Security and Privacy 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 and privacy.

A Secure Network

The Libra Blockchain is a distributed system that manages both ownership of Libra and the transfer of Libra from one user to another. This means that it is important that every user of Libra see 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 LibraBFT consensus protocol. LibraBFT builds on top of decades of research in computer science on ways in which groups of computers can work together despite the fact that 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. The database is maintained by the distributed network of validator nodes that follow 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. 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

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. At the beginning of the network, validator nodes will be run by the Founding Members — organizations that meet a list of criteria to ensure that they are reputable. Our target is to launch the network with 100 such members — meaning that up to 33 faulty nodes could be tolerated. Each organization will run its node independently and will isolate the node from other systems the organization runs. This will make it extraordinarily difficult for an attacker to compromise 33 separately run nodes that would be required to launch an attack against the system.

The Libra ecosystem is diverse — the organizations that make up the pool of validator nodes are from a variety of industries and sectors and will be located in different places around the world. This will create a strong and distributed infrastructure, which will increase resiliency and ensure 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 Libra Association relies on proven cryptography protocols. The EdDSA signature scheme is used to protect transactions. Noise is used to prevent a validator node from impersonating another node.

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.

In cases where proven algorithms and engineering discipline do not address an issue, Libra relies on innovative approaches. For example, a number of algorithmic approaches are being evaluated to help LibraBFT protect the network against Denial of Service attacks. The Libra Blockchain uses a new smart contract language called Move, which was developed expressly for Libra. Move is designed to make it safe to write programs that manage Libra assets.

Incident Response Readiness

The Libra Association will work to prepare responses to potential attacks. For example, the association will prepare 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 will also prepare strategies for other scenarios such as the discovery of software vulnerabilities.

Protecting User Privacy

The Libra Association recognizes the importance of privacy on the public blockchain — but also recognizes the risks of misuse. The association itself is not involved in processing transactions and does not store any personal data of Libra users. Transactions are processed and stored by validator nodes. Transactions are created by users of the system and typically contain information such as the sender and receiver's public blockchain address and the transaction amount. When stored on the Libra Blockchain, a transaction will be associated with metadata containing the time the transaction was committed to the blockchain and the validator node that added the transaction to the blockchain. Transactions do not contain links to a user's real-world identity.

This approach follows the norm of pseudonymous transactions adopted by other major blockchains. This approach is familiar to many users, developers, and regulators. The Libra Association will oversee the evolution of the Libra Blockchain protocol and network, and will continue to evaluate new techniques that enhance privacy in the blockchain while considering concerns of practicality, scalability, and regulatory impact.

Transparency and Accountability Towards the Community

Libra is designed to be transparent by default. The operation of all validators can be audited by any participant, and all transaction processing is available to be confirmed by anyone. The Libra Association facilitates comprehensive security reviews and will encourage security researchers to identify bugs in the blockchain software through the planned Bug Bounty program.

Additionally, the association is committed to developing the Libra Blockchain in the open to get early feedback as key design decisions are made, and it will use this feedback to turn the prototype into a robust production system. The association will also 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 ecosystem.

Working with Law Enforcement

As with any currency or financial infrastructure, bad actors will 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, because transactions on the Libra Blockchain are pseudonymous, it is possible for third parties to do analysis to detect fraud and illegal activity.