Note to readers: This report has been modified to incorporate updates to the Libra payment system as found in the White Paper v2.0.

Security on the Libra Network

Keeping the Libra network secure is the primary responsibility of the Libra Association. This document outlines the Libra Association's commitments to security.

A Secure Network

The Libra Blockchain is a distributed system that manages both ownership and transfer of single-currency Libra Coins and multi-currency Libra Coins (≋LBR) from one Libra Blockchain address to another. It is important that every user of the Libra network sees a consistent view of the system — otherwise, a malicious actor might be able to trick somebody into thinking that they were paid when, in fact, the malicious actor never sent the funds. This is known as a "double-spending attack."

The Libra Blockchain prevents this type of attack using the Libra Byzantine Fault Tolerant (LibraBFT) consensus protocol. LibraBFT builds on decades of research in computer science on ways in which groups of computers can work together even though some of those computers might experience faulty behavior — a class of algorithms that are referred to as Byzantine Fault Tolerant. The term "Byzantine" refers to the protocol's ability to tolerate faults in the presence of disruptive or erroneous behavior by a minority of computers — something that could happen because the computer was compromised or because of a bug.

The Libra protocol implements a cryptographically authenticated database to record accounts and their balances. The database is maintained by the distributed network of validator nodes that follow the LibraBFT consensus protocol. The protocol can tolerate up to one-third of the validator nodes being compromised and still guarantee consistency in processing transfers of Libra Coins. As part of the LibraBFT protocol, the validator nodes generate cryptographic signatures, attesting to the state of the Libra Blockchain. The Libra Blockchain uses a Merkle tree data structure to allow any user, anywhere in the world, to combine the cryptographic signatures of the validator nodes with a small piece of data — known as a "proof" — to get an authenticated record of any transaction on the Libra Blockchain, knowing that the transaction can never be changed or reversed.

Reliable Validator Nodes

Validator nodes will be run by Members, each of which will be subject to robust due diligence procedures by the Association. This model is referred to as permissioned, an approach that promotes security of the network based on the quality of participating Association Members. However, being permissioned does not imply closed participation. LibraBFT is designed to facilitate open and dynamic participation via reconfiguration. The Association will set open-call criteria to ensure that the selection processes for expanding and renewing the membership are objective and transparent.

LibraBFT allows the Libra Blockchain to tolerate faults within the validator network but still requires two-thirds of the validator nodes to function correctly in order for the network to be secure. Each organization will run (or have run on its behalf) its validator node independently and is expected to isolate the validator node from other systems the organization runs. This will make it extraordinarily difficult for an attacker to compromise over a third of nodes required to launch a successful attack against the system. The Libra network is diverse — the organizations that make up the pool of validator nodes are geographically diverse and from a variety of industries and sectors. This will create a strong and distributed infrastructure, which will increase resiliency and is designed to ensure that the validator nodes are not subject to common influence or attack.

Secure Software

Keeping the Libra Blockchain secure also requires well-written, secure software — otherwise, all of the validator nodes could suffer from a common vulnerability. Writing secure software requires a combination of proven techniques, engineering discipline, and innovation.

Using standard, proven technology is a way to keep software secure. The Association has chosen to implement the Libra Core — the reference implementation of the Libra protocol — using Rust because this memory-safe language can help mitigate some of the most common and dangerous security vulnerabilities. The Association relies on proven cryptography protocols. The EdDSA signature scheme is used to protect transactions. The Noise Protocol is used to prevent a validator node from impersonating another validator node and to secure their network communications.

In other cases, security depends on software engineering discipline. For example, Libra Core is designed to isolate the core parts of the software that the network relies on for security from other less sensitive parts of the system. This ensures that even if the less sensitive parts of the software have a bug, the core system functionality will not be impacted.

The Libra Blockchain uses a new smart contract language called Move, which was developed specifically for the Libra network. Move is designed to make it safe to write programs that manage Libra Coins. Every Move method is subjected to bytecode-level verification before it is deployed. Additionally, Move is designed to make it easier to express and automatically prove that transactions satisfy certain properties. For example, payment transactions may only change the account balances of the payer and receiver. A team of renowned researchers is working toward a semantic-level smart-contract verification system that incorporates advanced formal methods toward verifying Move contracts.

Incident Response Readiness

The Libra Association is preparing responses to potential attacks. For example, the Association is preparing a strategy for addressing the exceptionally unlikely scenario that one-third of the validator nodes behave maliciously and cause a fork. This strategy would involve temporarily halting the processing of transactions from the Libra Reserve, determining the extent of the damage from the attack, and publishing a recommendation as to how software updates should be applied to resolve the fork. The Association is also preparing strategies for other scenarios, such as the discovery of software vulnerabilities, by defining secure software update protocols and their governance.

Transparency and Accountability Towards the Community

The Libra payment system is designed to be transparent by default. Any participant can audit the operation of all validators, and all on-chain transaction processing is available to be confirmed by anyone. Digital signatures on payments prevent unauthorized transfers since they can be detected through audits on the public chain. The Association facilitates comprehensive security reviews and will encourage security researchers to identify bugs in the Libra Blockchain open-source software.

Since the announcement of the Libra project in June 2019, the Association has worked with regulators, central bankers, elected officials, and various stakeholders around the world to determine the best way to marry blockchain technology with accepted regulatory frameworks. The Association is committed to continuing to involve the open-source community and using the best open-source practices to engineer a robust payment system. The Association held a Bug Bounty program on its testnet and will continue to work closely with the worldwide community of experts in areas like data protection, security, cryptography, engineering, user experience, and policy in order to review, develop, and share best practices to ensure the security of the entire Libra network.

Working with Law Enforcement

As with any currency or financial infrastructure, bad actors will inevitably try to exploit the Libra network. While the network is open and accessible to everyone with internet access, the network's main endpoints will need to follow applicable laws and regulations and collaborate with law enforcement. In addition, since transactions on the Libra Blockchain are recorded on a public chain, it is possible for third parties to conduct analyses to detect patterns of fraud and potentially illegal activity. The Association will operate a Financial Intelligence Unit Function to monitor the network and flag potential suspicious and sanctioned activity on the Libra network, and work with both government authorities and service providers to seek to detect and deter inappropriate use of the platform.