Moving Toward Permissionless Consensus

Shehar Bano, Christian Catalini, George Danezis, Nick Doudchenko, Ben Maurer,
Alberto Sonnino, Nils Wernerfelt*

This document outlines some of the questions, decisions, and challenges the Libra Association will face on the journey to permissionless governance and consensus.

A key distinction in the blockchain space is the one between **permissioned systems**, in which only a defined set of entities can shape consensus and governance, and **permissionless systems**, where anyone that follows the rules of the protocol and contributes the right types of resources (e.g., computing power in the case of a proof-of-work system) can do so.

This distinction is important not only from a technical perspective but also from an economic one: **permissionless systems have low barriers to entry and innovation, are resistant to censorship attacks, and encourage healthy competition** among infrastructure providers (e.g., who can participate in consensus) as well as the developers of applications on top of the network [1]. Since nobody can exclude others from the market or censor their transactions, permissionless systems provide stronger guarantees to participants that **no single party will be able to unilaterally change the rules of the network** to their advantage at a future date. At their core, permissionless systems make irreversible commitments to operating as open networks where changes can only be implemented if they are democratically supported by a majority of constituents.

For all these reasons, and to ensure that Libra is truly open and always operates in the best interest of its users, our ambition is for the Libra network to become permissionless. The challenge is that as of today we do not believe that there is a proven solution that can deliver the scale, stability, and security needed to support billions of people and transactions across the globe through a permissionless network.

With the testnet, the association starts the journey toward building a permissionless system. And while there are a number of technical and economic challenges that will need to be solved together with the open-source community to make this a reality, we believe that for the Libra network to achieve its full potential, it needs to be permissionless. **As a result, one of the association's directives will be to work with the community to research and implement this transition, which will begin within five years of the public launch of the Libra Blockchain and ecosystem.**

Essential to the spirit of Libra, in both its permissioned and permissionless states, the Libra Blockchain will be open to everyone — any consumer, developer, or business can use the Libra network, build products on top of it, and add value through their services. Open access ensures low barriers to entry and innovation and encourages healthy competition that benefits consumers. This is foundational to the goal of building more inclusive financial options for the world.

Revised August 14th, 2019

1 Starting Point

Since the association had to start as a permissioned system, it introduced measures to **mitigate some of the major concerns about permissioned networks.**

1. No Centralized Control: The degree of influence platform architects retain over permissioned networks and their ability to change the rules of protocol to their advantage after others have joined (what economists call a "hold-up problem") was an area of concern.

- **Therefore, the Libra Association was established**, composed of entities acting as validator nodes, collectively and democratically making decisions on the future of the network and protocol. The Libra Association is an independent, not-for-profit entity that no single Founding Member can control. All decisions require participation by a majority of the Founding Members.
- To ensure a **plurality of opinions and voices**, Founding Members of the association are geographically distributed and diverse businesses, nonprofit and multilateral organizations, and academic institutions.

2. Distributed Reserve Collateral: We introduced the reserve to ensure that Libra is a great medium of exchange and store of value from day one. However, we did not want the assets used to back coins to become a single point of failure or for the reserve to be able to mint coins without backing, which would introduce inflation in the system.

- This is why the reserve will be held by a **geographically distributed and highly respected global network of custodians with investment-grade credit rating to limit counterparty risk.** Safeguarding the assets, providing extremely high auditability and transparency, avoiding the risks of a centralized reserve, and achieving operational efficiency are the key parameters we will follow in custody selection and design.
- **The reserve cannot print coins without full backing** and can only use as assets certain currencies and treasuries of highly stable and respected central banks. Changes to the composition of the basket require a supermajority vote by the association.

3. Progressive Opening of Participation in the Network: While at launch the Founding Members will advance the governance of the association and will be in charge of running validator nodes and protecting the network, irreversible commitments have been made to rapidly open up participation to new members.

- **It was determined that membership decisions should neither become an area of contention nor a way to increase barriers to entry for new players.** Nonprofit and multilateral organizations and social impact partners will also be able to apply for grants to join the network.
- There will be a reliance on these criteria (which the association will expand over time) to ensure that the entities joining the network in its early phases — when it is most vulnerable — have an established reputation offline and can be trusted with securely operating validator nodes and defending the network.
- As the technology matures, the Libra Blockchain will transition from relying on the votes based on association membership — in order to operate validator nodes and vote on governance — to relying on ownership of Libra coins. The basic intuition is that at scale the network should be owned by its users and should always evolve in a way to protect their interests and assets.

2 Open Technical and Economic Challenges

Before the network can be truly permissionless, the association will need to find technical and economic answers to the open problems below. Some of these are challenging, unsolved research and development questions, and some involve high-assurance engineering, which takes time. With the help of the open-source community, substantial progress will be made toward solving them. The association will also dedicate grants for researchers and entrepreneurial teams interested in helping us get there.

2.1 Technical and economic challenges:

- **Defining on-chain governance contracts.** Some governance actions and processes, such as the definition of the validator node set in epochs, distribution of fees, abuse reporting, etc., may initially be performed off-chain by the association. For the network to become permissionless, progressively more of these governance actions should be implemented on-chain, including the ability to modify the rules of the network over time.
- **Market design.** We have started to understand the governance and equilibrium structure of a financial system based on stake holdings and consumer confidence in wallets and other delegates. In the process, we have identified new market design trade-offs between the Libra approach and more established alternatives like proof of work. Nevertheless, more research is needed to determine how best to maintain long-run competition in the ecosystem while ensuring the security and efficiency of the network. Furthermore, as stake-based governance introduces path dependence in influence, it is essential to explore mechanisms for protecting smaller stakeholders and service providers [2].
- **Scaling.** The initial system that will be built aims to have 1,000 tx/sec for a set of 100 validator nodes. As the validator node set grows, that will lead to a decline in performance. The association needs to understand how to maintain acceptable performance while expanding participation and increasing the number of validators.
- **Understanding the Sybil resistance assumption.** The current assumption is that more than two-thirds of the votes are coming from honest participants. Once the network transitions, it will require that at least two-thirds of coin holders are acting honestly. Since a malicious entity can accumulate coin holdings and try to attack the system, safeguards will need to be in place to prevent such behavior. In time, such safeguards can be relaxed once the total value of Libra in circulation is large enough to make such an attack impractical.
- **Defining an effective and fair model for delegation of stake and for responding to validator node misbehavior.** Since anyone holding Libra will be able to become a validator node when the network is permissionless, the association needs to define how users that do not wish to take part in the consensus process will be able to delegate this role to entities they can trust, and, importantly, what information needs to be provided to them to update their decision if abuse is detected. Rules for responding to abuse will also need to be established. Fairness concerns will also need to be addressed to allow the ecosystem to thrive in the long run.
- **Defining a strategy for extending the Move platform on top of a permissionless network.** The Move language is currently only exposed to built-in smart contracts such as the ones that manage the validator node set and the Libra coin. As the language stabilizes, the association plans to open up the language to third-party development. In order to enable effective decision making after the transition to permissionless, the association will need to establish guiding principles that help the community make decisions around key questions, such as the direction of innovation of the language, and the pace of core updates to it. The association will also need to establish community best practices around formal verification, security, etc.

- **Decentralizing the reserve function.** The reserve allows users of the system to enjoy a relatively stable medium of exchange from the start. At the same time, it also represents a centralized function. For the network to be fully permissionless, the association will have to explore ways to further distribute and decentralize the reserve, including automating the verification of the assets in the basket and the process of minting and burning of coins. Increasing market competition in the custody and management of the reserve will also be explored to improve the efficiency of this service, and the costs it imposes on users and custodians over time.

2.2 Governance Challenges

- **Defining processes for the evolution of the protocol.** Protocols need to evolve and introduce new features in response to new needs that the network will discover as it scales. This work happens through the interaction between the open-source community and the association. While at the beginning the evolution of the protocol will be supported by the coordination work of the Founding Members, as the network transitions to permissionless, the community will need to develop a robust process and clear principles for managing improvement proposals and providing open-source leadership.
- **Understanding how the association can support a healthy ecosystem.** When governance is distributed, the association will have to design robust on-chain procedures for coordinating responses and stopping the most dangerous abuses of the network.
- **Defining emergency governance and breaks.** What happens if the network comes under a large-scale attack, connectivity breaks, or other global events take place that affect the operations of the network? How can a response be effectively coordinated when ownership and governance are fully distributed across coin holders? To ensure safety, the association will need to develop robust processes for coordination to emerge in a decentralized way.

Acknowledgments

We would like to thank the following people for helpful discussions and feedback on this paper: Adrien Auclert, Morgan Beller, Dan Boneh, Ravi Jagadeesan, Scott Duke Kominers, Roberto Rigobon, Catherine Tucker, and Kevin Zhang.

References

[1] C. Catalini and J. S. Gans, "Some simple economics of the blockchain." *National Bureau of Economic Research*, 2016.

[2] C. Catalini S. D. Kominers and R. Jagadeesan, "Market design for a blockchain-based financial system." *Social Science Research Network*, 2019.