loki invalidera les tentatives de dépenser ces sorties verrouillées. Loki utilise ce processus pour prouver qu'un montant est détenu par un nœud de service spécifique, empêchant ainsi le mélange des garanties. Pour s'inscrire en tant que nœud de service, un opérateur crée une sortie et doit avoir la quantité nécessaire qui se déverrouille après qu'un minimum de 21 600 blocs se soit écoulé (environ 30 jours).

Dans le champ supplémentaire de la transaction, l'opérateur du nœud de service inclut l'adresse Loki qui peut recevoir des récompenses de nœud de service. Cette adresse sera également utilisée comme clé publique pour les opérations de nœud de service telles que le vote en Swarm. Les portefeuilles peuvent éviter d'utiliser ces transactions d'enregistrement de nœuds de service en tant que Mixins, car leurs montants réels et leur destination sont divulgués et ne sont donc pas utiles pour fournir un anonymat supplémentaire à une transaction.

Il faut retenir qu'avant que chaque nœud ne rejoigne le réseau de nœuds de service, les autres nœuds doivent confirmer individuellement que la couverture de garantie de ces nœuds correspond au nombre requis. En sachant que les transactions de garantie expirent après 30 jours, le porte-monnaie disposera d'une fonctionnalité de renouvellement automatique.

5 Lokinet

Les protocoles de routage d'Onion permettent aux utilisateurs de former des tunnels via un réseau distribué, en utilisant plusieurs nœuds ce qui permet de masquer la destination et l'origine des paquets de données. Les nœuds de service sur le réseau Loki utiliseront un protocole de routage d'Onion avec une faible latence, formant un réseau superposé entièrement décentralisé, appelé Lokinet. Le réseau ne repose pas sur des autorités de confiance etc..., Lokinet repose sur la blockchain. Les utilisateurs peuvent se connecter à des nœuds de service individuels et créer des chemins bidirectionnels pour acheminer les paquets. Le réseau peut être utilisé pour accéder à des services hébergés en interne appelés SNApps. Les utilisateurs peuvent utiliser la fonctionnalité de sortie du nœud de service pour naviguer sur Internet sans que leur adresse IP ne soit révélée.

5.1 Protocole de routage anonyme à faible latence (LLARP)

Pour ce faire, toutes les applications des nœuds de service reposent sur un protocole de routage anonyme, qui définit la manière dont chaque nœud de service communique avec ses compères. Loki propose un nouveau protocole de routage qui se nomme LLARP [12] conçu comme un hybride entre Tor et I2P pour fournir des propriétés supplémentaires souhaitables par rapport à tout protocole de routage existant. Le protocole LLARP est spécialement conçu pour s'exécuter sur le réseau des nœuds de service Loki et toutes les optimisations LLARP prennent en compte cette architecture. Pour comprendre les objectifs de LLARP, il est préférable de procéder à une analyse des protocoles de routage existants et d'analyser la manière dont LLARP les améliorent.

Le routeur Onion (Tor)

Tor est le mixnet anonyme le plus célèbre depuis quelques années. Le réseau Tor permet d'avoir une forte résistance à la censure et s'est avéré être un outil précieux pour préserver la confidentialité et l'anonymat sur Internet. En revanche, Tor n'est pas un réseau décentralisé. Concernant le fonctionnement de Tor, il s'appuie sur des serveurs centralisés gérés par un groupe de volontaires proches de la Tor Foundation [13]. Ces autorités de répertoire remplissent deux fonctions principales. Premièrement, ils agissent en tant que rapporteurs de confiance sur l'état des nœuds du réseau. Lorsqu'un utilisateur (ou relais) Tor se connecte au réseau pour la première fois, il peut se connecter à l'une des dix autorités de répertoire codées en dur. Ces autorités de répertoire fournissent à l'utilisateur ou au relais un fichier

appelé consensus. Ce fichier fournit une liste de tous les relais, nœuds de garde et nœuds de sortie actuellement utilisés (à l'exclusion des ponts) sur le réseau Tor. Deuxièmement, les autorités de répertoire mesurent également la bande passante que chaque relais peut fournir au réseau. Ils utilisent ces informations pour trier les relais en catégories, en déterminant si les nœuds peuvent fonctionner en tant que relais, nœuds de garde ou nœuds de sortie.

Ce niveau élevé de centralisation crée des brèches qui rendent Tor vulnérable. En 2014, Tor a reçu des informations concernant une menace crédible de suppression des serveurs d'autorité de répertoire [14]. Si les autorités de répertoire des États-Unis et de l'Allemagne ou des Pays-Bas devaient être fermées, cela suffirait à arrêter cinq des dix serveurs d'autorités de répertoire. Ce qui voudrait dire que le réseau Tor est très instable, la capacité des nouveaux relais à interagir avec le réseau étant considérablement réduite.

Les méthodes de communication dans Tor sont très limitées, car Tor ne permet que la communication via TCP. IP over, avec un manque de support pour les protocoles basés sur UDP (tels que VoIP).

Le projet d'Internet invisible (I2P)

I2P propose une approche complètement différente de l'architecture Mixnet, en maintenant un niveau de confiance plus élevé en se référant à une table de hachage distribuée (DHT) pour déterminer l'état du réseau au lieu des autorités de répertoire fiables [15]. I2P permet également le trafic TCP et UDP, prenant en charge un plus grand nombre d'interactions de protocole. Cependant, I2P n'a pas reçu un développement continu donc il a accumulé avec le temps un grand retard technique, surtout en ce qui concerne l'utilisation de la cryptographie. I2P utilise ElGamal à 2048 bits, ce qui ralentit le cryptage et le décryptage, contrairement aux opérations sur les courbes elliptiques. Malgré que des plans de migration de ElGamal existent dans la feuille de route I2P, les progrès ont été lents.

Par ailleurs, I2P manque de support pour les nœuds de sortie, ce qui veut dire que la majorité du trafic sur le réseau accède à des sites Web hébergés en interne, sous le nom d'Eepsites. On peut constater que cela a vraiment diminué la capacité du réseau I2P à atteindre les utilisateurs dont l'objectif principal est d'utiliser des réseaux permettant un anonymat et d'accéder à un réseau Internet plus vaste.

De plus, la manière dont I2P est construite signifie que la majorité des utilisateurs qui se connectent au réseau deviennent également des routeurs, ce qui pose problème car le réseau qui en résulte manque souvent de bande passante suffisante pour pouvoir créer des chemins avec une forte rapidité. Les vitesses réseaux dans les réseaux mixtes sont avalées par le nœud le moins performant de chaque circuit. Si par principe les utilisateurs peu performants deviennent des relais dans I2P alors nous constatons pour la performance globale une baisse.

Donc, pour finir, I2P est différent de Tor avec ce qu'elle propose, un réseau à commutation de paquets (plutôt que de commutation de circuits). Au lieu d'établir un tunnel à long terme unique sur lequel circule tout le trafic. I2P établit plusieurs chemins, chaque paquet en cours de communication peut être utilisé pour emprunter un itinéraire différent sur le réseau. Cela donne à I2P la possibilité d'acheminer de manière transparente l'afflux du réseau et les défaillances de nœuds.

I2P et Tor n'ont pas complètement diminuer les attaques de Sybil. Une personne avec une forte motivation et disposant de suffisamment de temps et d'argent pour acheter de grandes quantités de relais, peut effectuer une analyse temporelle qui compromettrait la confidentialité des utilisateurs. L'efficacité de cette analyse augmente le nombre de nœuds de sortie, de relais et de nœuds de garde utilisé par l'attaquant [16]. Tor et I2P sont gérés entièrement

par des personnes bénévoles qui donnent leurs temps et leurs argents pour mener à bien le fonctionnement des nœuds. Nous pensons qu'un réseau construit à partir d'incitations financières plutôt que de façon bénévole permettrait une plus grande résistance face aux attaques, tout en fournissant un service bien plus fiable.

LLARP

LLARP a la capacité de fonctionner sans qu'il soit nécessaire d'utiliser des autorités de répertoire, au contraire il s'avère qu'il repose sur un DHT construit à partir de la blockchain. Ce qui permet aux nœuds de service d'agir en tant que routeurs du réseau. La bande passante n'est pas surveillée ou enregistrée dans le DHT. Au lieu de cela, la bande passante résulte de la mesure et le triage Swarm qui évaluent chaque nœud et porter un jugement sur la capacité des nœuds à fournir une bande passante appropriée au réseau.

Dans le modèle d'interconnexion de systèmes ouverts (modèle OSI), LLARP tente uniquement de fournir une couche de réseau anonyme. Cela signifie qu'il prend en charge une plus grande gamme de protocoles de pro- Internet et réduit également les frais généraux pour le stockage des descripteurs de fichiers doivent quitter les nœuds passent par User Datagram Protocol (UDP) du trafic [17]. De plus, LLARP opte pour un routage basé sur la commutation par paquets au lieu d'un routage basé sur un tunnel, ce qui permet un meilleur équilibrage de la charge et une meilleure redondance sur le réseau.

Les utilisateurs finaux de Lokinet ne sont pas attendus (ou même permis) pour acheminer les paquets.Donc, pour simplifier, cela signifie que Lokinet s'expose à une surface d'attaque beaucoup plus faible pour une attaque Sybil en raison de la mise de fonds importante requise pour commencer l'exploitation des nœuds de services.

6 Les services Loki

Avec une forte ressemblance à l'investissement que les mineurs font dans le matériel, chaque opérateur de nœud de service bloque les pièces de monnaie Loki lorsqu'elles commencent à exploiter un nœud de service. Le capital qui est gelé sert à deux objectifs

1. Chaque opérateur de nœud de service a une part importante dans la réussite du réseau. Il ne faudra pas fournir de mauvaises performances au réseau ou agir de manière malhonnête, ils compromettent et risquent de dévaluer leur propre participation au sein du réseau.
2. Si le réseau est capable de limiter efficacement les nœuds malhonnêtes de recevoir une récompense, les nœuds malhonnêtes doivent supporter pouvoir supporter la perte de récompense et le temps de blocage restant sur leur garantie.

Nous pouvons imposer des punitions agressives pour les nœuds qui ne se comportent pas correctement, nous pouvons créer des groupes de nœuds de service avec des comportements spéciaux des nœuds hors chaîne. Dans Loki, ce comportement concerne les activités de réseau et de stockage. Ces activités hors chaîne sont combinées pour constituer le back-end des applications tournées vers l'utilisateur qui exploitent ces propriétés souhaitables, appelées services Loki.

6.1 Loki Messenger

Loki Messenger sera le premier service Loki à être développé et déployé sur le réseau Loki. Loki Messenger sera une application de messagerie privée cryptée et décentralisée de bout en bout appelée Loki Messenger.

Les applications de messageries cryptées qui permettent aux utilisateurs d'envoyer des messages sans révéler leur contenu existent déjà sur le marché, mais elles reposent sur des serveurs centralisés pouvant être ciblés, bloqués, arrêtés ou même saisis [18][19]. Ces applications de services centralisés présentent un risque élevé pour l'anonymat des parties communicantes, car souvent elles nécessitent que l'utilisateur enregistre un numéro de téléphone, son email ou d'autres informations d'identification, il ne faut pas oublier aussi que l'utilisateur se connecte directement via son adresse IP. Ces informations peuvent être sorties des serveurs à cause des fuites de données ou par des processus légaux et utilisées contre l'utilisateur. En tirant parti de l'architecture des nœuds de service sur le réseau Loki, nous pouvons fournir et garantir un service similaire aux applications de messagerie cryptées centralisées les plus répandues, telles que Signal. Loki Messenger aura une plus grande résistance à la confidentialité et à la censure quel qu'elle soit.

6.1.1 Le Routage de Loki Messenger

Le routage des messages sur le réseau Loki change selon si l'utilisateur destinataire est en ligne ou hors ligne. Si les deux utilisateurs (expéditeur et destinataire) sont en ligne, alors des communications à bande passante plus élevée peuvent avoir lieu, car les messages ne doivent pas être forcément stockés sur les nœuds de service.

Dans Loki, une clé publique sert à la fois de clé de chiffrement à long terme et d'adresse de routage. De façon la plus simple et la plus sécurisante, cette clé doit être échangée hors bande pour assurer une protection contre une attaque de type «man-in-the-middle». Un tel échange devrait avoir lieu en main propre ou soit par un autre mode de communication sécurisée (voir 6.1.2).

Messagerie en ligne

Pour expliquer le plus simplement, nous allons prendre comme exemple Alice et Bob. Ils joueront le rôle de l'émetteur et récepteur. Lorsque Alice connaît la clé publique Bob, elle pense qu'il est en ligne et tente de lui créer un chemin. Pour cela, Alice interroge le DHT d'un nœud de service et obtient un ensemble d'introduction correspondant à la clé publique Bob. Dans LLARP, les ensembles d'introduction répertorient les introducteurs gérés par chaque utilisateur. C'est par ces introducteurs que des chemins peuvent être établis. Alice choisit maintenant trois nœuds de service aléatoires pour agir comme des sauts intermédiaires entre son origine et sa destination. Un chemin a maintenant été établi, grâce auquel Alice et Bob peuvent transmettre des messages. Si elles sont correctement authentifiées et utilisent OTR (voir 6.1.2), Alice et Bob peuvent désormais communiquer tout en maintenant le plus haut niveau de confidentialité sans révéler à qui que ce soit l'origine de la conversation.

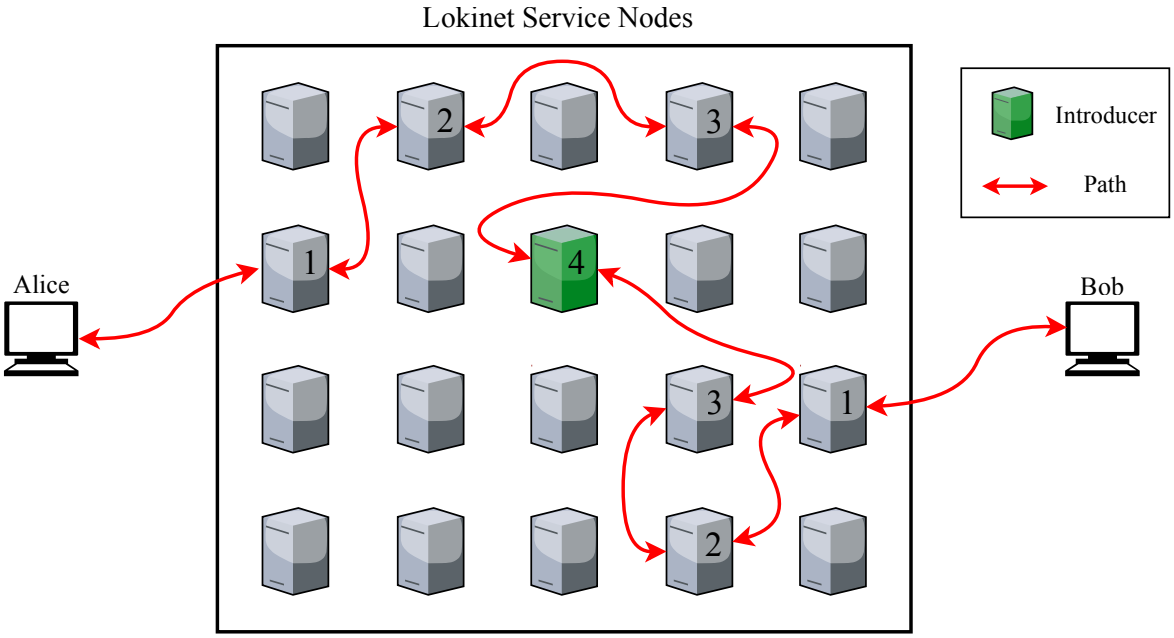

FIGURE 1: *Schéma simplifié du routage en ligne montrant Alice qui communique avec Bob, en utilisant des nœuds de service aléatoires pour établir un chemin via le réseau.*

Messagerie hors ligne

Si par exemple Alice ne parvient pas à recevoir une réponse de Bob, elle a le choix de lancer le processus de messagerie hors connexion. Le routage hors ligne utilise une version modifiée de Postal Services over swarm (PSS) [20]. Les swarms sont des regroupements logiques de nœuds de service, basés à la fois sur leurs clés publiques et sur le hachage du bloc dans lequel leur transaction est apparue pour la première fois. Chaque swarm a un SwarmID et se compose de 9 nœuds. Pour envoyer un message à Bob, Alice peut utiliser sa clé publique pour calculer à quel swarm Bob appartient. Grâce à cette information, Alice peut envoyer anonymement un message via le réseau vers un nœud de service aléatoire dans ce swarm. Lorsqu'un nœud de service reçoit un message unique destiné à son swarm, il doit distribuer ce message aux 8 autres nœuds du swarm. Il faut savoir que de plus, tous les nœuds doivent stocker les messages correspondant à leur durée de vie (TTL) attribuée. Quand Bob est en ligne, il peut interroger deux nœuds de son swarm pour les messages qu'il peut déchiffrer. La messagerie hors ligne est protégée contre les spams grâce à une preuve de travail associée à chaque message.

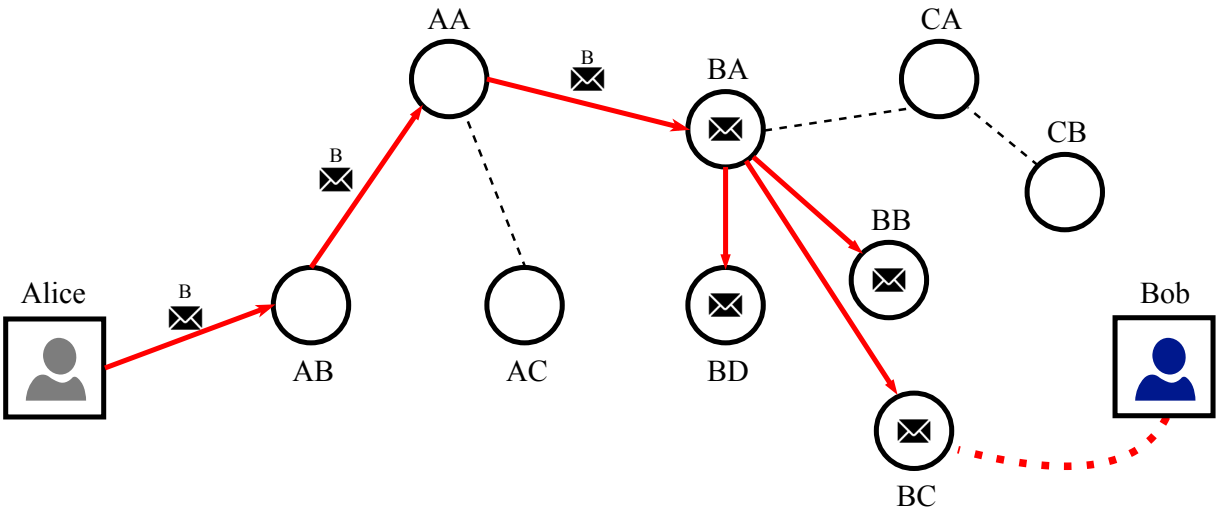

FIGURE 2: *Par exemple, Alice envoie un message à Bob, Bob est attribué au swarm B, quand Bob est en ligne, il interroge un nœud aléatoire dans son swarm et reçoit le message Alice.*

6.1.2 Chiffrement et authentification de Messenger

Une fois la chaîne de messages établie, Loki Messenger applique la confidentialité PFS (Perfect Forward Secrecy) et DA (Deniable Authentication). PFS et DA sont des concepts du protocole de messagerie Off the Record (OTR) [21]. Les services de messagerie centralisés comme Signal ou WhatsApp, utilisent des fonctionnalités de chiffrement qui gardent les protections OTR. Loki modifie son implémentation OTR par rapport au protocole Tox, qui est un protocole de messagerie instantanée distribué en peer-to-peer qui utilise la bibliothèque NaCl [22].

PFS permet de résister aux attaques lorsqu'une clé à long terme est exposée. Une nouvelle clé de cryptage partagée est utilisée pour chaque session, donc si une seule clé de session est révélée, la conversation entière n'est pas compromise. Si un tiers souhaitait rompre le cryptage d'une chaîne de messages, il devait obtenir les clés pour chaque session individuelle. PFS garantit que Loki Messenger est extrêmement difficile à compromettre par rapport aux méthodes existantes, telles que le chiffrement PGP (Pretty Good Privacy), où une seule paire de clés à long terme est nécessaire pour compromettre la chaîne de messages entiers (conversation entière).

DA désigne la possibilité pour deux parties de se prouver mutuellement qu'elles sont les expéditeurs de chaque nouveau message. En revanche, une autre personne quel qu'il soit ne peut pas savoir qui est le véritable expéditeur d'un message. Lors de l'utilisation de DA, les codes d'authentification de message (MACs) sont publiés après chaque session, permettant à des tiers de créer de manière plausible des messages qui apparaissent comme provenant de l'adresse publique de l'expéditeur. Lorsqu'il est correctement implémenté, il est impossible à un tiers de prouver qu'un expéditeur d'un message spécifique était l'expéditeur réel.

Authentification d'utilisateur

L'authentification des utilisateurs est essentielle pour garantir une protection contre les attaques de type intermédiaire. Par exemple, si Bob attend un message d'Alice mais ne connaît pas encore sa clé publique alors, une autre personne par exemple Eve, elle peut envoyer un

message à Bob en prétendant être Alice. C'est pour cela qu'il est indispensable que les utilisateurs doivent s'authentifier mutuellement avant de partager des informations personnelles.

Comme Pidgin et les autres services de messagerie OTR, Loki Messenger utilise l'authentification par clé pré-partagée (PSK). Les utilisateurs ont plusieurs choix pour la création d'un PSK. Ils peuvent établir une clé hors bande, ou alors ils peuvent s'accorder sur un PSK sur Loki Messenger en posant à l'autre personne une question à laquelle aucune autre personne ne connaîtrait la réponse. Loki implémente l'authentification PSK basée sur une version modifiée du plug-in Pidgin qui est plug-in de chiffrement d'authentification [23].

6.2 SNApps (applications de nœud de service)

La fonction de SNApps est similaire à celle des services cachés dans Tor. Ils fournissent aux utilisateurs un moyen d'interagir avec l'environnement Mixnet, en offrant un niveau d'anonymat encore plus élevé que celui pouvant être atteint lors de l'accès à un contenu hébergé en externe. Les applications SNApp permettent aux utilisateurs de configurer et d'héberger des site web, des forums, des médias sociaux et la plupart des autres applications d'Internet sur leurs propres machines ou serveurs, tout en gardant l'anonymat côté serveur et utilisateur. Grâce à cela, ça élargit considérablement la portée du réseau et il est possible aux utilisateurs de créer des communautés significatives au sein de Lokinet.

Les opérateurs SNApp utilisent le modèle client vers serveur qui est actuellement une opération courante, la principale différence étant que les nœuds de services seront des intermédiaires dans une connexion d'utilisateurs via Lokinet. Lorsqu'un SNApp souhaite s'inscrire sur le réseau, il doit mettre à jour le DHT avec son descripteur. Ce descripteur contient différents introducteurs, qui sont des nœuds de services spécifiques que les utilisateurs peuvent le contacter pour créer un chemin vers le SNApp. Lorsque ces chemins sont paramétrés, les utilisateurs peuvent se connecter au SNApp sans qu'aucune des parties sachant où l'autre se trouve sur le réseau.

6.3 Nœuds de sortie

Les nœuds de sortie permettent aux utilisateurs de faire des recherches sur Internet et de renvoyer ces requêtes via un mixnet. Si les nœuds de sortie sont utilisés correctement, ils permettent aux utilisateurs de naviguer sur Internet en privé et sans que l'adresse IP de l'utilisateur ne soit révélée au serveur.

Bien que le fonctionnement des nœuds de sortie est indispensable à Loki, forcer tous les opérateurs de nœuds de service à agir en tant que nœuds de sortie pourrait être préjudiciable. Agir en tant que nœud de sortie peut exposer l'opérateur à des risques juridiques, car les utilisateurs du nœud de sortie peuvent effectuer une activité malveillante tout en l'utilisant comme proxy. Comme les nœuds de sortie transmettent simplement le trafic d'Internet à l'utilisateur final, les nœuds de sortie reçoivent souvent des demandes DMCA (Digital Millennium Copyright Act) ou sont souvent supposés être à l'origine de tentatives de piratage. Bien que, dans la plupart des juridictions, les lois concernant l'hébergement sécurisées protègent les opérateurs de nœuds de sortie, les fournisseurs de services Internet qui acheminent le trafic des nœuds de service sur leurs serveurs peuvent craindre des risques juridiques et interruption du service vers le nœud de sortie.

Au démarrage, un nœud de service se voit attribuer un indicateur de relais il est limité au routage des paquets au sein de Lokinet, mais ne fait jamais de demande sur Internet au sens large. Un opérateur doit s'inscrire s'il souhaite devenir un nœud de sortie, démontrant ainsi une compréhension totale des risques tout en se soumettant à des tests swarm supplémentaires (voir 8.3.1).

L'inscription en tant que nœud de sortie permet à l'opérateur de doubler la récompense d'un relais normal lorsqu'il est sélectionné pour une récompense en bloc. Cette incitation est fournie pour garantir que les opérateurs de nœuds de sortie disposent de fond financier suffisant pour exploiter les nœuds de sortie, contribuant ainsi à protéger contre les attaques de type Sybil spécialement destinées à prendre le contrôle du réseau de nœuds de sortie. C'est une vulnérabilité dont Tor souffre en raison de son faible ratio de nœuds de sortie par rapport aux relais.

6.4 Nœuds distants

Sur n'importe quel réseau de cryptomonnaie, stocker une copie complète de la blockchain n'est pas possible pour de nombreux utilisateurs. Avec le Bitcoin et l'Ethereum, les utilisateurs peuvent choisir de se connecter à un nœud public complet contenant une copie de la chaîne de blocs et pouvant interroger et soumettre des transactions au réseau. Cela fonctionne parce que les nœuds complets du Bitcoin et l'Ethereum peuvent rechercher efficacement la chaîne de blocs pour les transactions qui ont pour cible la clé publique des utilisateurs.

En raison de la construction des devises CryptoNote, les nœuds publics complets (appelés nœuds distants) subissent beaucoup plus de stress. Lorsqu'un utilisateur se connecte à un nœud distant, il doit télécharger temporairement chaque bloc (lors de la création du portefeuille ou du dernier bloc vérifié) sur sa machine locale et vérifier chaque transaction pour une clé de transaction publique pouvant être générée à partir de la clé privée. Ce processus peut avoir un impact significatif sur les performances des nœuds distants. Étant donné qu'il n'y a pas de récompense pour ce service, il peut dissuader les utilisateurs d'exécuter des services de synchronisation pour les clients légers. Les portefeuilles mobiles CryptoNote sont souvent peu fiables et doivent parfois basculer plusieurs fois entre des nœuds distants avant d'établir une connexion fiable pour analyser la blockchain ou soumettre une transaction.

Par ailleurs, les opérateurs de nœuds distants malveillants exécutant l'un des rares nœuds connus qui peux enregistrer l'adresse IP des utilisateurs lorsqu'ils font des transactions spécifiques. Bien qu'aucune information sur la transaction ne soit révélée par cette attaque, les adresses IP peuvent être liées à des transactions qui peuvent ensuite remonter jusqu'à l'identité réelle, compromettant ainsi la confidentialité des utilisateurs.

Loki contourne ces problèmes en exigeant que chaque nœud de service agisse comme un nœud distant pouvant être utilisé par les utilisateurs. Les nœuds de service répondant à ce travail car ils possèdent déjà une copie complète de la chaîne de blocs et forment un réseau largement distribué de nœuds à large bande passante. En utilisant les nœuds de service en tant que nœuds distants, il existe une limite financière inhérente à la quantité de réseaux de nœuds distant pouvant être détenue par une partie donnée, et par conséquent, à la quantité de données qu'un opérateur de nœud malveillant peut collecter.

6.5 Blink

Dans un système de chaîne de blocs typique, le temps de confirmation pour une transaction donnée est le temps nécessaire pour qu'une transaction soit incluse dans un bloc. Et puis avec de la concurrence des mineurs, des blocs bloqués et des attaques Finney, les destinataires ont besoin généralement de la création d'un certain nombre de blocs supplémentaires sur le bloc contenant une transaction pour que l'on puisse la considérer comme complète [24]. Avec plusieurs facteurs concernant chaque blockchain, ce processus peut durer de 10 à 60 minutes. Cela s'avère donc peu pratique pour les commerçants qui doivent attendre confirmation et les clients qui doivent aussi patienter pour récupérer leurs marchandises ou leurs services.

Grâce à l'architecture des nœuds de service de Loki, les transactions quasi-instantanées sont possibles. Blink permet de confirmer les transactions qui se produiraient sur le réseau Loki avant de les mettre dans un bloc. Cela permet d'assurer la validité de la transaction à l'expéditeur ainsi qu'au destinataire et protégeant ainsi le destinataire contre une double dépense.

Blink fonctionne de la même façon que InstantSend de DASH. Chaque bloc swarm de nœuds de service est sélectionné de manière déterministe pour agir comme un ensemble de preuves qui confirment la validité des transactions et empêchent que la transaction ne soit dépensée deux fois. Cela permet d'éviter que les sorties non utilisées dans la transaction soit verrouillé comme avec DASH. En revanche les images clé sont verrouillées. Les images clé sont des clés uniques attachées à chaque sortie non dépensée dans une signature de cercle. Pour fournir des confirmations immédiates, Blink donne le pouvoir au swarm choisi pour signaler au réseau qu'une image clef associée à une sortie doit être verrouillée tant que la transaction n'est pas incluse dans un bloc. Si une double dépense sur la même sortie non dépensée est effectuée, une image clef identique est produite, qui serait alors rejetée par le swarm et donc le réseau dans son ensemble.

Les utilisateurs auront la possibilité de payer des frais plus élevés pour envoyer une transaction Blink qui sera confirmée beaucoup plus rapidement (en quelques secondes plutôt qu'en minutes). Cela permet une palette d'utilisation plus large pour Loki, où des paiements en direct deviennent de plus en plus pratiques et les paiements en ligne plus faciles à intégrer. Toutes les fonctionnalités de confidentialité inhérentes à Loki sont assurées tout au long de ce processus.

7 Altérations de CryptoNote

En tant que crypto-monnaie, Loki a un fonctionnement similaire aux autres pièces CryptoNote. Cependant, il existe des différences essentielles au-delà de l'ajout de nœuds de service et des fonctions associées qui vont avec.

7.1 Résistance ASIC

Un circuit intégré propre à une application (ASIC) est une puce d'ordinateur spécialement construite pour une seule fonction. Dans le contexte de l'exploitation minière, les ASIC sont utilisés pour calculer des algorithmes de hachage spécifiques. Ils présentent un risque pour la décentralisation parce qu'ils surpassent toutes les autres méthodes de minage, sont fabriqués par des sociétés spécifiques, ont des canaux de distribution très limités en raison

de la spécificité du matériel, et ils nécessitent des capitaux importants pour se développer et fonctionner de manière profitable.Il existe des avantages potentiels pour les ASIC, tels que les coûts d'investissement que les mineurs doivent engager pour investir dans du matériel spécifique à l'algorithme : cela rend moins probable les comportements malhonnêtes, car cela saperait leur propre investissement. Cependant, la distribution et la fabrication de puces ASIC, avec des algorithmes de hachage matures, sont encore centralisées autour de quelques grandes entreprises. Ces entreprises peuvent refuser l'expédition à certaines régions, décider quelles régions et quels clients obtiennent les ASIC les plus performants, fabriquer des tirages limités et manipuler les prix.

Pour empêcher les mineurs ASIC de monopoliser le hachage du réseau, de nombreuses cryptomonnaies développent des algorithmes de hachage résistants aux ASIC, comme Scrypt et Ethash [25][26]. Jusque récemment, Monero a utilisé l'algorithme de hachage CryptoNight, qui nécessite de grandes quantités de cache L3 pour fonctionner. En théorie, cela aurait dû rendre difficile la production d'une puce ASIC avec de grandes exigences de mémoire. Cependant en 2018, Bitmain a publié le X3, une puce ASIC spécifique pour CryptoNight, qui est capable d'extraire jusqu'à dix fois la vitesse d'un processeur graphique (GPU) [27]. D'autres algorithmes de hachage ont subi des sorts similaires : Scrypt, Ethash, et Equihash sont maintenant tous exploités par des ASICs.

Pour lutter contre l'utilisation des ASICs, Monero a proposé une stratégie de modification majeure de protocole (appelée « hard fork » en anglais) tous les 3-6 mois pour changer sensiblement l'algorithme de hachage CryptoNight (la première modification passe à CryptoNightV7) [28]. Le capital et le temps requis pour construire un ASIC sont importants, et avec de grandes spécificités matérielles, de petites modifications dans un algorithme de hachage devraient invalider la conception de la puce, et ainsi gaspiller temps et argent des fabricants d'ASIC. Cependant, cette approche a aussi ses problèmes. Si les modifications apportées à l'algorithme sont insuffisantes pour empêcher les ASIC d'être reprogrammés, le réseau peut devenir vulnérable à la centralisation des taux de hachage jusqu'à ce qu'une autre modification majeure soit possible. Les réseaux de portes programmés (FPGA en anglais - Field Programmable Gate Arrays) devraient également être pris en compte dans les stratégies de résistance aux ASICs. En effet, de légères modifications non fréquentes de l'algorithme peuvent être facilement reprogrammés pour les FPGAs. Les changements réguliers des mécanismes fondamentaux de consensus introduisent la possibilité de bogues involontaires et généralement centralisent le développement autour de l'équipe de base des développeurs, ce qui est aussi préoccupant.

Un certain nombre d'algorithmes alternatifs en preuve de travail ont été proposés pour lutter contre la nécessité de modifier régulièrement le protocole, y compris des algorithmes de hachage difficilement mémorisables comme Argon2, Balloon hash, et des algorithmes de hachage polymorphes comme ProgPoW et RandProg [29][30][31][32].L'équipe Loki publiera des recherches supplémentaires sur les algorithmes susmentionnés pour développer une solution à long terme à la résistance ASIC.

Alors que ce travail est entrepris, Loki incorporera une version de CryptoNight appelée CryptoNight Heavy, qui maintient une résistance ASIC contre les mineurs ASIC de CryptoNight. CryptoNight Heavy diffère de CryptoNight V7 de plusieurs façons : il fournit une augmentation de la taille du bloc-notes (scatchpad) à 4 Mo, et un changement dans la manière dont les implosions et explosions sont traitées [33]. Ces changements le distinguent de Monero CryptoNight V7, qui est la plus grande cible pour les mineurs ASIC, et fournissent également une protection plus robuste contre le développement ASIC jusqu'à ce qu'une solution plus permanente soit proposée.

7.2 Taille de bloc dynamique

Comme les autres pièces CryptoNote, Loki n'a pas de taille de bloc fixe. Ainsi, la taille des blocs évolue dans le temps, augmentant pour inclure plus de transactions lorsque le réseau atteint des niveaux plus élevés de débit de transactions. La taille des blocs de Loki se mesure en observant la moyenne des tailles de blocs sur les 100 derniers blocs, et en conséquence, recible peu à peu la taille maximale de chaque nouveau bloc.

La préoccupation à long terme des autres crypto-monnaies est que les grandes tailles de bloc surchargent les nœuds qui stockent et vérifient les transactions. À mesure que les tailles de bloc augmentent, les nœuds qui fonctionnent sur du matériel de qualité inférieure sont incapables de traiter et de propager de nouveaux blocs, ce qui entraîne la centralisation du réseau de nœuds parmi ceux ayant un intérêt commercial dans le maintien des nœuds. Ce qui peut être inquiétant car distribuer la chaîne de blocs (plus communément appelée « blockchain ») à travers de nombreux nœuds permet à l'état de la chaîne d'être confirmée par différentes parties, ajoutant ainsi à sa validité et à sa résistance à la censure.

Pour Loki, une partie de la récompense de bloc est donnée aux nœuds de service qui traitent et propagent les blocs en tant que nœuds complets. Du fait que les nœuds de service avec une bande passante et une performance insuffisante sont supprimés du réseau de nœuds de service, le groupe (« pool ») qui sera récompensé s'auto-impose une exigence de performance. Cette incitation ne garantit pas seulement que le nombre de nœuds reste élevé, mais aussi que ces nœuds soient d'un niveau de performance suffisant pour réussir partager les données de la blockchain sur le réseau, quelle que soit la croissance de la blockchain ou à quel point le besoin en bande passante est exigeant. Même ainsi, les optimisations de taille des transactions sont toujours nécessaires pour garantir que le réseau évolue de manière efficace afin de conserver les coûts opérationnels des nœuds de service bas, de sorte qu'un grand nombre de nœuds puisse être maintenu sur le long terme.

7.3 Taille de la signature de cercle

Les signatures de cercle sont utilisées pour masquer les sorties réelles parmi d'autres dans une transaction donnée. La taille d'une signature de cercle fait référence au nombre de signatures combinées (« mixins » en anglais) utilisées pour construire le cercle.

Monero a actuellement une taille de signature de cercle minimale obligatoire de sept, avec six signatures combinées utilisées en marge de la sortie réelle non dépensée dans une transaction. L'effet de plus grandes tailles de cercles a été peu étudié, cependant, dans le document 0001 (publié par le Monero Research Lab), l'effet de modifier les tailles de cercle a été analysé contre un pirate qui possédait un grand nombre de sorties sur la blockchain [34]. Il en résulte que de plus grandes tailles de cercle réduisent le délai pendant lequel un pirate malveillant possédant de nombreuses sorties non dépensées serait en mesure d'effectuer une analyse efficace des transactions. Utiliser de plus grandes tailles de cercle protège également contre une attaque théorique connue sous le nom d'attaque EABE / Knacc [35], où un tiers (ici un échange) peut effectuer une analyse temporelle limitée sur les transactions entre deux utilisateurs.

De plus, Monero n'a pas de taille de cercle maximale imposée par les règles de consensus réseau. Beaucoup de portefeuilles comme le portefeuille GUI Monero plafonne la taille du cercle à 26. Cependant, un utilisateur est libre de manuellement créer une transaction avec n'importe quelle taille de cercle, tant qu'elle est au-dessus de la taille de sept. Le problème

est que la plupart des portefeuilles ont une taille de cercle par défaut de sept. Augmenter la taille de cercle d'une transaction au-dessus de sept fait qu'elle se remarque (figure 3). De plus, si des transactions individuelles devaient toujours utiliser un cercle de taille non standard dans Monero (dix par exemple), un tiers passif pourrait analyser les blockchains et en déduire des modèles en utilisant l'analyse temporelle.

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

FIGURE 3: *xmrchain.net (explorateur de blocs Monero) qui montre comment se distinguent les tailles de cercle non standard*

Loki améliore ces deux problèmes en appliquant de manière statique des tailles de cercle et en définissant cette taille à dix. Rendre statique la taille de cercle maximale protège les utilisateurs qui construisent des cercles avec plus de neuf signatures combinées et régler la taille de cercle minimale à dix empêche un pirate possédant un grand nombre de sorties de discerner les vraies sorties dépensées dans une signature de cercle. De plus grandes tailles de cercle augmentent également l'efficacité des combinaisons par défaut de manière non linéaire, devenant plus efficaces à mesure que les tailles de cercle augmentent.

Dans le schéma de transaction actuel, augmenter la taille de cercle à 10 conduirait à une augmentation de 2,6% de la taille de la transaction. Cependant, lorsque les pare-balles sont implémentés, cela représentera une augmentation d'environ 8 à 13% de la taille d'une transaction. C'est à cause de la réduction globale de la taille des transactions occasionnée par les pare-balles. L'augmentation de la taille minimale de cercle peut présenter un problème sur un réseau qui manque d'architecture pour prendre en charge des transactions de plus grande taille, en raison de l'augmentation des frais généraux. Avec Loki cependant, cette charge peut être portée par le service de nœuds, qui sont incités à fonctionner et fournir une bande passante suffisante.

8 Prévention des attaques

8.1 IP et blocage des paquets

Bien que le réseau de nœuds de service n'ait pas de défaillances importantes, deux menaces importantes sont à considérer pour le réseau : les attaques de collecte et l'inspection approfondie des paquets [36][37]. Les attaques de collecte cherchent à rassembler les adresses IP de tous les nœuds de service du réseau et à utiliser des remaniements de niveau ISP pour bloquer les connexions à ces adresses particulières. Ce type de censure est régulièrement effectué sur le réseau Tor en Chine [38]. L'inspection approfondie des paquets (DPI) vise à étudier la structure de chaque paquet individuel qui passe à travers un pare-feu, et supprime ou bloque une sélection de paquets qui semblent se rapporter à un service particulier. Encore une fois, le DPI a été largement utilisé par des acteurs étatiques [39].

Beaucoup de travail a été fait pour concevoir des systèmes qui échappent au DPI. Les utilisateurs peuvent tirer parti des types de transports enfichables qui modifient la signature de chaque paquet pour apparaître comme un trajet normal non bloqué. Le blocage d'IP est généralement évité en exécutant des ponts de façade de domaine (« domain fronting bridges ») qui crypteront le trafic avec des requêtes HTTPS permettant de débloquer des services tels qu'Azure ou Cloudfare. Une fois qu'ils atteignent le service débloqué, le pont transmettra la demande à l'endroit désiré. Dans le cas d'un front de domaine, il devient difficile pour un acteur au niveau de l'Etat d'empêcher l'ensemble des flux de trafic vers les ponts reconnus sans causer de perturbation significative à l'utilisation générale d'Internet.

Les mécanismes de gouvernance intégrés à Loki peuvent être utilisés pour faire fonctionner les ponts de façade de domaine afin que les utilisateurs puissent accéder aux services Loki dans les pays où la censure Internet est légion. De plus, le support de transport enfichable OBFS4 sera fourni avec la sortie du nœud de service lié au portefeuille Loki pour aider à protéger davantage contre les DPI [40].

8.2 Attaques par déni de service

Les utilisateurs de la blockchain décentralisée ne sont pas tenus de fournir des identifiants numériques ou physiques. Cela peut être bénéfique pour les utilisateurs qui n'ont plus de pièces d'identité ou qui sont persécutés à cause de cela. Cependant, les systèmes qui ne nécessitent pas d'identification de l'utilisateur deviennent vulnérables à des attaques Sybil, où un acteur malveillant produit de nombreuses fausses identités (dans le cas de Loki, de nombreuses paires de clés publiques-privées) et utilise ces identités pour spammer le réseau de requêtes.

Beaucoup de crypto-monnaies ont lutté contre ce problème, et sont forcées de mettre en œuvre soit un modèle avec des frais de service ou un modèle de preuve de travail. Dans les modèles de paiement à l'acte tels que Siacoin, les utilisateurs paient pour les services qu'ils utilisent. Dans le cas de Siacoin, le coût est déterminé par l'espace de stockage (n TB) utilisé par mois [41]. Les modèles de paiement contre un service sont efficaces pour réduire les attaques de Sybil, cependant, ils éloignent de nombreux utilisateurs du système, en particulier lorsque des services similaires sont disponibles gratuitement (comme Google Drive et Onedrive dans le cas de Siacoin). Les systèmes de preuve de travail tels que ceux utilisés dans Hashcash et Nano exigent que les utilisateurs calculent une petite preuve de travail avant d'envoyer un message ou une transaction [42][43]. Ces petits systèmes de preuve de travail sont sans doute plus égalitaires que le modèle de rémunération à l'acte, mais peuvent devenir la proie des attaquants qui possèdent de grandes quantités de puissance de calcul.

Loki propose un schéma de preuve de travail modifié pour répondre aux deux plus grandes attaques de Sybil auxquelles le système Loki fait face : les messages hors ligne et la création de chemin. Les messages hors ligne présentent une cible potentielle car chaque message doit être stocké par un swarm de neuf nœuds. Des abus potentiels pourraient survenir lorsqu'un utilisateur malveillant surcharge un swarm particulier avec un volume élevé de messages qu'il devrait stocker. Dans les attaques de création de chemin, l'attaquant cherche à s'engager dans le processus de création de chemin avec autant de nœuds que possible, en prenant les ressources de bande passante et refusant le service aux utilisateurs qui créent des chemins à travers le réseau à des fins légitimes.

Pour prévenir ces deux attaques, le réseau Loki exige qu'une courte preuve de travail soit

effectuée lorsque les messages et les chemins sont créés. Pour les messages, cette preuve de travail est calculée comme un hachage Blake2b du message. Pour la création de chemin, la preuve de travail est envoyée avec la demande d'inclusion d'un nœud dans le processus de construction de chemin. Pour assurer l'évolutivité et l'accessibilité pour les utilisateurs mobiles, l'exigence de preuve de travail est basée sur le Durée de vie (TTL) du message ou du chemin, et non basée sur l'activité réseau globale.

8.3 Marquage du swarm

Lorsque les nœuds fonctionnent dans un environnement sans confiance et sans un chef central faisant respecter des règles primordiales, le maintien du bon comportement des nœuds sur le réseau devient difficile. Bien que Les nœuds de service dans Loki doivent contenir l'exigence de garantie correcte, ils peuvent choisir de ne pas acheminer le trafic ou stocker des données dans leurs pools de mémoire. Parce que cette option est financièrement avantageuse (en utilisant moins de bande passante / cycles CPU / stockage), un système de signalement doit être proposé d'éliminer les nœuds sous-performant.

Pour Loki, un tel système de signalement distribué fait face à des problèmes majeurs de mise en œuvre. Fondamentalement, chaque Le nœud de service est financièrement incité à signaler tous les autres nœuds de service en tant que mauvais acteur. Lorsque un nœud de service est signalé, il sera confronté au retrait du groupe et de ce fait, cela augmente les chances aux signaleurs de gagner une récompense. Une méthode potentielle pour ce système de signalement distribué est celui dans lequel une preuve est fournie lorsqu'un signalement se produit, cependant, cette solution tombe en proie à des nœuds fabriquant des preuves en leur faveur. Inversement, signalé sans restriction permet à des nœuds individuels ou à des groupes de nœuds collaboratifs d'intentionnellement signaler des nœuds honnêtes afin d'améliorer leurs chances de gagner des récompenses de bloc. Afin de contourner ces problèmes, Loki propose un signalement en swarm (« swarm flagging »).

Un signalement en swarm fonctionne en utilisant des swarms existants pour choisir les membres qui participent à chaque tour de test. Chaque nœud de service contient une copie de la blockchain, et chaque bloc créé par un mineur sélectionnera de manière déterministe un certain nombre de swarms de test. Pour chaque bloc, 1% des swarm de réseaux sont sélectionnés pour participer à un swarm d'essais. Pour calculer les swarms participants, le hash des cinq blocs précédents est utilisé pour distribuer une fonction « Mersenne Twister » qui sélectionne ensuite les swarms par ordre de leur position dans la liste déterministe.

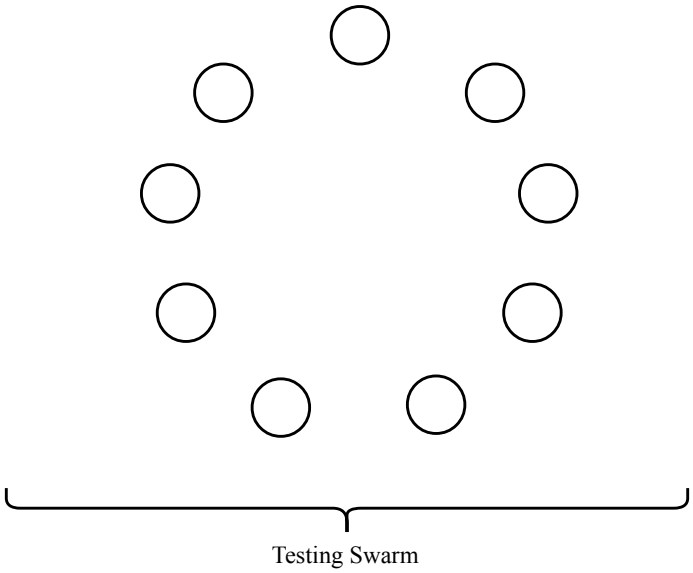

FIGURE 4: *Un swarm de test est un swarm sélectionné de 9 nœuds*

Lorsqu'un swarm test a été sélectionné pour participer, chaque nœud de ce swarm doit effectuer un certain nombre de tests sur tous les autres nœuds du swarm. Ce ne sont pas des tests actifs ; chaque nœud stocke plutôt des informations historiques sur ses interactions avec tous les autres nœuds dans son swarm. L'information sur la bande passante, le stockage des messages, les requêtes sur la blockchain, et la fonctionnalité de sortie de nœud est collectée et conservée au fil du temps. Les nouveaux entrants dans le swarm qui doivent encore recueillir cette information peut interroger les nœuds de service en dehors de leur swarm immédiat afin pour recueillir des données sur chacun des nœuds de service qu'ils testent.

Chaque nœud de service décide comment voter sur chacun des autres membres du swarm. Une fois qu'il a pris sa décision sur la base des tests susmentionnés, elle recueille et diffuse ses votes dans le swarm. Chaque nœud du swarm peut maintenant vérifier les votes pour tous les membres. Si un seul nœud dans le swarm a plus de 50% des nœuds votants contre lui, chaque membre du swarm a les informations nécessaires pour construire une transaction de désenregistrement. Une fois cette transaction validée et incluse dans un bloc, tous les nœuds de service mettent à jour leur DHT, purgeant tous les nœuds qui ont été votés négativement.

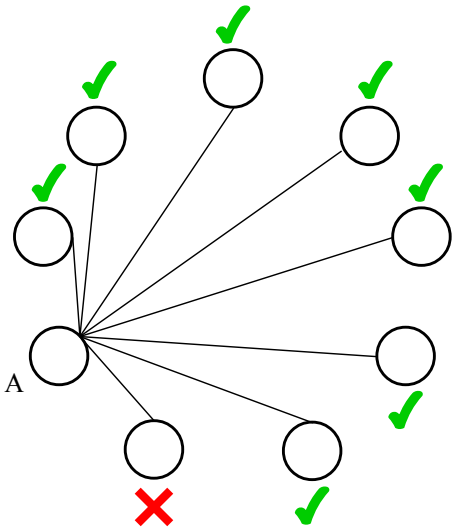

FIGURE 5: *Le noeud malhonnête est testé par le noeud A, si le noeud malhonnête échoue à un test. Le nœud A parvient à comprendre en local les nœuds qui échouent ou qui réussissent les tests.*

8.3.1 Suite de tests

Afin de permettre au réseau d'auto-appliquer les normes de performance, les nœuds de service doivent être équipés des outils nécessaires pour tester d'autres nœuds de service. Ces tests devraient couvrir la portée de toutes les fonctionnalités fournies par les nœuds de service pour empêcher les attaques paresseuses de masternode [44]. Dans cette conception initiale, quatre tests fondamentaux sont proposés. D'autres tests peuvent être ajoutés à cette suite de tests parallèlement au développement des nœuds de service.

Lorsqu'un opérateur exécute le logiciel de nœud de service pour la première fois, un fichier vide avec une taille prédéterminée est alloué sur un disque pour garantir la présence d'espace pour les tâches nécessitant un stockage. Par la suite, un simple test de bande passante est effectué entre le nœud de service et un ensemble de serveurs de test reconnus par la Fondation Loki. Ces vérifications sont facultatives, et Les nœuds de service sont autorisés à les passer, les ignorer ou les échouer, et à rejoindre un groupe de nœuds de services non fiables. Cependant, lancer et passer ces tests fournit un bon indicateur à tout candidat potentiel en tant qu'opérateur de nœuds de service pour savoir s'ils doivent risquer de bloquer du collatéral dans un nœud qui ne répond pas aux exigences minimales. Une fois qu'un nœud de service rejoint un groupe de nœuds de service non approuvé, leur collatéral est verrouillé et ils sont testés par le prochain swarm choisi. Les tests de swarm sont réalisés par consensus et les nouveaux entrants dans le réseau de nœuds de service ne peuvent échapper à ces tests. Si un nœud réussit tous les tests de swarm, il reçoit une mention de nœud de confiance et peut commencer routage des paquets. A défaut, ils sont retirés du réseau et leur collatéral reste verrouillé pendant 30 jours.

Test de bande passante

The bandwidth test forms the backbone of the Loki network test suite. If a node passes this test then it is assumed to be honestly routing packets above the minimum threshold.

Chaque fois qu'un nœud interagit avec un autre nœud de service, il crée et conserve un enregistrement de la bande passante entrante fournie. Au fil du temps, les nœuds seront

inclus dans des milliers de chemins et achemineront des millions de messages. Ces interactions formeront la des tables de bandes passantes de chaque nœud. À partir de cette table, un nœud peut répondre aux tests de bande passante sur les nœuds de service à l'intérieur son swarm.

Tous les nœuds doivent également répondre aux requêtes des autres nœuds sur leurs propres tables de bande passante. Cela signifie que même les nœuds qui ont récemment rejoint le réseau peuvent interroger le réseau plus large pour des informations sur n'importe quel nœud de leur swarm.

Test de stockage de messages

Le stockage des messages est essentiel pour la fonctionnalité de messagerie hots ligne pour les utilisateurs de Loki Messenger. Les nœuds de service doivent être testés pour leur capacité à mettre en cache les messages et à les transmettre aux utilisateurs au cours du Time-to-live (TTL) du message.

Les utilisateurs qui envoient des messages hors ligne sélectionnent de manière aléatoire un nœud de service parmi le swarm des utilisateurs destinataire. Ce nœud doit distribuer une copie du message parmi le reste du swarm. En fonction de la preuve de travail attachée à l'en-tête du message, les nœuds de service qui reçoivent une copie stockeront les données pour le TTL. Lorsque le TTL sur le message original atteint la finalité, le nœud de distribution envoie un nonce à tous les autres membres du swarm. Le swarm utilise le nonce en l'ajoutant au message puis en hachant le résultat puis en l'envoyant en retour au nœud de distribution. Ce test garantit que les nœuds de service contiennent des messages jusqu'à la finalité du TTL, et font face à l'expulsion si elles sont incapables de produire le résumé du message correct. Comme l'échantillonnage du nœud de distribution est aléatoire, avec le temps, chaque nœud de service pourra collecter des données de performance sur leurs homologues dans le swarm en question.

Test de stockage sur la blockchain

Service Nodes are expected to hold a full copy of the Loki blockchain. By holding a full copy of the blockchain, Service Nodes can perform a number of tasks that are essential to users of the network including acting as a remote node, validating transactions, and locking transactions in Blink.

Comme les nœuds honnêtes détiennent aussi une copie de la blockchain, un nœud malhonnête pourrait éviter de détenir une copie complète en demandant simplement des blocs d'un nœud honnête lors des tests. Pour éviter cela résultat, le test de stockage sur la blockchain est conçu de sorte que les nœuds honnêtes qui détiennent une copie de la blockchain peuvent passer ce test, contrairement aux nœuds malhonnêtes.

Pour arriver à cela, le nœud de test demande à chaque nœud testé de faire une sélection aléatoire de K transactions dans l'histoire de la blockchain qui sont ensuite concaténées et hachées. Ce hachage est ensuite renvoyé au nœud de test. En mesurant la latence de cette requête, le nœud de test peut comparer la latence avec le temps de retour attendu T. La valeur exacte pour T sera définie pour différencier exactement la latence attendue entre le chargement à partir du disque et le téléchargement des blocs du réseau. Pour tout attaquant, il devrait être impossible de télécharger et hacher K blocs en un temps T, et ainsi les attaques de ferroutage deviennent difficiles.

Exit Node Test

Les nœuds de service qui opèrent comme nœuds de sortie reçoivent des récompenses supplémentaires, et donc des tests fonctionnels sont nécessaires pour s'assurer que cette récompense supplémentaire n'est pas abusée.

Pour qu'un test de sortie fonctionnel se produise, un nœud de service doit être en mesure d'émuler le comportement de recherche d'un humain. Si un nœud de service peut détecter qu'il est testé, il peut répondre uniquement aux tests et rejeter les demandes d'utilisateurs légitimes. Émuler un comportement naturel de requête d'une page est difficile, cependant, les tests de sortie peuvent être conçus de manière à rendre les efforts de tri entre les demandes légitimes et les tests suffisamment difficiles pour que la différence de coût de bande passante entre l'exécution d'un nœud légitime et un nœud malveillant est négligeable.

Les nœuds de service utilisent une liste de moteurs de recherche, détenus localement, combinés à un dictionnaire de manière à construire des termes de recherche naturels pseudo-aléatoires. Les termes de recherche sont ensuite introduits dans les moteurs de recherche et les pages Web sont choisis au hasard parmi les résultats. Le nœud Service peut maintenant générer un chemin avec des nœuds aléatoires faisant office de relais et le nœud étant testé en tant que nœud de sortie. De cette sortie, le nœud de service demande le résultat de la page Web générée à partir de sa recherche pseudo-aléatoire. Si le résultat renvoyé par le nœud de sortie correspond au résultat généré par le nœud de service, le nœud de sortie est réputé avoir passé le test.

9 Gouvernance, financement et vote

La gouvernance est une partie essentielle de la conception de crypto-monnaie et devrait être soutenue au niveau de protocole. Le risque d'une gouvernance faible et informelle a été étudié de manière approfondie tout au long de l'histoire de la technologie de la blockchain. Bitcoin et Ethereum ont expérimenté des modifications de protocole qui ont divisées l'attention et les efforts de leurs communautés respectives. Bien que ces modifications puissent être utilisées comme stratégie de gouvernance, elles doivent toujours être considérées comme un dernier recours plutôt que la solution à tous les problèmes litigieux. Le système de gouvernance Loki est conçu pour résoudre les problèmes potentiels en fournissant un environnement structuré pour la discussion et la représentation, et aussi pour financer le développement de Loki sans dépendance avec des influenceurs externe or sans être guidé par l'altruisme.

Au-delà de la prévention des modifications de protocoles, les structures de gouvernance devraient créer les moyens de financer en interne de nouveaux projets qui améliorent l'écosystème de Loki. Le financement interne de projets peut empêcher la formation de groupes d'intérêts spéciaux qui n'ont pas nécessairement les motivations qui correspondent aux utilisateurs, aux mineurs ou aux nœuds de service. Nous avons vu cela dans Bitcoin et diverses modifications du Bitcoin avec la formation de sociétés à but lucratif, telles que Blockstream, Bitcoin ABC, et Bitcoin Unlimited, qui ont été fréquemment accusés d'embaucher des développeurs pour apporter des changements spécifiques au protocole Bitcoin et Bitcoin Cash visant à poursuivre leurs propres objectifs commerciaux ou suivre leur idéologie spécifique.

C'est pour cette raison que dans chaque bloc de Loki, 5% de la récompense est allouée à cette fin de la gouvernance du réseau. Cela fournit un flux constant de Loki qui sera distribué parmi projets communautaires, les développeurs de logiciels et les équipes d'intégration. De cette

récompense de 5%, 3,75% est contrôlé par la Fondation Loki et 1,25% est contrôlé par les nœuds de service grâce au système de financement Loki. Ce qui encourage une représentation équitable des nœuds de service et permet des propositions de financement communautaire qui peuvent se produire en dehors du contrôle direct de la Fondation Loki.

9.1 La Fondation Loki

La fondation Loki est une organisation à but non lucratif basée en Australie. Cette entité centrale légale existe pour permettre au projet Loki de fonctionner dans un cadre juridique bien défini et de donner à ceux qui travaillent sur le projet des protections juridiques et des obligations. La fondation Loki a été constituée en Australie en 2018 et utilise la même constitution que l'exemple fourni par l'Australian Charities and Non-Profit Commission (ACNC) [45]. Cette constitution donne à la fondation la même structure de gouvernance d'entreprise que autres organisations sans but lucratif, lorsque la société n'a ni actionnaires ni bénéficiaires, les membres du conseil d'administration ont chacun des sièges assortis d'un mandat et mènent des actions en votant sur les résolutions proposées par leurs collègues. La fondation Loki est structurée pour obtenir le statut d'organisme de bienfaisance enregistré en Australie.

Cette organisation est constitutionnellement tenue de dépenser tout revenu (y compris la gouvernance récompense en bloc) sur l'avancement du projet et les initiatives alignées au projet. En tant qu'organisation externe auditée, la transparence est essentielle au maintien de tout statut d'organisme de bienfaisance que la fondation Loki reçoit, et d'assurer le grand public que la fondation Loki demeure honnête et maintient ses dépenses dans des limites raisonnables. La fondation Loki est responsable devant la communauté et ses auditeurs. Si ce système devait finalement échouer à servir Loki et ses projets environnants, des protections dures existent. Si une modification de protocole avec suffisamment de consensus sur le réseau émerge, il existe une possibilité d'enlever ou de remplacer la fondation Loki en tant que destinataire de cette récompense de bloc.

9.2 Le système de financement Loki

Bien que la fondation Loki soit faite à partir d'un groupe diversifié de personnes qui représentent le projet Loki, la fondation est soumise à la fois à sa propre constitution et aux lois australiennes. Cela pourrait s'avérer un facteur limitant dans l'éventail des décisions que la fondation peut prendre. Le système de financement Loki permet à une partie de la récompense d'être exercé uniquement par un vote des nœuds de service. Les nœuds de service représentent des entités de partout dans le monde et ne sont pas obligés d'apporter leur contribution à l'équipe ou à la fondation du projet Loki, cela leur permet d'atteindre un nouveau niveau d'autonomie dans les décisions qu'ils peuvent prendre. Les nœuds de service sont les participants les plus impliqués dans le réseau et ils sont incités financièrement pour prendre des décisions qui augmentent la valeur de Loki.

9.2.1 Proposals

Chaque proposition présentée aux nœuds de service est publiée dans la blockchain Loki. Si une partie donnée veut présenter une proposition aux nœuds de service, la partie doit

construire une transaction de proposition. Parce que le contenu des transactions de propositions doit être lisible et les sorties doivent être brûlées, elles renoncent aux caractéristiques de confidentialité des transactions typiques de Loki.

Des blocs de financement sont créés tous les 43 000 blocs (environ 60 jours). Les meneurs de propositions peuvent soumettre leurs propositions à tout moment pendant cette période. Cependant, il devrait être considéré que plus ils se rapprochent du début de chaque phase de proposition, plus ils auront de temps pour accumuler des votes de la part de chaque nœud de service.

Chaque transaction est accompagnée d'un champ supplémentaire contenant les informations que chaque Le nœud de service doit comprendre pour voter sur la proposition. Cette information comprend : un titre pour la proposition, une URL reliant à une explication détaillée de la proposition, la quantité de Loki dont la proposition a besoin, une adresse de paiement, et un agent pour le séquestre si choisi.

En attendant l'accord de la fondation Loki, les utilisateurs qui font des propositions peuvent également choisir la fondation Loki ou toute autre tierce partie à agir en tant qu'agent de séquestre, libérant des fonds lorsque les objectifs sont atteints. De plus, pour encourager un haut niveau de propositions et prévenir du spam de ces transactions, chaque transaction de proposition doit brûler un montant non-trivial de Loki.

9.2.2 Vote

Chaque nœud de service porte une clé spécifique pour le vote. Cette clé peut être exportée et utilisée pour voter au nom d'un nœud de service sans avoir à se connecter au serveur sur lequel il est hébergé.

Le vote ne se fait pas sur la blockchain, mais chaque nœud de service signale son soutien, sa dissidence ou l'abstinence pour chaque proposition active sur la blockchain. Les nœuds de service peuvent voter sur des propositions dès qu'ils sont engagés dans la blockchain jusqu'au prochain bloc de financement bimestriel. Peu de temps avant la création du prochain bloc de financement, un swarm est choisi pour recueillir un décompte de tous les votes qui ont été exprimés. Ce décompte est ensuite soumis dans les groupes mémoire de nœuds et vit là jusqu'à ce qu'un mineur atteigne le bloc de financement. Cette information est ensuite utilisée pour construire le bloc qui alloue une récompense aux propositions gagnantes. Les propositions sont seulement passées lorsque le résultat des votes « oui » moins ceux du « non » est égal à 15% du nombre de nœuds sur le réseau du nœud de service.

9.2.3 Distribution des fonds

Tous les produits du système de financement Loki sont payés par des blocs de financement. Les récompenses des blocs de financement fonctionnent de la même manière que les récompenses traditionnelles, comme un moyen entièrement libérateur de distribuer des Loki. Tous les 43 000 blocs (environ 60 jours), un bloc de financement est construit par les mineurs. Ce bloc contient 1,25% de la récompense globale du bloc pour l'ensemble de la période du bloc de financement.

Pour construire un bloc de financement valide, les mineurs doivent être en mesure d'évaluer les propositions qui ont atteint le pourcentage requis de votes. Ceci est fait en utilisant les informations que les nœuds de service partagent à la blockchain, qui contient à la fois les

adresses à payer et l'état de tous les votes. Tous les nœuds de service valideront le bloc de financement des mineurs et élimineront tout financement de bloc sur des adresses invalides.

Souvent, la somme de Loki requise par les propositions approuvées dépassera ou sera inférieure au montant total accumulé au cours de cette période de 60 jours. Si la somme totale des propositions approuvées dépasse ce qui est disponible dans le bloc de financement, le mineur construira le bloc de financement en priorisant les propositions qui ont été validées dans la blockchain plus tôt. Les propositions approuvées restantes resteront engagées dans la blockchain jusqu'au prochain bloc de financement.

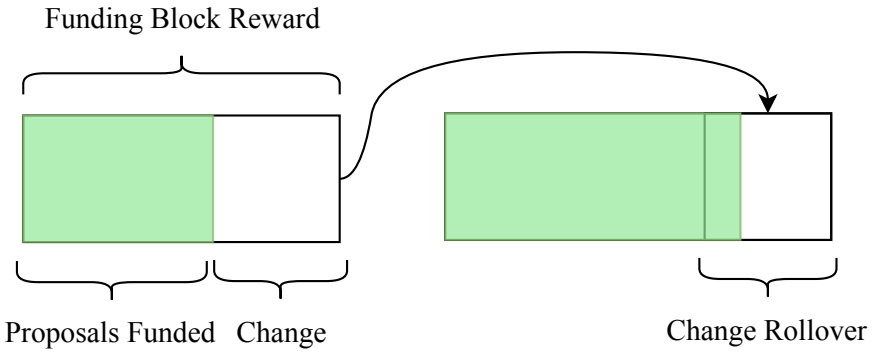

FIGURE 6: *Les fonds inutilisés qui sont laissés créent un changement intéressant qui augmente la récompense du prochain bloc de financement.*

10 Conclusion

Loki propose un modèle pour les transactions anonymes et la communication décentralisée basé sur un réseau de nœuds économiquement incités. Loki utilise les fondations du protocole CryptoNote pour assurer la confidentialité et met en œuvre un système de nœud collatéralisé pour améliorer la résistance et la fonctionnalité du réseau.

De plus, Loki propose des améliorations sur des recherches antérieures et des projets open source et puis présente un nouveau protocole de routage anonyme qui offre d'importants avantages par rapport aux protocoles existants. La combinaison d'une architecture unique et d'une conception de protocole crée un réseau avec une résistance Sybil, diminuant l'efficacité de l'analyse temporelle, et fournissant aux utilisateurs un degré élevé de confidentialité numérique.

Références

[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 : Eqypt 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.