Libra Blockchain

libra

An overview of libra

libra

Nearly 1.7 billion adults globally remain outside of the financial system with no access to a traditional bank, people with less money pay more for financial services. The world truly needs a reliable digital currency and infrastructure that together can deliver on the promise of "the internet of money." Moving money around globally should be as easy and cost-effective as — and even more safe and secure than — sending a text message or sharing a photo. So, Facebook introduced libra blockchain (programmable database).

The mission for Libra is a simple global currency and financial infrastructure that empowers billions of people. Libra is made up of three parts that will work together to create a more inclusive financial system:

- It is built on a secure, scalable, and reliable blockchain
- It is backed by a reserve of assets designed to give it stability
- It is governed by the independent Libra Association tasked with evolving the ecosystem.

The unit of this currency is called "Libra." Libra will need to be accepted in many places and easy to access for those who want to use it. Libra will start as a permissioned blockchain with ambition for the Libra network to become permissionless.

The Libra Association

Libra Association is an independent, not-for-profit, membership organization headquartered in Geneva, Switzerland. The association is governed by the Libra Association council, which comprises of one representative per validator node. Together, they make decisions on the governance of the network and reserve. Initially, this group consists of the founding members: businesses, nonprofit and multilateral organizations, and academic institutions from around the world. All decisions are brought to the council and major policy or technical decisions require the consent of two-thirds of the votes, the same supermajority of the network required in the BFT consensus protocol.

Technical overview

Consensus and Incentivization

The consensus algorithm is like practical Byzantine Fault Tolerance with few tweaks and it is called LibraBFT which is a variant of the HotStuff consensus protocol.

In the case of validators process transactions submitted by client and other validators, to make consensus protocol reliable even in case the presence of malicious and erroneous behaviour by majority of validators, validators take turns driving the process of accepting transactions. When a validator acts as a leader, it proposes transactions, both - those directly submitted to it by clients and those indirectly submitted through other validators. The leader is selected by an unpredictable leader election mechanism in which the leader of a round is determined by the proposer of the latest committed block using a verifiable random function. Gas will be consumed to execute transactions which will be given to validators as incentive.

Initially only defined validations are allowed voting for transactions validations but in future Libra plans to gradually transition to a proof-of-stake system where validators are assigned voting rights proportional to the number of Libra coins they hold.

Smart contracts and languages

Smart contracts will be written in Move, a programming language built for the Libra blockchain . According to the language whitepaper, Move is an “executable bytecode language used to implement custom transactions and smart contracts”. One of the features of this currently-permissioned blockchain is out-of-the-box smart contracts that are pre-approved for running on the network. However, these smart contracts will be the only ones that are able to be executed at the time of the network’s launch. While this set up limits the possible functionalities on day one for companies and individuals adopting the chain, this limitation also reduces the likelihood of any error that occurs on chain, such as the Ethereum Parity Wallet incident as the only functions allowed are peer reviewed amongst the consortium and in the open-source community.

Move has three important roles in the system:

To enable flexible transactions via transaction scripts.

To allow user-defined code and data types, including “smart contracts” via modules.

To support configuration and extensibility of the Libra protocol

A Two-Token system

Just like in MakerDao's MKR (governance token) & DAI (stablecoin) system, and other two-token systems in the crypto asset industry, there will be a governance token called the Libra Investment Token (LIT), which will allow for participation in the governance of the network. The value of this token stems from the value of partaking in this governance, or potentially any revenues or rewards paid to network maintainers and is decoupled from the day-to-day value of the payments token. Instead, the value of the governance token relies on the longevity and utility value of the payments token offered by the consortium.

However, it is important to note that nonprofits, NGOs, and other impact-oriented organizations may be able to participate in the governance without holding the minimum $10M worth of LIT. With many impact-oriented organizations conducting international payments and transactions, Libra's lowered barrier to entry for such institutions may be a significant incentive for adoption, as seen by the already-announced participation from 3 major social impact organizations: Kiva, Mercy Corps, & Women's World Banking.

For regular, non-impact-oriented entities, it will be important to clarify down the road if this threshold to participate is measured in USD terms, or as a % of holdings of the total network (i.e. 1% assuming a max of 100 validators).

Performance

The mission of the Libra protocol is to support a global financial infrastructure. Performance is an integral part of meeting that need.

There are three main components of blockchain performance:

- Throughput: The number of transactions that the blockchain can process per second.

- Latency: The time between a client submitting a transaction to the blockchain and another party seeing that the transaction was committed.

- Capacity: The ability of the blockchain to store a large number of accounts.

Libra protocol support 1,000 payment transactions per second with transactions per second with a 10-second finality time between a transaction being submitted and committed.

Node requirements to meet this 1,000 payment transactions:-

Bandwidth:

Each transaction requires around 5 KB of traffic — including the cost of receiving the transaction via the mempool, rebroadcasting it, receiving blocks from the leader, and replicating to clients — then validators require a 40 Mbps internet connection to support 1,000 transactions per second.

CPU:

Signature verification is a significant computational cost associated with a payment transaction. The protocol to allow parallel verification of transaction signatures. Modern signature schemes support over 1,000 verifications per second over a commodity CPU.

Disk:

Servers with 16 TB of SSD storage, if accounts are approximately 4 KB, then this allows validators to store 4 billion accounts

Conclusion

Facebook's initiative, with the Libra cryptocurrency at the center of the project, will have a significant impact on the financial industry and global economies from both a medium and long-term perspective. Backed by a basket of fiat currency-denominated assets in its initial release, Libra represents a first attempt at creating a world currency, on-chain or not, with everyday usage by billions of individuals and institutions across the globe. However, the magnitude of its success will vary greatly on how Libra can convince regulators and financial institutions to collaborate with the consortium in establishing an agile framework that satisfies the need for decentralized governance while being compliant with existing domestic and international regulations.

Thank You

Contact Us

brian@coingape.com