Sécurité et confidentialité du réseau Libra

La sécurisation du réseau Libra est la responsabilité principale de l'association Libra. Ce document décrit les engagements de l'association Libra en matière de sécurité et de confidentialité.

Un réseau sécurisé

La blockchain Libra est un système distribué qui gère la possession de Libra ainsi que leur transfert d'un utilisateur à un autre. Il est donc important que chaque utilisateur de Libra possède une vision cohérente du système, sans quoi un acteur malveillant pourrait faire croire à quelqu'un qu'il a déjà été payé alors que les fonds n'ont jamais été versés. Cette pratique est connue sous le nom de « l'attaque des 51 % ».

La blockchain Libra se protège de ce type d'attaque grâce au protocole de consensus LibraBFT. Le LibraBFT s'appuie sur des décennies de recherche en informatique sur la manière dont des groupes d'ordinateurs peuvent travailler ensemble même dans le cas où des comportements fautifs affectent certains de ces ordinateurs. Cette catégorie d'algorithmes est connue sous le nom de Byzantine Fault Tolerant. Le terme « Byzantine » fait référence à la capacité du protocole à tolérer des fautes en présence de comportements perturbants ou erronés d'une minorité d'ordinateurs (par exemple suite au piratage d'un ordinateur ou à un bug).

Le protocole Libra implémente une base de données authentifiée de façon cryptographique. La base de données est gérée par le réseau distribué de nœuds de validation qui suivent le protocole de consensus LibraBFT. Le protocole peut tolérer jusqu'à un tiers de nœuds de validation compromis et malgré tout continuer à garantir la cohérence du traitement des transferts de Libra. Dans le cadre du protocole LibraBFT, les nœuds de validation génèrent des signatures cryptographiques attestant de l'état de la blockchain Libra. La blockchain Libra utilise des arbres de Merkle. Il s'agit d'une structure de données qui permet aux utilisateurs du monde entier de combiner les signatures cryptographiques des nœuds de validation avec des données connues sous le nom de « preuves ». Ce faisant, ils obtiennent une entrée authentifiée pour une transaction donnée sur la blockchain Libra, sachant que la transaction ne peut pas être modifiée ou annulée.

Nœuds de validation fiables

Le LibraBFT permet à la blockchain Libra de tolérer des fautes au sein du réseau de validation, mais nécessite que deux tiers des nœuds de validation fonctionnent correctement pour assurer la sécurité du réseau. Au lancement du réseau, les nœuds de validation seront exécutés par les Membres fondateurs, c'est-à-dire par des organisations qui répondent à une liste de critères garantissant leur réputation. Notre objectif est de lancer le réseau avec cent membres fondateurs, ce qui signifie qu'un maximum de trente-trois nœuds fautifs peut être toléré. Chaque organisation exécutera son nœud de façon indépendante et l'isolera des autres systèmes exécutés par l'organisation. Il sera donc extrêmement difficile de pirater trente-trois nœuds exécutés séparément pour lancer une attaque contre le système.

L'écosystème Libra est diversifié : les organisations qui composent le groupe de nœuds de validation proviennent de plusieurs secteurs et industries et sont d'origines géographiques diverses. Cela permettra de créer une infrastructure solide et répartie dans le monde entier, ce qui augmentera sa résilience et évitera que les nœuds de validation deviennent la cible d'une influence ou d'une attaque commune.

Logiciel sécurisé

La sécurisation de la blockchain Libra nécessite également un logiciel sécurisé et bien développé, sans quoi tous les nœuds de validation pourraient être vulnérables. Développer un logiciel sécurisé requiert un mélange de techniques éprouvées, d'ingénierie et d'innovation.

Utiliser une technologie éprouvée standard permet d'assurer la sécurité du logiciel. L'association a choisi d'implémenter Libra Core (l'implémentation de référence du protocole Libra) à l'aide de Rust, car ce langage à mémoire sécurisée permet d'atténuer certaines des failles de sécurité dangereuses les plus courantes. L'association Libra repose sur des protocoles de cryptographie éprouvés. Le procédé de signature EdDSA est utilisé pour protéger les transactions. Noise est utilisé pour empêcher un nœud de validation d'en imiter un autre.

Dans d'autres cas, la sécurité dépend du domaine du génie logiciel. Par exemple, Libra Core est conçue pour isoler les composants essentiels du logiciel sur lesquels le réseau s'appuie pour la sécurité des autres composants moins sensibles du système. Ainsi, la fonctionnalité principale du système n'est pas affectée, même si les composants moins sensibles du logiciel comportent un bug.

Dans le cas où les algorithmes et l'ingénierie ne résoudraient pas le problème, Libra s'appuie sur des approches innovantes. Par exemple, plusieurs approches algorithmiques sont en cours d'évaluation pour aider LibraBFT à protéger le réseau des attaques par déni de service. La blockchain Libra utilise Move, un nouveau langage de contrat intelligent spécialement développé pour Libra. Move est conçu pour sécuriser l'écriture des programmes qui gèrent les ressources Libra.

Préparation de réponse en cas d'incident

L'association Libra veillera à préparer des réponses en cas d'attaques potentielles. Par exemple, l'association élaborera une stratégie pour répondre au scénario peu probable et exceptionnel dans lequel un tiers des nœuds de validation ont un comportement malveillant et causent un embranchement. Cette stratégie nécessiterait d'arrêter temporairement le traitement des transactions de la réserve Libra, de déterminer l'étendue des dégâts de l'attaque et de publier une recommandation sur la façon d'appliquer des mises à jour logicielles pour résoudre l'embranchement. L'association élaborera également des stratégies pour d'autres scénarios, tels que la découverte de failles logicielles.

Protection de la confidentialité des utilisateurs

L'association Libra reconnaît l'importance de la confidentialité sur la blockchain publique, mais est également consciente des risques d'utilisation détournée. L'association en elle-même n'est pas impliquée dans le traitement des transactions et ne stocke aucune donnée personnelle des utilisateurs de Libra. Les transactions sont traitées et stockées par les nœuds de validation. Les transactions sont créées par les utilisateurs du système et contiennent généralement des informations telles que l'adresse de l'expéditeur et du destinataire sur la blockchain publique, ainsi que le montant de la transaction. Lorsqu'elle est stockée

sur la blockchain Libra, une transaction est associée à des métadonnées qui contiennent l'heure de son enregistrement sur la blockchain et le nœud de validation à l'origine de son ajout. Les transactions ne contiennent pas de liens menant à l'identité réelle d'un utilisateur.

Cette approche suit la norme des transactions pseudonymes adoptées par d'autres blockchains majeures. Cette approche est bien connue de nombreux utilisateurs, développeurs et régulateurs. L'association Libra surveillera l'évolution du protocole et du réseau de la blockchain Libra. Elle continuera à évaluer des techniques inédites pour renforcer la confidentialité de la blockchain, tout en tenant compte des problématiques pratiques et évolutives ainsi que de l'impact de la réglementation.

Transparence et responsabilité envers la communauté

Libra est conçue pour être transparente par défaut. Le fonctionnement de tous les validateurs peut être audité par n'importe quel participant et l'ensemble du traitement des transactions est disponible pour être confirmé par chacun. L'association Libra favorise des examens complets de sécurité et encouragera les chercheurs dans le domaine de la sécurité à identifier les bugs de la blockchain grâce au programme de signalement de bugs basé sur un système de récompenses prévu.

L'association s'engage par ailleurs à développer la blockchain Libra de façon publique afin de recueillir des avis rapidement, à mesure que des décisions clés en matière de conception sont prises. Elle utilisera ces avis pour transformer le prototype en système de production fiable. L'association travaillera également en étroite collaboration avec une communauté d'experts mondiaux dans des domaines tels que la protection des données, la sécurité, la cryptographie, l'ingénierie, l'expérience utilisateur et les politiques afin d'examiner, de développer et de partager des recommandations pour garantir la sécurité de l'ensemble de l'écosystème Libra.

Travailler avec l'application de la loi

Comme dans le cadre de n'importe quelle devise ou infrastructure financière, des malfaiteurs tenteront d'exploiter le réseau Libra. Tant que le réseau est ouvert et accessible à toutes les personnes qui ont accès à Internet, les principaux points de terminaison du réseau devront respecter les lois et réglementations applicables et collaborer avec les organismes d'application de la loi. De plus, le fait que les transactions sur la blockchain Libra se fassent sur la base du pseudonymat permet à des tiers de réaliser des analyses afin de détecter toute activité frauduleuse ou illégale.