Facebook's Libra: design and potential shortcomings as a means of digital payment

Kazuhiro Sudo
10.September.2019

Nomura Research Institute, Ltd.

Executive Summary

Facebook created a big stir globally when it announced plans to issue its own cryptocurrency, Libra. Libra is designed to meet the minimum requirements of a means-of-payment currency–price stability, scalability and privacy–but it may need more work both technologically and on the regulatory front.

Kazuhiro Sudo

Senior Consultant

Financial DX Business Design Department

Facebook's forthcoming Libra cryptocurrency

Facebook recently created a big stir globally by announcing plans to launch its own blockchain-based cryptocurrency named Libra in 2020. Initially called GlobalCoin, Libra is a financial inclusion initiative with a mission to establish "a simple global currency and financial infrastructure that empowers billions of people." It aims to give people throughout the world, including 1.7 billion of those who do not have bank accounts, access to widely circulating global currency. Libra can be used for everyday transactions, and eventually achieve the "Internet of money."

Libra's features[1]

Libra will be issued as a currency for everyday use by the Libra Association, a Geneva-based NPO. Libra Association has an internationally diversified membership comprising 27 companies/organizations in addition to Facebook. It plans to expand to 100 members by Libra's launch date. Libra is designed to be a stable store of value much less volatile than other cryptocurrencies like Bitcoin. It will be backed by a Libra Reserve consisting of low-risk liquid assets such as government securities and bank deposits denominated in multiple fiat currencies[2]. The reserve will be seeded with funding from Libra Association members, each of which will invest a minimum of US$10 million in exchange for Libra Investment Tokens. Interest earned on its assets will be distributed, net of expenses, to Libra Association members as dividends. Fiat currency payments received from users in exchange for newly minted Libra will also be deposited into the Libra Reserve but users will not receive dividends on their Libra holdings. All of the net income generated by the Libra Reserve's assets will be distributed to Libra Investment Token holders. Once the reserve reaches a certain critical mass, Libra Investment

NOTE
1) An introductory white paper on Libra is available in nine languages, including Japanese, at https://libra.org.

2) As of July 2019, the Libra Association plans to invest some 50% of the reserve in USD assets and the remainder in EUR, JPY and GBP assets.

Tokens' yield should increase in tandem with the reserve's size.

When users exchange fiat currency for Libra or vice-versa, they must do so through an authorized reseller. In Japan, the regulatory regime applicable to Libra resellers will depend on whether Libra is legally classified as a virtual currency (cryptoasset), forex trade or security. Additionally, users will need a wallet (the crypto-equivalent of a bank account) to hold, spend, transfer or otherwise use Libra. Facebook has established a subsidiary, Calibra, to develop and deploy a wallet. Wallet accounts will be subject to KYC (know your customer) requirements in compliance with anti-money-laundering and counter-terrorism-financing regulations. After exchanging fiat currency for Libra through an authorized reseller, end users will presumably store their Libra in a Calibra wallet and use it for payments/remittances[3].

3) Libra is slated to be transferable via messaging apps such as Messenger and WhatsApp. Eventually, it could conceivably be used for payments sent/received via Libra Association members' services.

Technologically, the Libra blockchain will require scalability sufficient to accommodate billions of accounts, robust security and the flexibility to effectively govern the Libra ecosystem. To meet these basic requirements more easily, the Libra Association plans to initially use a consortium blockchain before transitioning

Exhibit: Libra ecosystem (as of July 2019; assumption-based where noted)
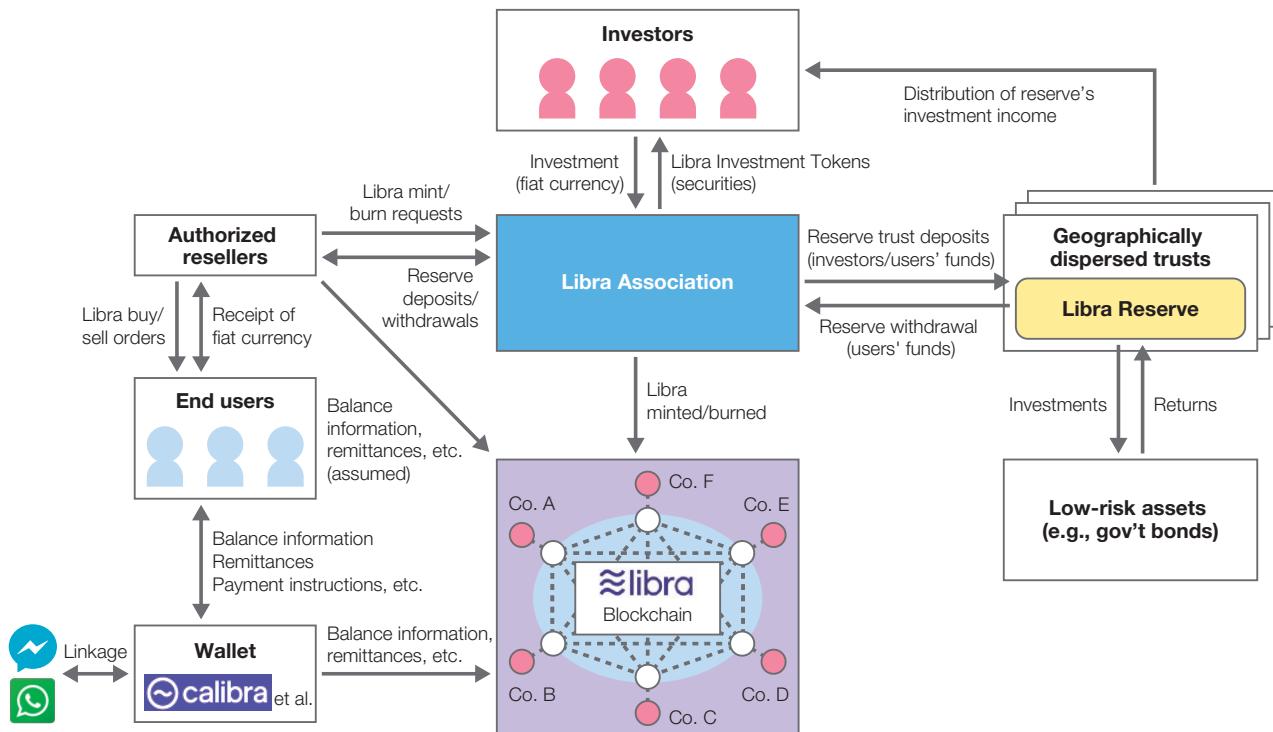
Source: NRI, based on Libra white paper

to an open-source public blockchain like Bitcoin's. Additionally, smart contracts will be implemented on the Libra blockchain using a newly developed secure programming language called Move. Libra may supplant existing smart contract platforms such as Ethereum and EOS.

Addressing Libra's potential shortcomings as a means of payment

How viable is Libra as a means of payment?[4] First, numerous stablecoins[5] designed to maintain a peg with a fiat currency have been issued in response to cryptocurrencies' price volatility. With Libra slated to be collateralized by a reserve denominated in a basket of fiat currencies, it should have some degree of price stability. However, given the reserve's planned 50% allocation to US dollar assets, users that purchase Libra with other currencies could be exposed to considerable dollar exchange-rate risk.

Second, to be scalable enough to accommodate routine payments[6], Libra will initially use a consensus algorithm that obtains consent from only trusted nodes of the consortium blockchain. While Libra has achieved a throughput of 1,000 transactions per second, roughly 100 times greater than Bitcoin's, it falls short of Visa's reported processing capacity by an order of magnitude. However, David Marcus, head of Calibra, has mentioned that many Libra transactions could potentially be processed by Calibra wallet servers instead of on the blockchain. If such centralization is permitted, it may resolve the throughput constraint.

Lastly, on the issue of privacy[7], Libra is currently similar to Bitcoin in that addresses and wallet balances and transaction histories linked to addresses are not encrypted. However, if the bulk of Libra transactions are processed by Calibra's wallet servers as Marcus hinted, transaction histories and wallet balances linked to KYC-compliant individuals could potentially be kept confidential from third parties by sequestering them within the Calibra wallet without recording them on the blockchain.

While Libra appears to broadly meet the requirements of a means-of-payment currency, it currently seems dependent on the Calibra wallet to adequately address scalability and privacy issues. If so, users would have to trust Calibra and its parent, Facebook, which was rocked by a data privacy scandal last year. Their perceived trustworthiness could be a major stumbling block. That said, with technology rapidly advancing throughout the cryptocurrency space, Libra

---

[4] Currencies typically serve as a unit of account, store of value and medium of exchange. We focus on the medium-of-exchange function, referred to herein as "means of payment."

[5] Stablecoins include cryptocurrencies that pursue price stability through algorithmically simulated central banking (e.g., Basis) in addition to those collateralized by fiat currencies (e.g., Tether, TrueUSD) or virtual currencies (e.g., MakerDAO).

[6] Means used to increase scalability include off-blockchain payment channels (e.g., Lightning Network) and sidechains (e.g., Plasma) in addition to improvements to the blockchain itself, such as changes in blockchain structure (e.g., block size enlargement, transaction size compression) and consensus algorithm changes (e.g., from proof of work to proof of stake).

[7] Certain cryptocurrencies (e.g., Monero, Zcash, Grin, Beam) have addressed the issue of privacy by anonymizing balances and/or transaction histories recorded on the blockchain.

8) Facebook's earnings report for the second quarter of 2019 disclosed that Facebook is at risk of incurring increased expenses or losing its investment in Libra if unable to roll out Libra and related services as planned or unable to do so at all.

might be able to resolve its scalability and privacy issues through a combination of technological innovation and migration from a consortium model to a public blockchain[8].

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $4.5 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including New York, London, Tokyo, Hong Kong and Singapore, and over 13,000 employees.
 For more information, visit https://www.nri.com/en
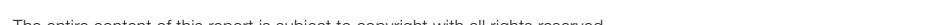
Inquiries to : Financial Market & Innovation Research Department
          Nomura Research Institute, Ltd.
          Otemachi Financial City Grand Cube,
          1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
          E-mail : kyara@nri.co.jp

http://fis.nri.co.jp/en/publication/kinyu_itf/backnumber.html