libra Compendium

XAVIER LAVAYSSIÈRE

hello@libracpd.com

https://libracompendium.com

Disclaimer

This report is intended to be an efficient overview of the Libra project for professionals. As it covers a broad range of specialized topics, it features simplifications and probably inaccuracies. Your expertise is more than welcome to rectify them: hello@libracpd.com

License

Academic Format (APA): Lavayssière, X. (2019). Libra Compendium <https://libracompendium.com>

Cover image: *Geneva* by Stéphane Pecorini, CC BY-SA

Early Release of July 9, 2019

Table of contents

> *If comitum vel baronum nostrorum, sive aliorum tenencium de nobis in capite per servicium militare, mortuus fuerit, and cum decesserit heres suus plene etatis fuerit and relevium debeat, habeat hereditatem suam per antiquum relevium; scilicet heres vel heredes de baronia comitis integra per centum libras;* [1]
>
> Magna Carta, 1215

Introduction

Libra is a project of a digital currency presented as means of payment for people less served by current banking and payment services. Facebook Inc, the main instigator of the project, positions itself as co-founder of the Libra Association and also as a user of the project via a subsidiary **Calibra**.

In recent years, the digital industry has begun a shift towards payments and financial services. **Wechat** and **Alipay** share a market in China worth more than $ 40 trillions in 2018[2]. **Google** and **Apple** are developing payment solutions[3] relying on their control of mobile operating systems. **Amazon** benefits from its intermediary position to offer payment solutions[4].

Between 2010 and 2013, Facebook had already proposed *Facebook Credits* to allow payment in games and applications. In 2015, the company gave the ability to make payment between users via Messenger[5] and extended it in Europe in 2017. The service was discontinued in April 2019. It should be noted that David Marcus, former president of Paypal, was then responsible for the messaging products at Facebook[6].

The firm must indeed offer additional services of its advertising activities to develop its ecosystem and to "diversify its revenue stream. Without devices or a large marketplace, the firm has to rely on its

[1] "If any of our earls or barons, or others holding of us in chief by military service shall have died, and at the time of his death his heir shall be of full age and owe relief he shall have his inheritance on payment of the ancient relief, namely the heir or heirs of an earl, 100 pounds for a whole earl's barony; the heir or heirs of a baron, 100 pounds for a whole barony; "

[2] People's Bank of China, Report 2018 http://www.gov.cn/xinwen/2019-03/20/content_5375401.htm

[3] Google Pay, Apple Pay, Apple Card

[4] Amazon Pay, Amazon gift cards, Amazon Store card, Amazon Rewards Visa Signature …

[5] Facebook, Press Release, March 2015

[6] See infra Teams

messaging system to be able to offer payment solutions. Nevertheless, this new project is notable for its stated ambition and model. Facebook's strategy has been included in a broader global currency project.

The organisation, vocabulary, and technologies used follow ideas and trends of cryptocurrencies and distributed systems over the last years. The project is presented as experimental at the technical and strategy level, published early in order to “encourage open discussion by design” [7]. Its outcome, final form, and scale are still uncertain. Nevertheless, this announcement allows envisioning profound political and regulatory effects as well as consequences on the development of the ecosystem of cryptocurrencies and related technologies.

[7] David Marcus, Libra, 2 weeks in, 3 July 2019
https://www.facebook.com/notes/david-marcus/libra-2-weeks-in/10158616513819148/

Equos [...] quamlibet commodis conpendioque priuato deriuandam duxerit esse iacturam, unius auri librae condemnatione multatus largitionibus nostris cogatur esse munificus.[8]

Theodosian code, 438

Economic Functioning

The objective is to provide an international payment system based on a relatively stable unit of account. Libra is based on a guarantee mechanism by a reserve whose management is ensured by a dedicated organization.

Assets

The project includes two crypto-assets[9]:

- **Libra**, a payment token with a stable value based on a panel of assets
- **Libra Investment Token** (LIT), an investment token entitling voting rights as well as a part of the interests of the panel of assets

Libra Reserve

A set of assets, "Libra Reserve" is intended to guarantee the value of the Libra. It will consist of bank deposits and treasury bills in different currencies[10]. The value of the currency will, therefore, be indexed to the value of the asset pool and guaranteed by the reserve.

On the valuation of the Libra, it is announced that inflation will be "low" although entirely dependent on the panel of assets. This currency panel concept for determining the value of a global asset is not

[8] "As for the [games] horses, [...] whoever thought he could divert them into advantage and private profit will be sentenced to the payment of a pound of gold which will benefit our Generosity because it is an official loss".

[9] See Glossary

[10] Announcement material has some slight variations in vocabulary. E.g. *bank deposits and short-term government securities* [Libra White Paper], *bank deposits and treasuries from high-quality central banks* [Libra Blockchain]

unlike ECU in Europe[11] or IMF's Special Drawing Right (SDR)[12], with the notable difference that the IMF does not guarantee this asset[13].

1 ≋ ⇔ 1 ●

The reserve will be managed with capital preservation and liquidity as priorities. Profits will be partly allocated to the development of the project and to pay the investors (with LIT). A set of "geographically distributed" custodians will hold the funds operationally.

To estimate the volume of this reserve, we can try an estimation of the size of the markets considered[14] : users of Mobile Money and more generally the people underserved by the traditional banking services. In 2018, there are 133 million Mobile Money accounts globally[15]. Users send transactions averaging $188 per month and hold $10 in their account[16]. With a comparable number of Libra users, that would represent a billion dollars in deposits. If every Facebook user did so, it would represent $24 billion.

If you look at people underserved by banking services in developed countries, the scale shifts[17]. In the United States alone, where Facebook covers nearly 80% of the population, there are 47 million people with limited access to these services[18]. If we take into account the average deposit of the most disadvantaged populations, $2018[19], that would correspond to an outstanding of $100 billion. By way of comparison, the outstanding amount of debt securities by central governments is $22 068 billion [20] and the European public debt represents €12 715 billion[21]. The scale is small enough for the project to be feasible but large enough to be considered as a systematic risk.

The management of this reserve will present several challenges:

- Macroeconomic and geopolitical effects of the reserve, especially on the treasury bonds' market
- Low yields of the treasury bonds in stable countries, even negative,
- Relative illiquidity of the reserve and therefore risks of an event of a mass exit
- Physical, organizational and legal management of the distributed fund
- Control of the convertibility between this currency and national currencies in the event of a crisis

Similar models

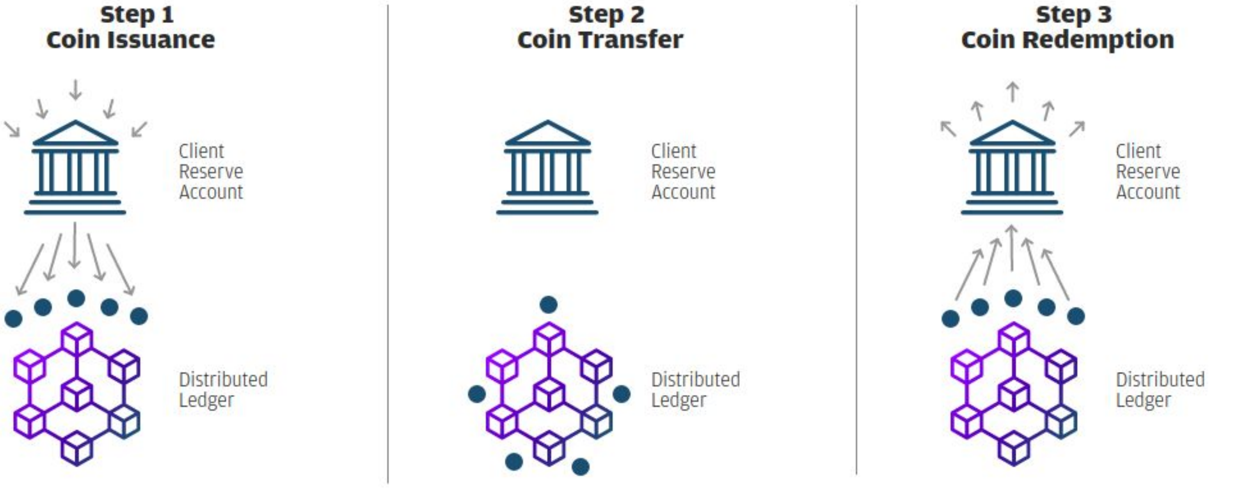
This model is similar to current projects of cryptoassets representing a reserve:

- JPM Coin by JPMorgan Chase, cryptoasset representing a dollar account of an institutional client at the bank. It can be traded during financial operations
- Utility Settlement Coin, an initiative of a consortium in order to facilitate settlement

[11] Council Regulation (EEC) No 3180/78 of 18 December 1978 changing the value of the unit of account used by the European Monetary Cooperation Fund
[12] Kaminska, Izabella et Smith, Colby, What exactly is Facebook's Libra reserve, Financial Times, 18 June 2019
[13] IMF Factsheet SDR:
https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/14/51/Special-Drawing-Right-SDR
[14] See. infra Potential Markets
[15] GSMA, State of the Industry: Report on Mobile Money 2018
[16] World Bank, Global Findex 2014
[17] World Bank, Global Findex, 2017
[18] Federal Reserve, Report on the Economic Well-Being of US Households in 2017, May 2018
[19] Annual income inferior to $25 000, Federal Reserve Survey of Consumer Finances, 2016
[20] Bank of International Settlements, Debt securities statistics, Q4 2018
[21] Eurostat, Transmission of deficit and debt data for 2018 - 1st notification, April 2019

- Central Bank Digital Currencies[22] (CBDC[23]), that can be represented using a cryptoasset[24]

In all three cases, there is a consensus about the concept, but these projects are still at prototypes or preliminary studies stage. Issues analyzed include openness (the unit is generally accessible only to a category of partners), security, and degree of anonymity of the technology.



Presentation of the JPM Coin model (Source: JPMorgan)

"Stable coins" have a similar objective, a cryptoasset with a relatively stable value compared to an identified national currency. However, there are several models to achieve this goal. The first category is based on a similar principle of a financial reserve. The Gemini dollar (GUSD)[25] by Gemini[26] (former partners of Mark Zuckerberg[27]), the USDC initiated by Coinbase (founding member of Libra) and Circle (one of the first players to obtain a BitLicence[28]) and Tether. The other categories of stable coins are based on a physical reserve (e.g. Digix Gold Tokens based on a gold reserve), another cryptoasset (e.g. DAI based on the Ether), or an algorithmic emission control model (Basis, closed project).

Libra Investment Token

The Libra Investment Token is initially associated with participating to the Libra Association as a founding member. Using the concept of "Security Tokens", it is a cryptoasset that represents voting rights and dividends on the project. Dividends stem from potential yield of the reserve. It is suggested that the asset could be made available to other investors. It is conceivable that the next phase of the project is financed by a public offer of this token (STO[29]).

[22] IMF, Fintech: The experience so far, June 2019
[23] Central Bank Digital Currencies CBDC ou Central Bank CryptoCurrencies, CBCC
[24] Bank of International Settlements, Central bank digital currencies, March 2018
[25] New York State, Department of Financial Service, New Currency Product Approvals, September 2018
[26] The initial trial ended with a settlement in 2008, challenged but dismissed on appeal
[27] Another Zodiac sign too...
[28] New York State, Department of Financial Services, Press Release, 2015
[29] Security Token Offering

Besides, the technical white paper envisages coding the governance of the association using a dedicated module[30] on the network. Holders of LIT tokens will then be able to participate directly in decisions via a smart contract (or possibly all Libra holders[31]). This is the model of Decentralized Autonomous Organization (DAO) sought by several current projects[32].

Since functioning, composition, and formalization of the Association have not yet been decided, the announcement of the Libra Investment Token and digitized governance must be seen as a mere intention.

Organization

Libra Association

The Libra Association is presented as a Swiss non-profit organization. Being a founding member of the Association also consists in maintaining necessarily a validating node and having a representative member on the Council of the association.

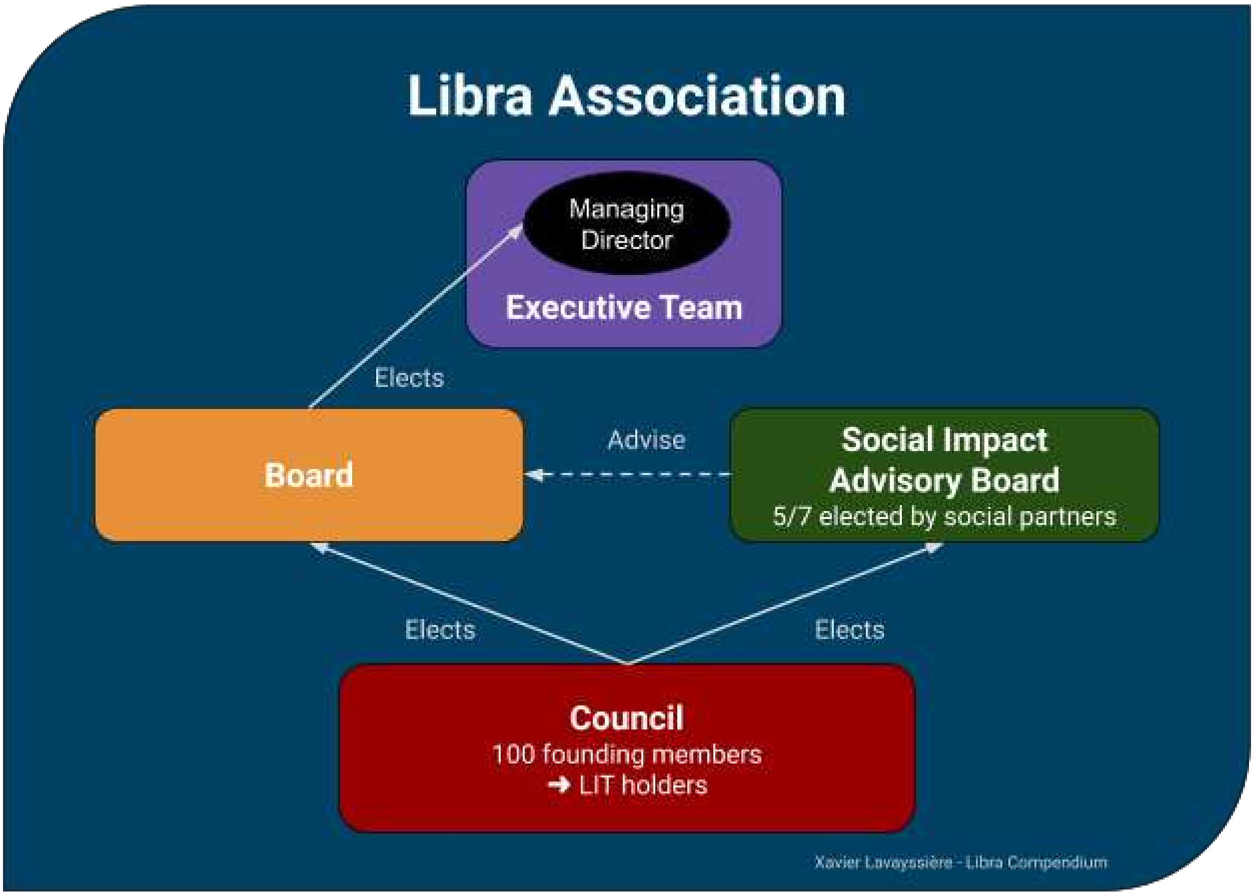
The main objectives of the Libra Association are:

- Overall governance
- Management of the reserve
- Supervision of technical development

The association is still in the process to be formalized. It does not have a Managing Director yet[33]. A first company, Libra Networks was registered on May 2nd[34] with 100 shares, probably planned for 100 companies, but with Facebook as a single partner[35]. On June 18th, the date of the announcement, the Libra brand was deposited in Switzerland by Libra Association[36] just moments from the filing by Facebook[37] of Calibra's brand[38].

Three governing bodies are currently planned: the *Libra Association Council* intended to validate essential decisions, including management of the reserve, the *Libra Association Board* and the *Social Impact Advisory Board (SIAB)*, representing social impact partners (SIP).

[30] See Glossary
[31] "Thus, the governance of the entire Libra ecosystem evolves as the validator set changes from the initial set of Founding Members to a set based on proof of stake."
[32] For instance on Ethereum: Colony, Aragon and DAOstack
[33] see infra Teams
[34] Notarial articles of the Association, april 12, 2019
[35] Registre du commerce of Geneva No réf. 08398/2019
[36] Request n° 08192/2019 june 18, 2019, IGE/IPE
[37] Via JLV, LLC, owner of "Libra" brand (USPTO n°88015297)
[38] Request n° 08193/2019 june 18, 2019, IGE/IPE



The *Council* is the fundamental body. Initially, it will consist of the 100 founding members with a planned transition to the LIT token holders, with a power proportional to assets held.

Among the responsibilities of the *Council:*

- Elect members of the *Board*
- Validation of the emissions of Libra, in proportion to the reserve
- Propose recommendations of modifications of the protocol ("Hard Forks")
- Authorization of the new intermediaries (see below)
- Validation of the new members of the association and their revocation
- Changes in the proportions of assets constituting the reserve basket
- Managing the technical development of the project

Founding members

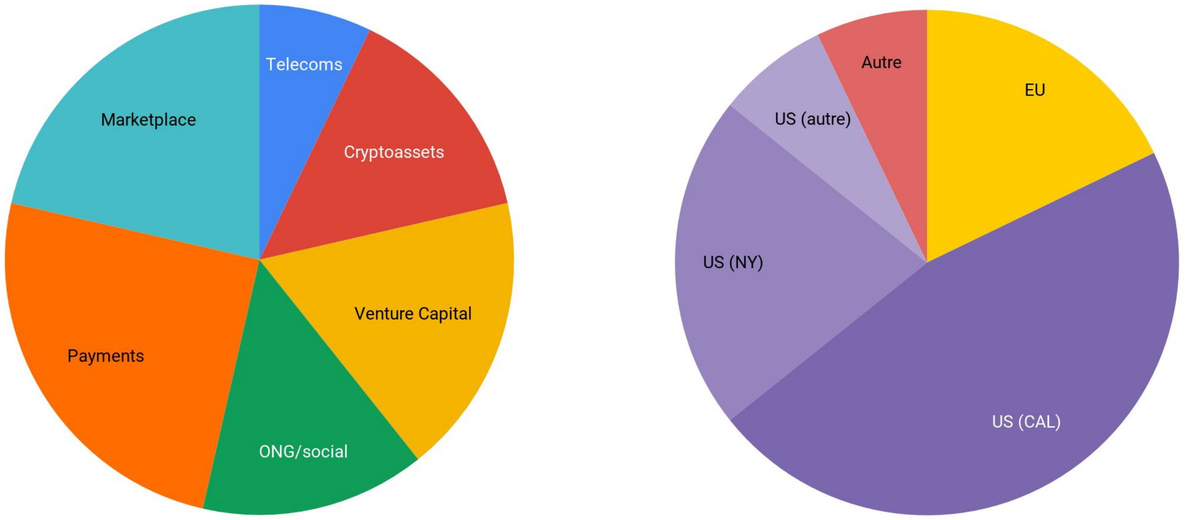
Among the founding members, we note five payment solutions, Mastercard, PayPal, PayU (Nasper), Stripe and Visa, marketplaces, Venture Capital firms, including Andreessen Horowitz, telecommunications companies, NGOs and actors in the cryptoasset industry: Coinbase, an exchange, Anchorage, a cryptoasset custodian, Xapo, a mobile custodial wallet[39] and Bison Trails, a blockchain infrastructure provider[40].

[39] *See Glossary wallet*

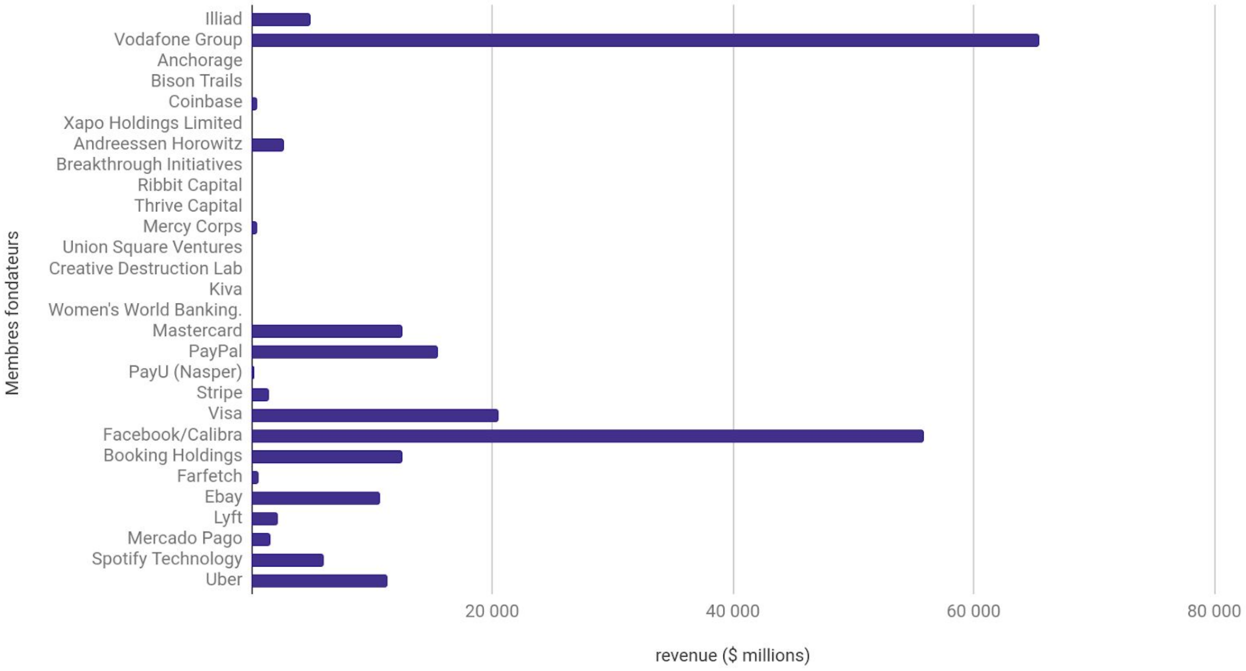
[40] https://overcast.fm/+Lb3AhXnLw podcast 21June 2019

Those profiles allow inducing elements of strategy: a payment solution intended for various marketplaces, access to which is managed by intermediaries, mainly on smartphones. We note the significant absence of banks and complementary financial services[41], Asian[42], and African players. Three-quarters of the founding members are based in the United States.

For the moment, governance mechanisms and profile of founding members do not seem able to guarantee the long-term missions of the organization.



Founding members announced on 18 June 2019 by industry (left) and headquarters (right). See Annex I



Revenue of founding members compared. Source: Financial Reports

[41] Leading players might have declined the offer (Goldman Sachs, JPMorgan Chase & Fidelity) N. Popper, Regulators Have Doubts About Facebook Cryptocurrency. So Do Its Partners, New York Times 25 June 2019 Albeit contested: Financial Times, Banks steer clear of Facebook's Libra project, 8 july 2019

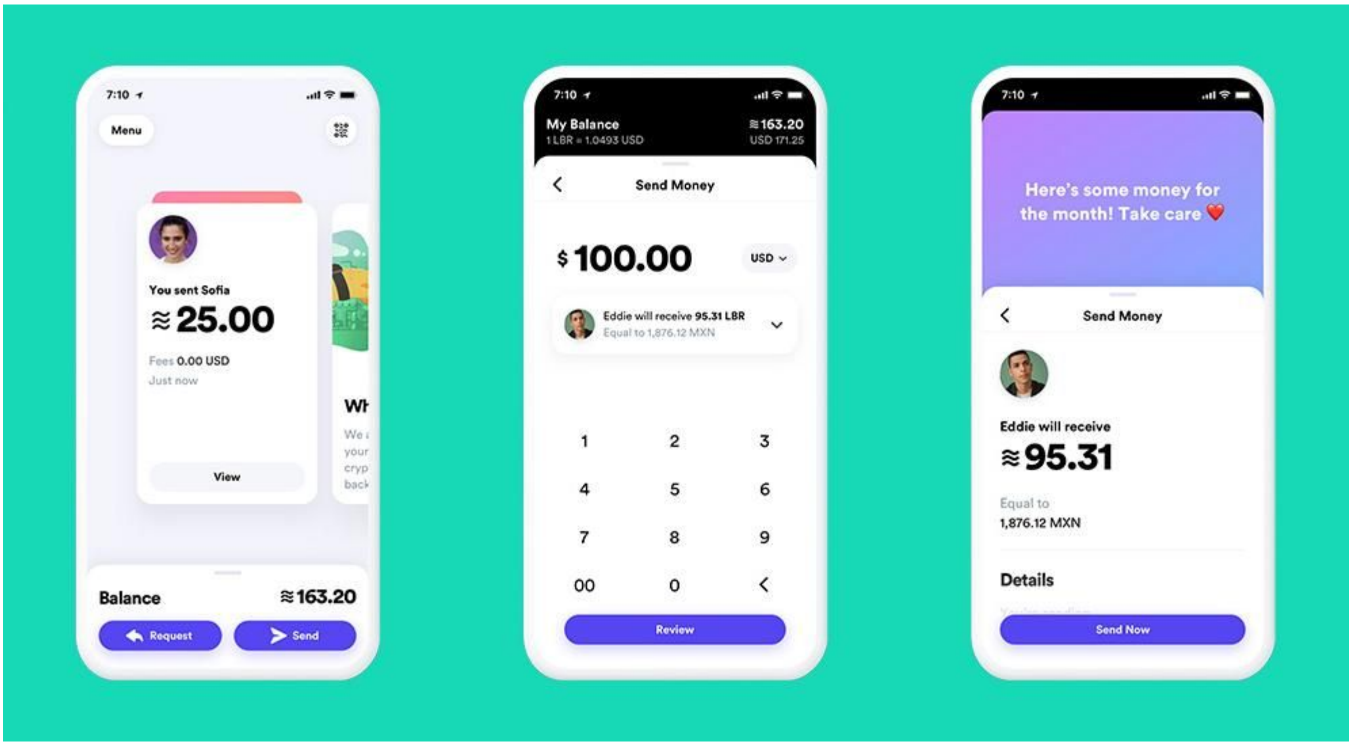
[42] Xapo is registered in Hong Kong and in Zug, Switzerland, but most investors and the board are US based. Pay U has significant activity in India

To become a founding member, a series of objective criteria has been published[43]. First, a member must be able to manage a validating node[44]. Then, a set of "reliability" criteria differentiating by type of institution:

- For a company, two of the three criteria: more than $ 1 billion in market value, 20 million consumers and recognized as one of the top 100 market players
- For crypto-centric investors, more than $ 1 billion in assets managed
- For blockchain companies, more than a year of operations, a high level of security and 100 million in assets managed on behalf of users.
- For charitable actors, alignment on the subject including financial inclusions for more than five years, credibility or breadth of operation.
- For academic institutions, among the top 100 universities globally or in Computer Science

Intermediaries

Intermediaries can exchange local currencies for libras. To become an intermediary one must receive the approval of the council of the Libra Association. It is planned that various actors will become so, in particular exchanges or suppliers of wallets. At first, only the 100 founding members will be able to convert currencies into libras and vice versa[45]. Among the first founders that could be intermediaries alongside Calibra there is Coinbase, one of the leading trading platforms in the US with a wallet, Xapo, which already provides such custodial wallet solution, Paypal that has already included cryptocurrency payments before and Mercado Libre, which solution Mercado Pago already offers various payment solutions at scale.



You sent Sofia
≈25.00
Fees 0.00 USD
Just now

Balance ≈163.20

My Balance ≈163.20
1 LBR = 1.0493 USD USD 171.25

Send Money
$100.00 USD
Eddie will receive 95.31 LBR
Equal to 1,876.12 MXN

Here's some money for the month! Take care ❤

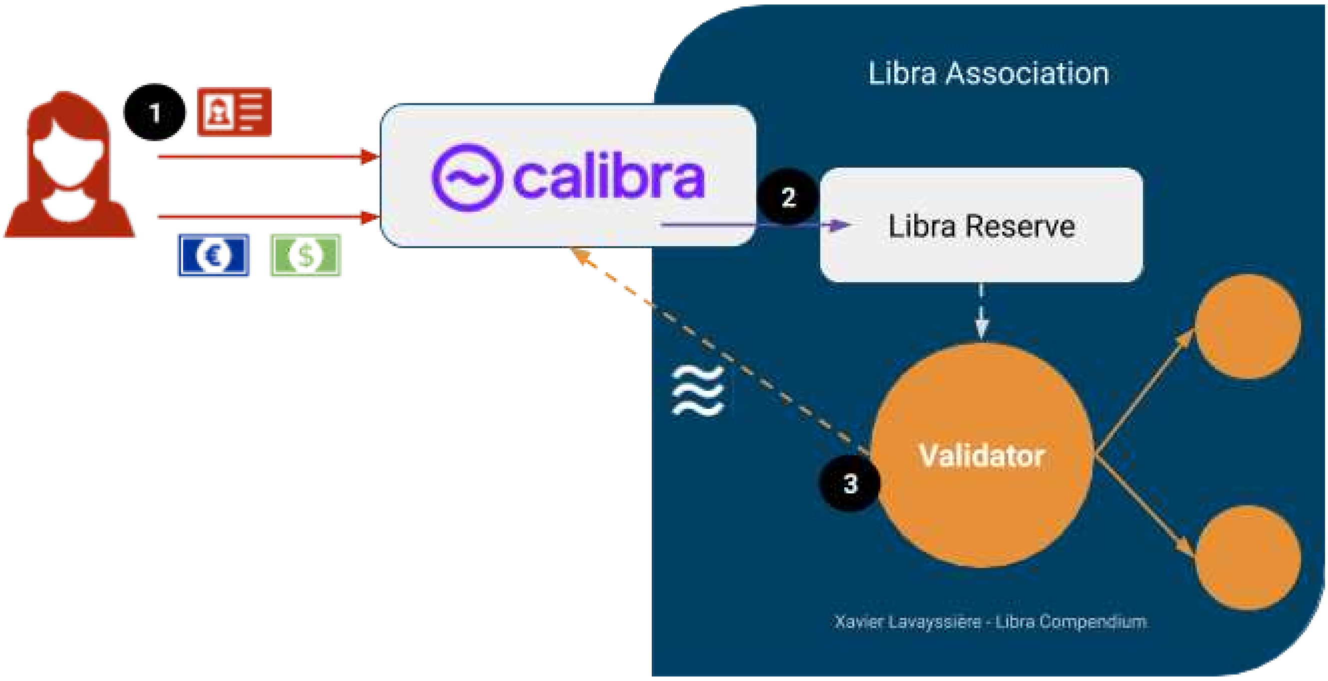
Send Money
Eddie will receive
≈95.31
Equal to
1,876.12 MXN
Details

Indeed, Facebook intends to position itself strongly on this segment. The subsidiary Calibra was registered on January 24, 2018[46] and entrusted to David Marcus, former president of Paypal and

[43] https://libracompendium.com/documents/HowtoBecomeaFoundingMember_en_US.pdf
[44] See infra Scalability
[45] Message of Carlos Maslaton, head of Xapo treasury, 18 June 2019
[46] Register of Delaware n° 7251336

responsible messaging products at Facebook. The solution is a *Custodial Wallet,* that is to say, a wallet of cryptoassets whose private keys are controlled by the company on behalf of its users. This type of service facilitates user experience and avoids losses. However, the company bears most of the operational risk and it has significant regulatory consequences (see below regulatory challenges).

Via a dedicated application or an interface in Messenger and Whatsapp, Calibra will allow users to register with an official ID or through a social network identity. Then, users will be able to transfer euros or dollars to obtain libras. The application will maintain the account and allow them to exchange it. Each exchange can be done within Calibra or by sending a transaction on the network via a validator.



Intermediaries role:

1. *A user provides his identity (national or social) and funds.*
2. *Funds are deposited in the Libra Reserve and indirectly command the issuance of libras*
3. *Validator nodes measure the outstanding libras and are queried by intermediaries*

Eodem cubito, eadem trutina, pari libra.[47]

European proverb

Technical

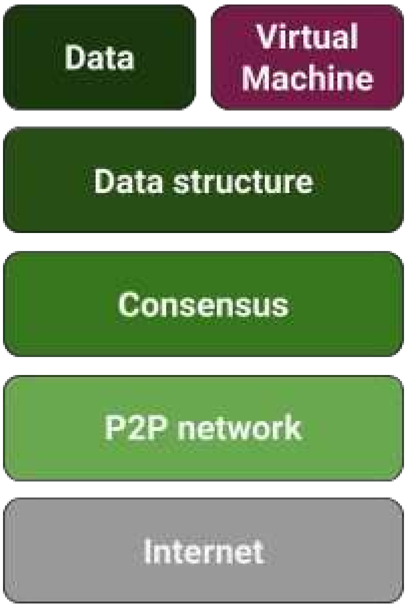
For the technical design of Libra, its authors drew from existing systems, projects and academic research ideas. Concepts will be familiar but also weaknesses, such anonymity and the ability to handle a large number of transactions. The system seems technically realistic. The published code is, however, a proof of concept for the moment.

Design

Fundamental Protocols

Distributed systems, including blockchains, rely on a stack of protocol layers. Each layer provides functionalities to the upper layers. The primary layer, for example, is the internet that allows communication between computers. The highest layer corresponds to the representation of accounts and cryptoassets.

The peer-to-peer network layer[48] provides functionalities on top of the internet to discover other nodes[49] and interact within the network. Libra is using a variant of libP2P[50] that has been suggested for other projects too.

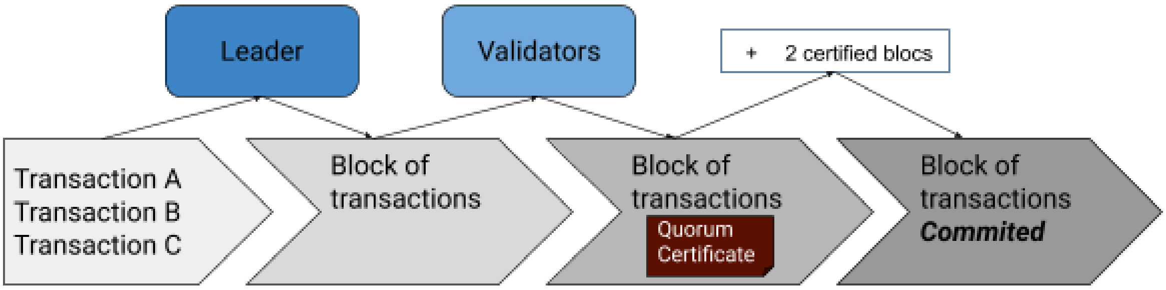


[47] You will be judged with the same measure you judge, E. Strauss, Dictionary of European Proverbs, 1994
[48] See Glossary
[49] See Glossary
[50] Library initially developed for IPFS https://libp2p.io/

Consensus

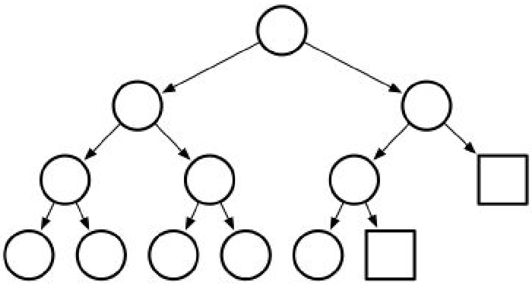
For consensus, a variant of practical Byzantine Fault Tolerant, a classic consensus algorithm[51] has been chosen[52]. These algorithms are based on the regular election of a *leader* that will suggest sets for transactions for validation and wait for majority approval from other validators. Sets of transactions are organized as "blocks". Once a sufficient quorum of validators signs a block, it is certified with the edition of a *Quorum Certificate*. Once two successor blocks are certified, the block is *committed* and considered final.

Timeouts ensure the liveness of the protocol to avoid stall situations. The whitepaper estimates that finality will be achieved in 10 seconds. The team relied on the "HotStuff" academic proposal[53] to improve the original algorithm in a distributed ledger contexts, with slight variations[54]. It is envisaged that this model could be modified later[55].



Timeline of the validation process. The leader creates blocks of transactions voted by other validators.

On Bitcoin and Ethereum, the fundamental data structure is a blockchain, a set of successive blocks with each a reference to the previous one. Here, Libra relies on a Merkle tree (See Glossary) structure of transactions. While this not a blockchain literally, like many projects in this area[56], fundamental properties such as integrity of the history are similarly guaranteed.



Merkle tree structure used in Libra as ledger history[57]

[51] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance." OSDI. Vol. 99. 1999.
[52] State Machine Replication in the Libra Blockchain, https://libracompendium.com/documents/libraBlockchainConsensus.pdf
[53] Yin, Maofan, et al. "HotStuff: BFT Consensus in the Lens of Blockchain.", 2018
[54] Abraham, Ittai, What is the difference between PBFT, Tendermint, SBFT and HotStuff ?, June 2019
[55] Christian Catalini, Ravi Jagadeesan, Scott Duke Kominers, Market Design for a Blockchain-Based Financial System, June 2019
[56] Xavier Lavayssière, L'émergence d'un ordre numérique, AJ Contrats, July 2019
[57] Source : "The Libra Blockchain" https://libracompendium.com/documents/the-libra-blockchain.pdf

	Libra	Ethereum	Cosmos	Quorum	Bitcoin
Native Cryptoasset	Libra	Ether	Atom	JPM Coin[58]	Bitcoin
User-defined Cryptoassets	Considered	Possible (ERC20, 721…)	Possible (user modules)	Theoretically possible[59]	Possible (colored coins)
Clients	Libra Core (Rust)	Geth (Go) Parity (Rust) Pantheon (Java)	Tendermint Core (Go)	Quorum (Geth Variant)	Bitcoin Core (C++)
Consensus	LibraBFT (HotStuff Variant)	- Proof Of Work - Clique - Aura	- Tendermint - Customizable	- Raft - Istanbul pBFT - Clique	Proof of Work
Usage	Main private network, potentially open	- Open public network - Side networks - Private networks	- Open public network - Side networks - Private networks	- Main private network - Private networks	- Open public network
Smart contracts language	Move	Solidity and Vyper	Various (mainly Go)	Solidity and Vyper	Bitcoin Script

Comparison of technical design choices with current main blockchain projects[60]

Smart contracts

On top of those mechanisms, we find a virtual machine able to execute code and data storage. Smart contracts are called *modules* and data fields *resources*. Each *resource* is a field, for instance, a balance, tied to an account and a module. The cryptocurrency Libra itself is implemented as a module that determines its functions of transfer, creation, and destruction of units of account. At first, developers will not be able to add new modules. The white paper announces that the programming language of these smart contracts *move*[61] will offer advanced features.

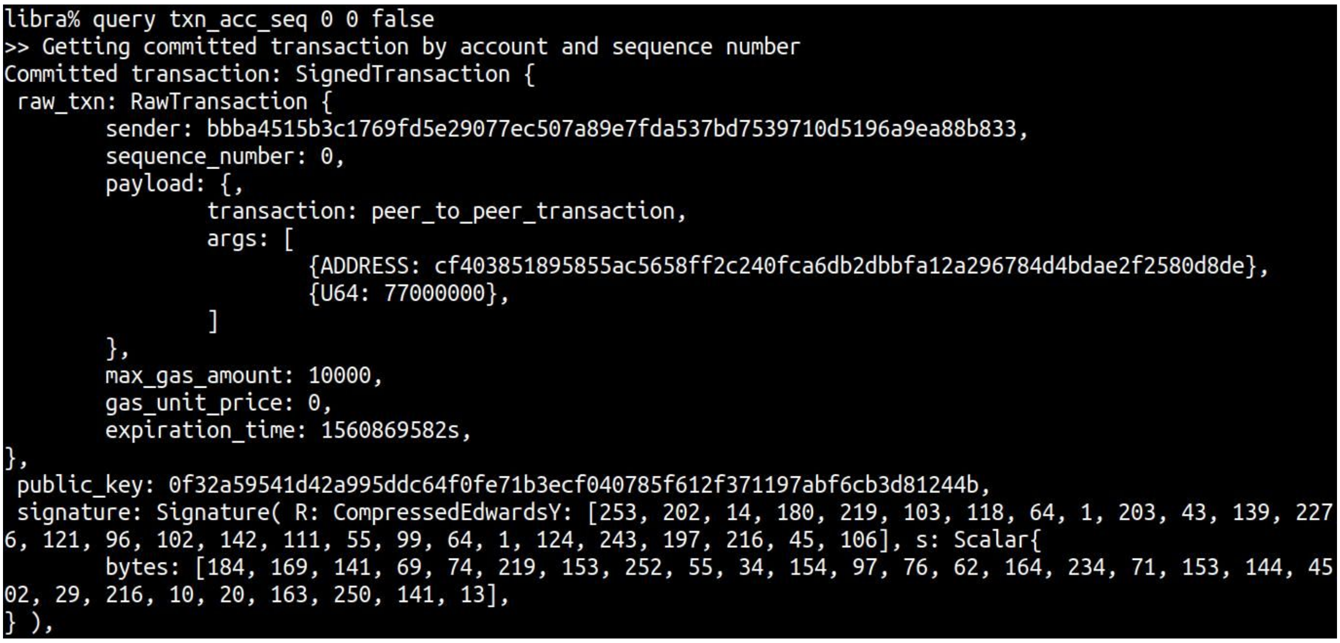
On the security side, as a module's code is immutable, as in Ethereum smart contracts, the white paper envisages the design of a reliable update mechanism. The programming language is presented as designed to avoid programming errors. However, creating a virtual machine and its language that are accessible for developers and secure is not trivial.

[58] Only on the network deployed by JPMorgan. Anybody can use the code to deploy a private network
[59] Theoretically Ethereum smart contracts are possible, but it is not applicable as the network is private
[60] Colors as a visual aid to identify similarities
[61] See Glossary

Implementation

Libra Core, the first implementation of a node is already available[62]. The Rust programming language[63] has been chosen, a relatively new language designed by Mozilla with security and performance in mind.

It is already possible to easily compile the client part in order to interact with one of the nodes of the testnet. It is also possible to compile and configure a node. We find the concept of addresses[64] associated with each user. Users sign each transaction using their private key, kept locally. Then the transaction is sent to a validator node. Transaction execution costs fees[65] that are paid in libras.

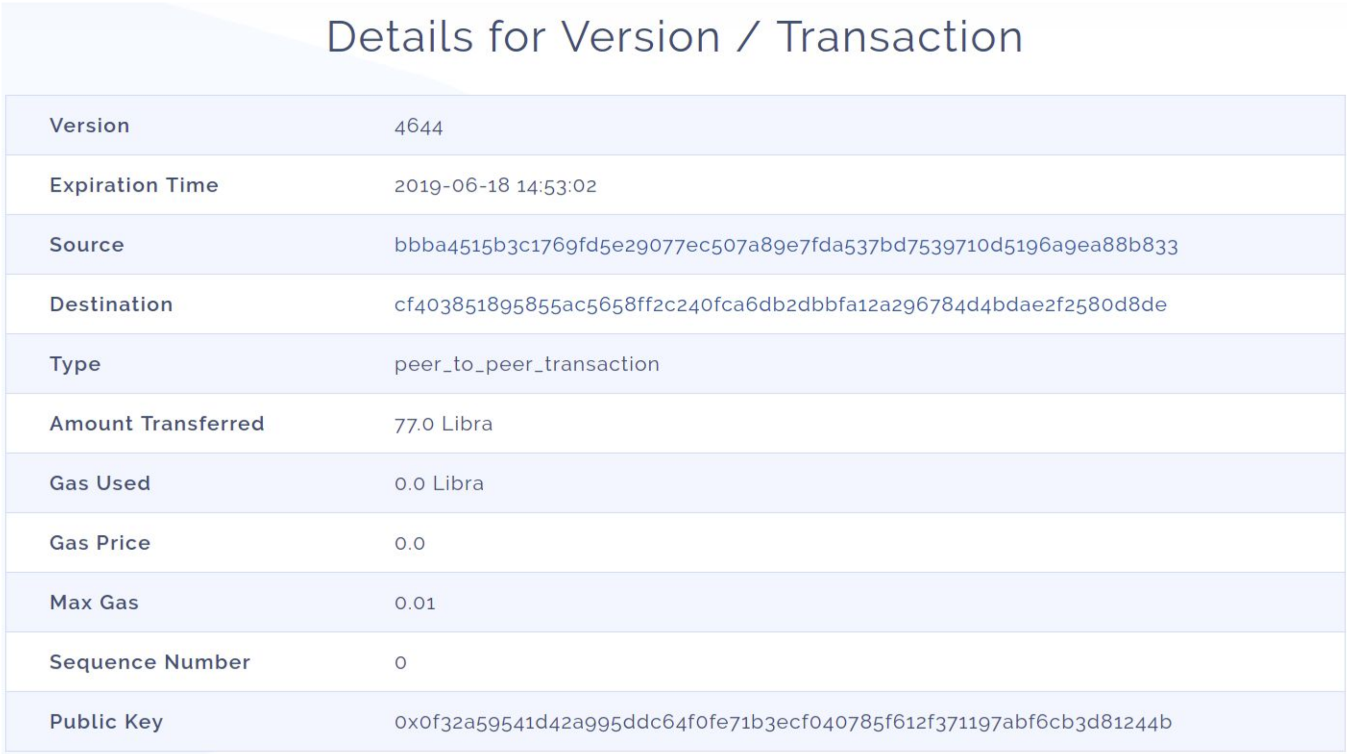


```
libra% query txn_acc_seq 0 0 false
>> Getting committed transaction by account and sequence number
Committed transaction: SignedTransaction {
 raw_txn: RawTransaction {
        sender: bbba4515b3c1769fd5e29077ec507a89e7fda537bd7539710d5196a9ea88b833,
        sequence_number: 0,
        payload: {,
                transaction: peer_to_peer_transaction,
                args: [
                        {ADDRESS: cf403851895855ac5658ff2c240fca6db2dbbfa12a296784d4bdae2f2580d8de},
                        {U64: 77000000},
                ]
        },
        max_gas_amount: 10000,
        gas_unit_price: 0,
        expiration_time: 1560869582s,
},
 public_key: 0f32a59541d42a995ddc64f0fe71b3ecf040785f612f371197abf6cb3d81244b,
 signature: Signature( R: CompressedEdwardsY: [253, 202, 14, 180, 219, 103, 118, 64, 1, 203, 43, 139, 227
6, 121, 96, 102, 142, 111, 55, 99, 64, 1, 124, 243, 197, 216, 45, 106], s: Scalar{
        bytes: [184, 169, 141, 69, 74, 219, 153, 252, 55, 34, 154, 97, 76, 62, 164, 234, 71, 153, 144, 45
02, 29, 216, 10, 20, 163, 250, 141, 13],
} ),
```

Example of a transaction of 77 Libra account bbba45 ... account cf40 ...[66]

[62] https://github.com/libra/libra
[63] Comment of Ben Maurer, 18 June 2019
[64] As for Bitcoin the address is the hash of the public key (see glossary)
[65] As for Ethereum, gas is an intermediary concept to represent the complexity of a transaction. Fees are equal to the number of gas units multiplied by an unit's price. The price of an unit of gas is fixed by validators https://community.libra.org/t/calculating-libra-transaction-fee/785
[66] June 18, 2019, https://twitter.com/XavierLava/status/1140999140324904961

As on Bitcoin and Ethereum transactions can be visualized on a public explorer[67]:



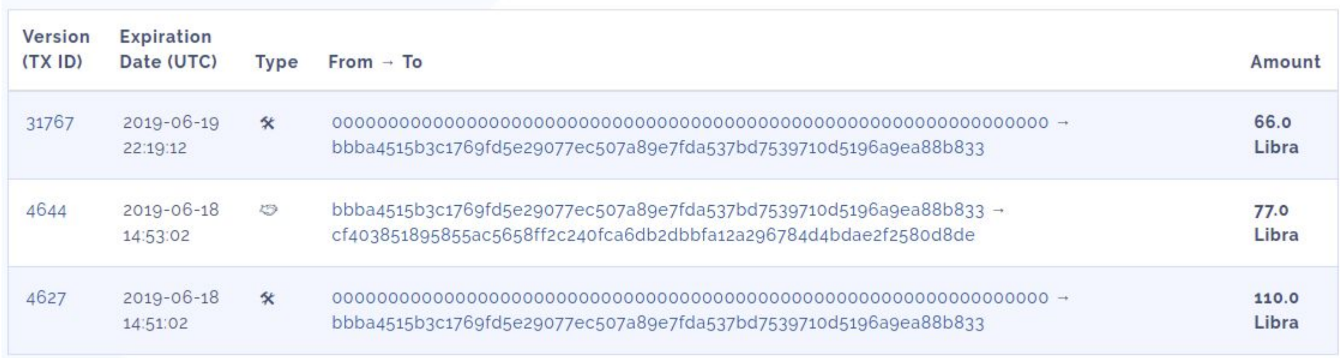
Details for Version / Transaction

Version	4644
Expiration Time	2019-06-18 14:53:02
Source	bbba4515b3c1769fd5e29077ec507a89e7fda537bd7539710d5196a9ea88b833
Destination	cf403851895855ac5658ff2c240fca6db2dbbfa12a296784d4bdae2f2580d8de
Type	peer_to_peer_transaction
Amount Transferred	77.0 Libra
Gas Used	0.0 Libra
Gas Price	0.0
Max Gas	0.01
Sequence Number	0
Public Key	0x0f32a59541d42a995ddc64f0fe71b3ecf040785f612f371197abf6cb3d81244b

Technical Challenges

Anonymity

Transactions are public and can be accessed via a node. A third party can identify the sending address, receiving address, time, date, and amount of each transaction. The history of all transactions tied to an address is also visible publicly.



Version (TX ID)	Expiration Date (UTC)	Type	From → To	Amount
31767	2019-06-19 22:19:12	⚒	0000000000000000000000000000000000000000000000000000000000000000 → bbba4515b3c1769fd5e29077ec507a89e7fda537bd7539710d5196a9ea88b833	66.0 Libra
4644	2019-06-18 14:53:02	🤝	bbba4515b3c1769fd5e29077ec507a89e7fda537bd7539710d5196a9ea88b833 → cf403851895855ac5658ff2c240fca6db2dbbfa12a296784d4bdae2f2580d8de	77.0 Libra
4627	2019-06-18 14:51:02	⚒	0000000000000000000000000000000000000000000000000000000000000000 → bbba4515b3c1769fd5e29077ec507a89e7fda537bd7539710d5196a9ea88b833	110.0 Libra

Visualization of the account history bbba45 ... used for the transaction above

Since the exchanges can associate their users to their address on the network, the *Custodial Wallet* Calibra will be able to follow the entire use of funds purchased or used through their intermediary. On Bitcoin, 90% of transactions come directly from exchanges[68], which immediately identify the user

[67] https://librabrowser.io/version/4644
[68] Data Chainalysis

associated with the address. Additional identification is possible currently on public blockchains via the clustering of related addresses and patterns.

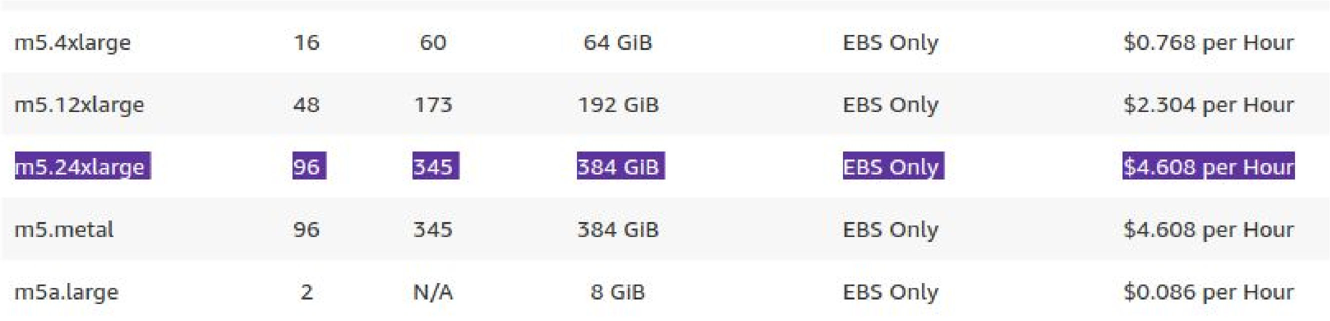
It should be noted that most blockchain projects are now actively working on solutions to improve anonymity relying on various techniques.The lack of any mention in the technical documents must be understood as a deliberate choice. The head of the technical team mentions that it would be possible to add these functionalities later, notably via modules in *move*[69].

Scalability

While any significant IT project needs to anticipate the effects of an increasing number of users on hardware and software operation, the problem is doubly accentuated here. On the one hand, as the objective is to obtain a consensus of a majority of the nodes of the network while maintaining a certain speed and regularity, the volume of information validated is necessarily constrained. On the other hand, the potential scale of the operation is out of proportion with most current payment systems, let alone blockchains.

The white paper envisions a network capable of supporting 1,000 transactions per second with a final confirmation in 10 seconds. Compared to current payment services, this seems limited. Visa claims a capacity of 65,000 transactions per second on its visanet network[70]. In practice, 124.3 billion transactions were completed in 2018,[71] hence 4,000 per second. It seems that the strategy will be to use the blockchain only as a settlement layer[72]

Besides, to support these 1,000 transactions, several conditions on the hardware and the connection of validators must be realized. The technical white paper states that each validator must have a connection at 40 Mbps (40 million bits per second), 16 TB SSD, and a standard server CPU. The online documentation[73] evokes a dedicated connection of 100 Mbit / s with redundancy, a dedicated engineer, and a machine type m5.24xlarge (amazon reference).



m5.4xlarge	16	60	64 GiB	EBS Only	$0.768 per Hour
m5.12xlarge	48	173	192 GiB	EBS Only	$2.304 per Hour
m5.24xlarge	96	345	384 GiB	EBS Only	$4.608 per Hour
m5.metal	96	345	384 GiB	EBS Only	$4.608 per Hour
m5a.large	2	N/A	8 GiB	EBS Only	$0.086 per Hour

Price on demand for an instance m5.24xlarge on Amazon Web Services (June 2019)

On the one hand, such performance constraints are weaknesses of the network. On the other hand, necessary costs (in the range of $ 100,000 per year) and management overhead are far from negligible for some members of the Association ($1 million range, NGO, academia…)

[69] Commentary of Ben Maurer, technical head, 19 June 2019

[70] Visa Fact sheet

[71] Visa 2018 Annual Report

[72] Letter to the US Senate Banking Committee, 8 July 2019 https://libracompendium.com/documents/FB-Letter-to-Senate-Banking-Committee.pdf

[73] https://libra.org/en-US/becoming-founding-member/#technical_requirements 19 June 2019

Security

The project's security spans multiple levels and constraints[74]. The first level of safety relies on network design and consensus mechanisms. There are, for example, risks of network saturation, network partition, a stall in consensus... It seems that the functioning of the network initially depends on the availability and connectivity of validator nodes (see above) which are commonly challenging to guarantee.

At a higher level, programmability and network services capabilities might also offer weaknesses. In addition to the question of the design of the programming language *Move* that seems analyzed, the connection between user applications to the network might present weaknesses. Third party service providers that are not necessarily vouched by the association might be compromised.

Finally, online financial services are particularly subject to fraud[75] and manipulations. A security policy must not only take into account pure technical aspect but also the ability of users to identify to avoid mistakes, identity with whom they interact...

Libra announced a reward program for the detection of vulnerabilities (*Bug Bounty Program*)[76]. This program includes the concept of focus areas on specific topics with more substantial rewards, an objective to have complete documentation, coordination with internal developers, partnerships with academic institutions and a partnership with HackerOne, a company specialized on bounty programs. Details will be published later this year.

From these critical technical challenges, it emerges that Libra has been initially designed to primarily rely on trusted custodian wallets in order to provide an instant, private, and large-scale payment service.

[74] A common framework is the combination of confidentiality, integrity and availability : J. Saltzer, and M. Schroeder, "The protection of information in computer systems", Proceedings of the IEEE 63(9), 1975

[75] For instance front running, a fraud where an intermediary, knowing an upcoming order, places an order ahead

[76] https://libracompendium.com/documents/LibraBugBountyProgram_en_US.pdf

East and alia species imaginariae solutionis, peres and libram;
quod and ipsum genus certis ex causis receptum is,
ueluti if quid eo nomine debeatur,
quod per aes and libram gestum sit, siue quid ex iudicati causa debeatur.[77]

Gaius, Institutes III, 161 A.D.

Main Regulatory Challenges

Details of the project have to be established for an in-depth legal analysis. The statutes of the core entities have not yet been filed[78]. But we can nevertheless identify the main legal challenges ahead, especially regarding intermediaries.

Privacy

The first question on confidentiality concerns the role of intermediaries and in particular Facebook. Calibra's Customer Commitment[79] announces that financial data will not be linked to social data or share with third parties "without customer consent". Additionally, this document lists cases where data may be shared in to suit needs "to keep people safe, comply with the law, and provide basic functionality". While Calibra was advertised as with "strong privacy commitments"[80], this commitment does not go further than existing legal obligations.

The second layer of complexity is added by using a distributed ledger. In Europe, the General Data Protection Regulation[81] (GDPR) requires in particular that the user may request the deletion of his personal data (Article 17). A financial transaction is a piece of personal information. It has already been established that pseudonymized data is not exempted[82] as long as the original information can be

[77] "There is another kind of imaginary payment which is effected by bronze and balance; but this is used only in certain cases; as, for instance, where something is due on the ground that there has been a transaction by bronze and balance, or for the reason that something is due on account of a judgment."
[78] See above, Libra Association
[79] Calibra, Customer Commitment, June 2018
[80] David Marcus, Twitter, https://twitter.com/davidmarcus/status/1140909519796441089
[81] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
[82] Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques WP216 (Brussels, 10 April 2014).

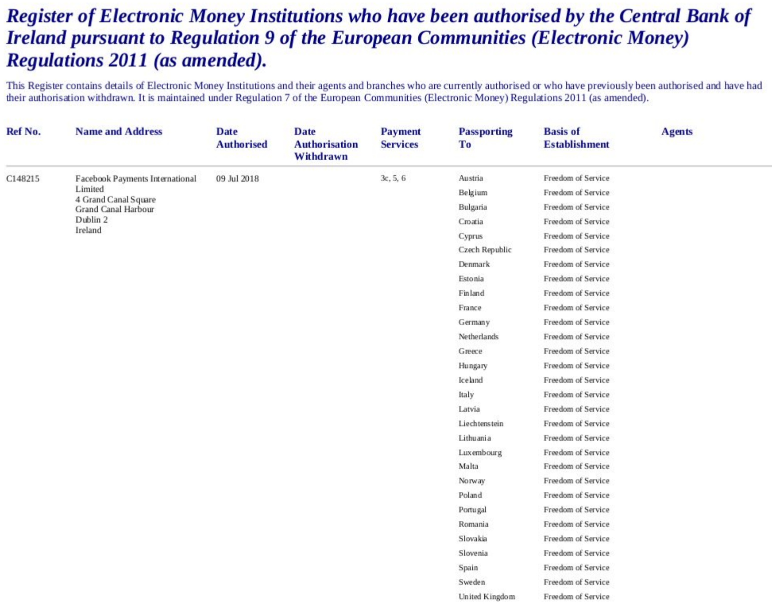
reconstituted[83]. On a related note, a recent decision of the CJEU considers that businesses using third party tracking solution is “jointly responsible”[84].

On these points, it seems that the instigators of Libra rely on Custodial Wallets by not registering most transactions on the blockchain[85]. Each intermediary will then individually bear the responsibility for this legislation. For transactions registered on the distributed ledger, it seems that unlike most public blockchains that are not associated with a legal entity, validators and the Libra Association will have to clarify their responsibilities.

Financial Regulation

Calibra announced that the company intends to comply with applicable financial regulations. For example, Calibra will not offer its services in countries where cryptocurrency is prohibited. Countries subject to sanctions by the United States will likely be also added to the list for Calibra. Moreover, as three-quarters of founding members are based in the U.S, the potential impact of those limitations on the overall project must be considered.

For several years Facebook has worked toward obtaining necessary licenses to be able to provide payment services. Facebook is licensed as a Money Transmitter in the fifty U.S States and Puerto-Rico[86]. In Europe, it has acquired the E-Money License in Ireland[87] and benefited from the European passport procedure[88] to extend this authorization to all Europeans States as well as Norway and Iceland.



Register of Electronic Money Institutions who have been authorised by the Central Bank of Ireland pursuant to Regulation 9 of the European Communities (Electronic Money) Regulations 2011 (as amended).

This Register contains details of Electronic Money Institutions and their agents and branches who are currently authorised or who have previously been authorised and have had their authorisation withdrawn. It is maintained under Regulation 7 of the European Communities (Electronic Money) Regulations 2011 (as amended).

Ref No.	Name and Address	Date Authorised	Date Authorisation Withdrawn	Payment Services	Passporting To	Basis of Establishment	Agents
C148215	Facebook Payments International Limited 4 Grand Canal Square Grand Canal Harbour Dublin 2 Ireland	09 Jul 2018		3c, 5, 6	Austria	Freedom of Service	
					Belgium	Freedom of Service	
					Bulgaria	Freedom of Service	
					Croatia	Freedom of Service	
					Cyprus	Freedom of Service	
					Czech Republic	Freedom of Service	
					Denmark	Freedom of Service	
					Estonia	Freedom of Service	
					Finland	Freedom of Service	
					France	Freedom of Service	
					Germany	Freedom of Service	
					Netherlands	Freedom of Service	
					Greece	Freedom of Service	
					Hungary	Freedom of Service	
					Iceland	Freedom of Service	
					Italy	Freedom of Service	
					Latvia	Freedom of Service	
					Liechtenstein	Freedom of Service	
					Lithuania	Freedom of Service	
					Luxembourg	Freedom of Service	
					Malta	Freedom of Service	
					Norway	Freedom of Service	
					Poland	Freedom of Service	
					Portugal	Freedom of Service	
					Romania	Freedom of Service	
					Slovakia	Freedom of Service	
					Slovenia	Freedom of Service	
					Spain	Freedom of Service	
					Sweden	Freedom of Service	
					United Kingdom	Freedom of Service	

Irish register of companies authorized by the central bank to carry out e-money activities and its extension[81]

Given the particular nature of the token, representing a fraction of a panel of assets, it is possible that additional regulations may be applicable, such as licenses to trade financial instruments. The sale of the Libra Investment Token, if it takes place, will also be subject to securities legislation. Moreover, financial companies are subject to stringent regulation in the United States[89] and Europe in terms of customer identification (KYC) and anti-money laundering (AML).

[83] CNIL, Blockchain, September 2018

[84]CJUE, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV (Case C-40/17), 2018

[85] Letter to the US Senate Banking Committee, 8 July 2019 https://libracompendium.com/documents/FB-Letter-to-Senate-Banking-Committee.pdf

[86] https://www.facebook.com/payments_terms/licenses

[87] Banque centrale d'Irlande, Register of Electronic Money Institutions

[88] https://acpr.banque-france.fr/autoriser/procedures-secteur-banque/passeports-europeens-banque

[89] Bank Secrecy Act, Securities Exchange Act...

Liability

For leading cryptocurrencies, there is a distinction between the different functions: developers contribute freely, minors validate transactions, users participate in the choice of valid blocks... Consequently, companies operating the most regulated activities, such as exchanges and the custodial wallets are solely responsible for this service.

Here, Facebook is the instigator of the network, a financial intermediary, and a custodian for a significant number of users. It is conceivable that the legal responsibility of the company is sought for the overall project. Nevertheless, it is more likely to take the form of political pressure.

Taxation

In the current state of the law, the purchase of services using libras would be subject to capital gains tax in most jurisdictions. Indeed, it will be necessary to identify for each transaction if the Libra has appreciated since the purchase of the units by the user. While amounts might be reasonable, especially as many countries have allowance regimes, accounting for these transactions could be problematic.

Among the solutions that seem to be emerging:

- A reporting tool, possibly integrated into the wallets
- A modification on the calculation rules and reporting below the thresholds
- A complete exemption considering the relatively stable nature of the unit

Legislative changes seem to be the favored option[90]. They will probably not be effective before 2021 as tax laws usually have a fixed timetable.

Competition law

The project consists of a global means of payment that will be controlled by a small number of large actors (see above, Founding Members). Depending on the success of the project, the accessibility conditions for new entrants or the competitive behavior of intermediaries, the situation may be fragile regarding competition law. Moreover, most founding members control one or several markets. For example, in early 2018, Facebook banned advertisements for public offers of cryptoassets (ICOs) and about cryptocurrencies[91], justified by the difficulty to distinguish fraud. At the announcement of Libra, suspicions of manipulation weighed, although formally denied [92].

[90] Chris Giles, Lawyers warn of Facebook's Libra tax risks in Europe, Financial Times 1 July 2019

[91] Leather, Rob, New Ads Policy: Improving Integrity and Security of Financial Products and Services, January 2018

[92] https://twitter.com/davidmarcus/status/1141409548235755520

You have a non-believer; I'm a Libra So I weigh the scales

Talib Kweli[93]

Elements of strategy

The core of this project is based on Facebook's interest to expand its services. The company is indeed in a dreary situation with public relations crises[94], a relatively stagnant user base in developed countries [95] and the development of regulation of platforms and personal data. A strategy specific to the Association is still being defined.

Announcements

Supports

Libra was announced on June 18, 2019, on social networks with the publication of two primary documents:

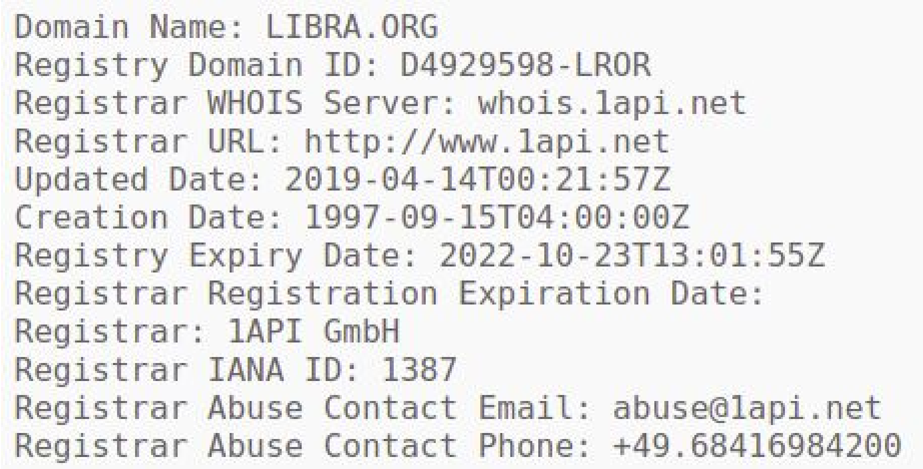
- "Libra White Paper" which presents the main elements of the project
- "The Libra Blockchain" which explains the technical design of the envisaged network

These two documents are very characteristic of ICO projects[96] since 2015, inspired by the Bitcoin white paper and financial prospectus regulations. Additionally, the website contains information including several detailed documents[97], Calibra's website with mirroring content and a Github repository[98] where we can already find the first implementation of a node and a client.

The announcement was originally published in 9 languages, which can give an indication of targeted markets: Indonesian, Simplified Continental Chinese (中文, 简体 中文), American English, French of France, German of Germany, Japanese, Brazilian Portuguese, Spanish of Latin America and Russian of Russia[99].

The domain name libra.org was previously a site dedicated to the astrological sign. It appears that the domain name was transferred on April 14, two months before the announcement. The principal preparation operations took place on May 15, 2019. The host of the main site is based in San Francisco [100]. The website for developers[101] and the forum[102] are hosted and managed independently.

[93] Reflection Eternals: Revolutions Per Minutes, So good
[94] Cambridge Analytica, role in the dissemination of hate speech in Myanmar …
[95] Facebook 2018 annual report https://libracompendium.com/documents/Facebook-2018-Annual-Report.pdf
[96] Initial Coin Offering: public sale of a cryptoasset (See glossary) in order to finance a project
[97] Move Programming Language, The Libra Reserve, Commitment to Compliance and Consumer Protection...
[98] https://github.com/libra/libra
[99] Using a best practice recommended by the IETF (relying on ISO-3166 and ISO-639 1 or 3) the website specifies the national declination of each language. Some languages do not seem to have well established variants.
[100] https://securitytrails.com/domain/libra.org/dns



```
Domain Name: LIBRA.ORG
Registry Domain ID: D4929598-LROR
Registrar WHOIS Server: whois.1api.net
Registrar URL: http://www.1api.net
Updated Date: 2019-04-14T00:21:57Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2022-10-23T13:01:55Z
Registrar Registration Expiration Date:
Registrar: 1API GmbH
Registrar IANA ID: 1387
Registrar Abuse Contact Email: abuse@1api.net
Registrar Abuse Contact Phone: +49.68416984200
```

Excerpt from the Whois information of libra.org domain name

While material released along with the announcement is evidence of a long preparatory work, we can note inconsistencies[103] or contradictions[104] of vocabulary. Presented objectives raise questions[105], the project seems to target migrant workers' remittances, US unbanked and mobile payments in developing countries.

It is interesting in this respect to draw a parallel with Internet.org[106], a Facebook initiative with six industrial partners (Samsung, Ericsson, MediaTek, Opera Software, Nokia and Qualcomm) to develop access to Internet. Presented as a humanitarian project, it has been the subject of controversy[107] or interdiction[108], suspected to offer a partial internet with detrimental consequences[109].

Repercussions

The announcement had two main effects. The first is media attention, especially in the specialized press on blockchains and cryptocurrencies. It is possible that one of the objectives was to sparkle interest of actors of this ecosystem.

The second consequence has been a quick response from politicians and regulators on the subject. Beyond systemic risks, security issues, and recent scandals of Facebook, the question of sovereignty is a central element. The Association had anticipated the topic by committing to "preserve and strengthen the capacity of governments to conduct monetary policy[110]. Examples of noteworthy reactions include:

- A cease and desist letter[111] and the convening of a US congressional hearing by the *Financial Services Committee* of the House of Representatives. The hearing will be held on July 17th. The *Banking Committee* Senate immediately scheduled a hearing on July 16[112]. Similarly, the

[101] https://developers.libra.org/ hosted as a github page
[102] https://community.libra.org/ Discourse forum
[103] For example *validators* are defined as *replicas* page 1 of the white paper and then distinguished page 14.
[104] The use of the expression "intrinsic value" while using a guaranty fund
[105] Greeley, Brendan, Facebook's Libra will not help the unbanked, Financial Times June 19, 2019
[106] https://info.internet.org/en/
[107] Steve Stecklow, Why Facebook is losing the war on hate speech in Myanmar, Reuters Investigate
[108] Rahul Bhatia, The inside story of Facebook's biggest setback, The Guardian, 12 May 2016
[109] Talbot, David "Facebook's Two Faces". Technology Review 2013
[110] https://libracompendium.com/documents/CommitmenttoComplianceandConsumerProtection.pdf
[111] US House of Representatives, Committee on Financial Services, Cease and desist Letter, July 2 2019, http://libracompendium.com/documents/Letter-Committee-Financial-Services.pdf
[112] US. Senate, Banking Committee, press release

chairman of the Duma's financial markets committee believes that the currency will be banned in Russia[113].

- The head of the People’s Bank of China’s Research bureau expressed concerns about th role this project could give to the US dollar[114].
- Requests for additional information from Bank of England Governor Mark Carney, US Federal Reserve Board Chairman Jerome H. Powell, Monetary Authority of Singapore Managing Director Ravi Menon, Financial Stability Board Chair Randal Quarles ...
- France’s Minister of Finance Bruno Le Maire reacted the same day, asking governors of the G7 for a report on risks for the consumer, in terms of money laundering, anticompetitive practices and in terms of sovereignty [115].

Potential markets

Mobile payments

The model for Facebook is that of WeChat[116], a messaging application that has become a leading payment player in China. There are equivalents in Japan with, for example, Line Pay and RatukenPay. Other messaging services have already gone through the creation of a cryptocurrency to take place in this market. Kik, a Canadian-based messaging application,[117] launched its 'Kin' cryptocurrency in 2017[118] Telegram, founded by brothers Nikolai and Pavel Durov, is conducting a public offering for its currency 'Gram' in several phases.

[113] TASS (News agency) 18 june 2019 https://tass.ru/ekonomika/6564301

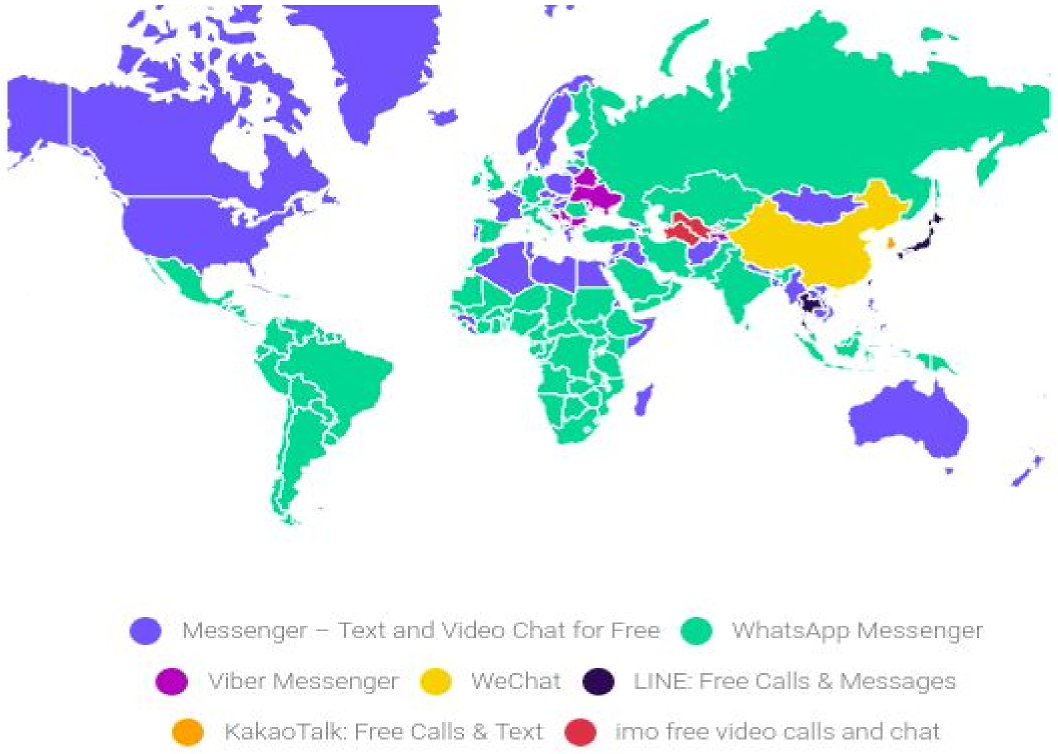
[114] South China Morning Post, Facebook’s Libra forcing China to step up plans for its own cryptocurrency, says central bank official, 8 July 2019 https://www.scmp.com/economy/china-economy/article/3017716/facebooks-libra-forcing-china-step-plans-its-own

[115] Bruno Le Maire, Speech at the National Assembly, June 18, 2019

[116] Ted Livingston, Facebook Is not Going After Bitcoin. It's Going After the Dollar, Medium

[117] Funded in 2015 by Tencent, the parent company of WeChat for $ 50 million
Reuters, China's Tencent invests $ 50 million in Canada's Kik Interactive,18 August 2015

[118] The latter nonetheless subject to prosecution by the US S.E.C. : US. SEC vs Kik Interactive, Case No. 19-cv-5244

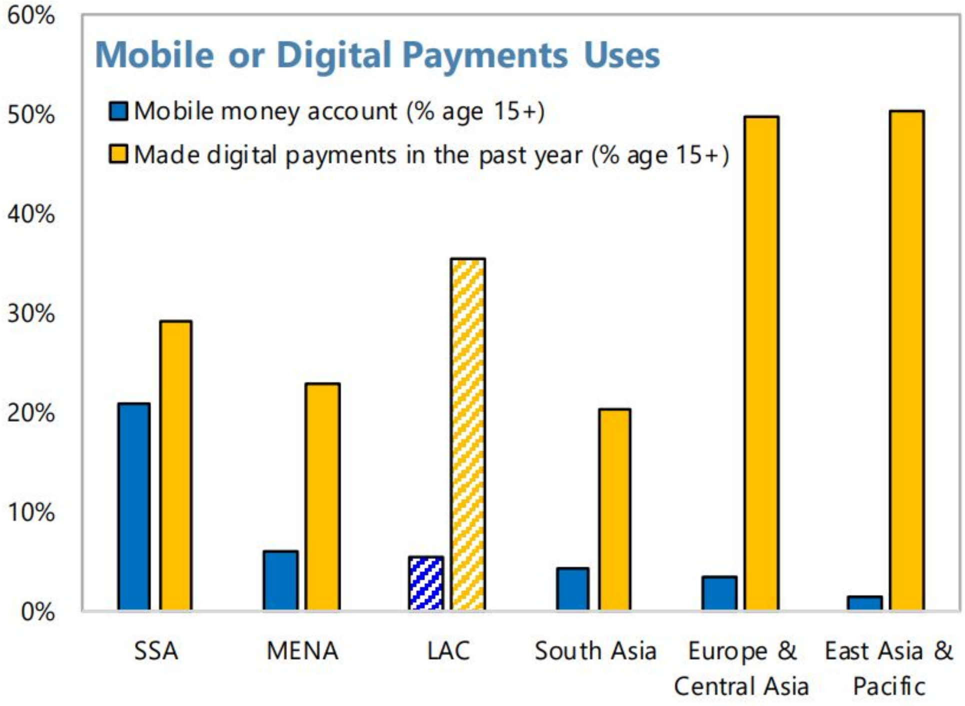

● Messenger – Text and Video Chat for Free
● WhatsApp Messenger
● Viber Messenger
● WeChat
● LINE: Free Calls & Messages
● KakaoTalk: Free Calls & Text
● imo free video calls and chat

Source, Similar Web data from the android store[119]

Digital payments markets are nevertheless competitive. Along with messaging apps, Apple, Google, and Samsung offer integrated solutions, combined with traditional players and new entrants. Finally, players like Lydia, Paylib, and Venmo[120] provide complementary solutions, especially for payments between individual users. Depending on the region, adoption, use cases, and the technology used (NFC[121] or QR code[122]) vary.

It is worth noting a particular case of this market, *Mobile Money,* which has experienced a boom in Sub-Saharan Africa in recent years[123]. These transfers are often based on more primitive technologies than internet data (SMS, USSD) and are operated by the telephone operators. The two founding members are already active in these markets. Vodafone participated in the launch of M-Pesa in 2007, which is regarded as a model for the industry. Tigo, the second operator in Senegal was bought in 2018 by a consortium including Xavier Niel, Iliad's founder[124].

[119] Liron Hakim Bobrov, Mobile Messaging App Map of the World, June 2019
[120] Venmo is a service of Paypal
[121] Near Field Communication: technology allowing contactless exchange of information
[122] Quick Response Code: Generated squared barcode that can be read by a camera
[123] IMF, Fintech : The experience so far, June 2019
[124] Telecom Paper, Millicom completes sale of Tigo Senegal to Saga Africa Holdings consortium, April 2018



SSA: Sub-Saharan Africa, MENA: Middle East and North Africa, LAC: Latin America
Source: World Bank, World Development Indicator Database; The Global Findex Database[125]

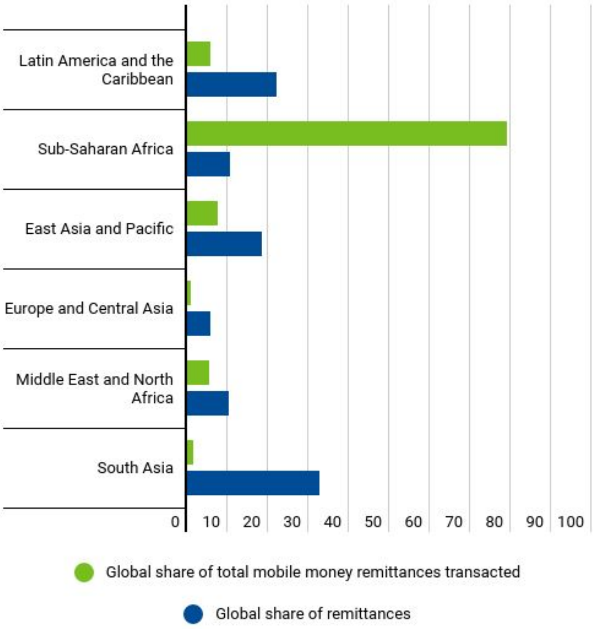
[125] IMF Fintech in Latin America and the Caribbean: Stocktaking, March 2019

In this market, it is also worth noticing that two founding members are originally from Argentina with US and Latin America operations, MercadoLibre et Xapo. MercadoLibre launched a payment solution Mercado Pago, reaching $18 billion in transaction volume in 2018[126]. With a high mobile equipment rate[127] and rampant inflation, Libra's value proposition could be particularly well suited.

International Remittances

The international remittances market represented $529 billion in 2018 for more than 160 million economic migrants[128]. Transaction costs are high with an average of 6.94% to transfer $200[129], reaching even 9% for the countries of sub-Saharan Africa.

Mobile payment and remittances are not necessarily uncorrelated. Thus, the success of Mobile Money in sub-Saharan Africa helps to make it a vehicle for remittances.

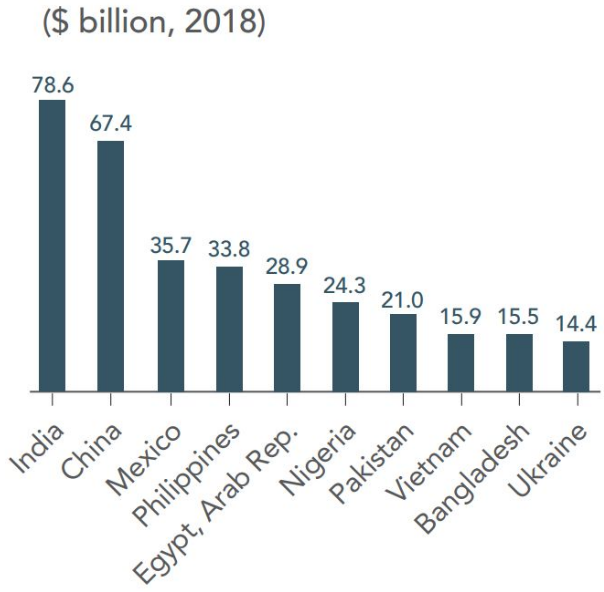


Global share of remissions (2017) Sources: Global System for Mobile Communications Association (GSMA), World Bank, IMF staff calculations

For intermediaries, remittances offer potential higher margins at lower volumes. Nevertheless, two obstacles must be overcome. First, 90% of remittances made through Money Transfer Organizations (MTO) are received in cash[130]. The solution must, therefore, be adopted locally as a payment method for it to be credible as an international transfer solution. MTOs are already working to diversify reception solutions[131]. The second difficulty is that part of the transfer costs are linked to regulatory constraints that will be difficult to reduce significantly..

[126] MercadoLibre, Inc. Reports Quarterly Financial Results 2018
[127] 140 mobile subscription for 100 inhabitants, World Bank, IT.CEL.SETS.P2 indicator, June 2018
[128] ILO, Global Estimates on International Migrant Workers: Results and Methodology 2018 (Reference year: 2017)
[129] World Bank, Remittance Prices Worldwide, in Q3 2018,
[130] IFAD, Global Forum on Remittances, Investment and Development 2018 Asia-Pacific Report
[131] BIS, Cross-border retail payments, February 2018

India, the primary recipient country of these flows, is of strategic importance. Facebook and WhatsApp are well-established[132] and the government has started a cashless policy[133]. Nevertheless, the regulatory status of cryptoassets is uncertain[134].



Principal Recipient Countries in 2018, Sources: World Bank & IMF[135]

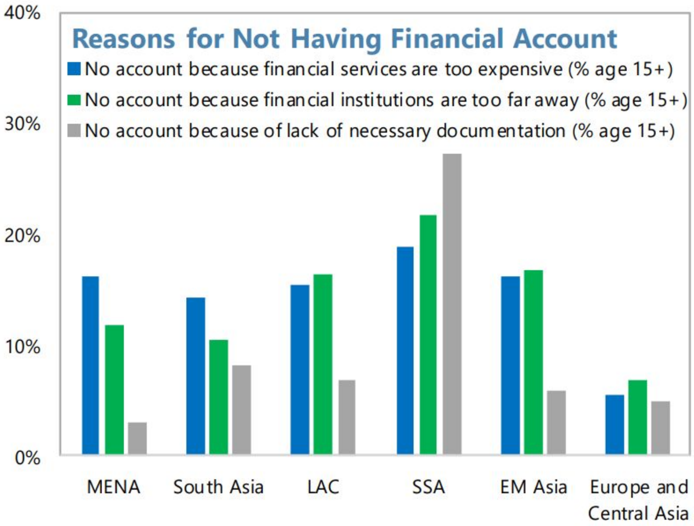
Online Identity

Identity on the Internet is a challenge as old as the network. Several large companies have tried to become the reference platform[136], including Facebook. In contrast, several entities work nowadays on identification standards where users would control their information and rely on multiple providers.

In this line of ideas, several blockchain startups[137] and standards[138] have been launched. Early 2019, Facebook bought Chainspace, a startup that had worked on a solution, *coconut*, allowing a selective sharing of information[139]. A standardization process is also being finalized with by W3C around the concepts of *Decentralized Identifiers*[140] and *Verifiable Credentials*[141]. It seems that US authorities are already interested in the model[142].

[132] More than 200 millions active users per month claimed in February 2017
[133] http://cashlessindia.gov.in/
[134] Sanghamitra Kar, Government departments discuss draft bill to ban cryptocurrencies, The Economic Times
[135] World Bank, Migration and Remittances, Recent Developments and Outlook, Avril 2019
[136] Microsoft Passport since the 90's, Facebook connect, Google connect …
[137] Everynm, Uport, Sovrin …
[138] For instance for Ethereum https://erc725alliance.org/
[139] Alberto Sonnino, Musta fa Al-Bassam, Shehar Bano, Sarah Meiklejohn and George Danezis, *Coconut: Threshold Issuance Selective Disclosure Credentials with Applications to Distributed Ledgers*, NDSS 2019
[140] W3C, Decentralized Identifiers (DIDs) v0.13, Draft Community Group Report 20 June 2019
[141] W3C, Verifiable Credentials Data Model 1.0, W3C Candidate Recommendation 26 March 2019
[142] Testimony of Douglas Maughan (US Department of Homeland Security) before the US House, 8 may 2018

The white paper states that the development and promotion of an open, decentralized, and portable identity standard is one of the objectives of the Association. One of the ideas presented to avoid the KYC process to be a factor of exclusion from the financial system[143]. Facebook already has the experience of having established industrial standards[144], and it seems a necessary condition in line with current industrial efforts.



The main reason for not having a financial account in sub-Saharan Africa (SSA): the lack of official documents
Source: World Bank, World Development Indicator Database; The Global Findex Databaseskills[145]

Teams

Calibra

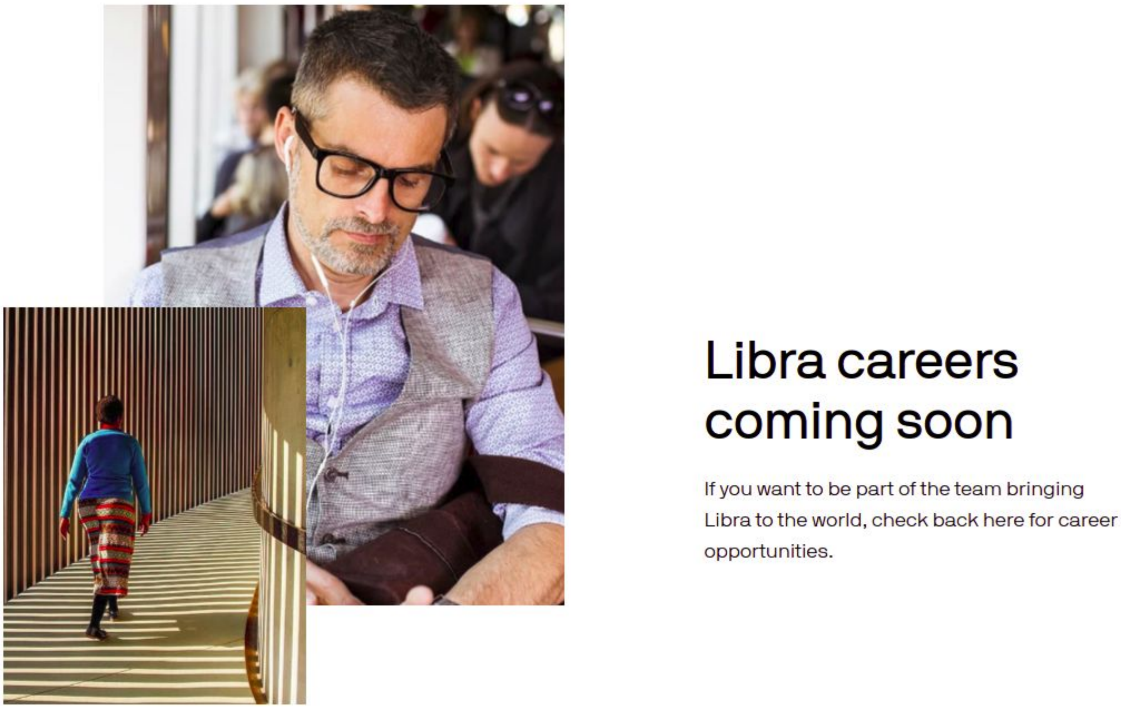
About 50 people are currently working on Calibra, mainly based in San Francisco, except notably Computer Science scientists acquired from major universities (MIT, UCL ...)

David Marcus, Head of Calibra
Previously **VP Messaging of products** at Facebook since 2014, David is especially credited for transforming Messenger into a real platform. Born in Paris, studying in Geneva, David founded several technology companies. In 2008 he co-founded Zong, a mobile payment solution for games and social networks. Acquired in 2011 by Paypal, he joined the company and became president in 2012.

[143] "By default, because of KYC requirements financial, de-risking has pushed billions of people on the margins of finance" Dante Disparte, Al Jazeera, 26 June 2019
[144] For instance *Open Graph* http://ogp.me/
[145] IMF, Fintech in Latin America and the Caribbean: Stocktaking, March 2019

Libra association

The Libra Association does not have a *Managing Director* yet, while essential to the organization. There are currently a few employees, based in different cities. It is expected that the team will move to Geneva. Their experience is mainly in technology companies (Bittorrent, Paypal, Zong, ...) with the notable exception of the policy and communication director, Dante A. Disparte, previously CEO of a consulting and insurance brokerage firm in Washington.



Libra careers coming soon

If you want to be part of the team bringing Libra to the world, check back here for career opportunities.

Libra.org career page on July 8, 2019

Intra breuissimum tempus Aries extollitur, Libra tardissime emergit:
and hoc tamen sidus and illud eiusdem naturae est,
cum illud exiguo tempore ascendat, illud diu proferatur.[146]

Seneca, Naturales quaestiones, Book VII

Potential outcomes

The project, presented as experimental, still has many uncertain parameters. Several outcomes are possible in the next phases of the project. In any case, this project will have a significant impact on the development of similar or complementary solutions.

Scenario 1: Failure to launch the project
Although the probability is low, it is possible that the project will not result in the launch of Libra and the corresponding network. First, there are some uncertainties inherent in the development of a large-scale IT project. Secondly, it seems to us that the main weaknesses lie on the governance side of the association. The announced founding members are not yet aligned at the strategy level, with diverging initiatives and interests. The Libra Association has no governance, director, or strategy at this stage. Finally, there is the risk of frontal political opposition, particularly in the United States in the run-up to the 2020 presidential elections. In the case of a complete failure of Libra, Facebook's effort around Calibra could be reorganized to provide a more traditional payment solution.

Scenario 2: A limited launch in 2020 with a gradual adoption
The Libra solution and a commercial offer from Facebook are confronted with the status quo in several ways. First, the regulations would require adjustments. Libra is a complex product, particularly for tax law and financial regulations. Furthermore, the context is that of a strengthening of regulators, particularly to prevent fraud and money laundering. Secondly, the payment, peer-to-peer, and international transfer markets are now in the process of being reconfigured with many institutions and new entrants. Thirdly, on the user side, these are solutions whose adoption is linked to local and sociological practices.

The 2.4 billion users of the social network do not easily make it a global payment operator. It is therefore likely that in 2020 the deployment of the solution will be limited to a certain number of states and use cases. Then the adoption of the solution could be gradual over the next five to ten years. This process might imply significant investments.

Scenario 3: Libra as a global financial infrastructure
One of the reasons for creating Libra as a separate project with a distinct entity is to allow the emergence of a complete ecosystem.

For mainly political reasons, it does not seem conceivable that Libra or associated technologies could be globally adopted as the large-scale architecture of the global financial system by established

[146] "Aries again rises in a moment, Libra lifts its scales very slowly; yet the one sign is of the same nature as the other, though that one mounts in a brief space, this comes forth very deliberately."

institutions. Nevertheless, new entrants in payments or finance may rely on this currency to provide services. Facebook already has experience converting its services into platforms for third parties. However, given the stakes, it will be necessary to guarantee the stability and quality of the interfaces (APIs) over the long term. This requires a change in culture compared to the history of messaging service APIs and social networks. Moreover, Calibra's positioning as a key player and the influence Facebook teams have had so far distorts competition and may alter overall trust.

The project announces a broader opening of the project within five years with the switch to governance rules guaranteed by the system and an open process of validation. However, the success of the platform will depend on the ability to attract third-party investments, the quality of its design and the absence of regulatory or governance deadlocks. Given the current landscape, it seems conceivable that the solution could constitute, as a network and as a technology, an important component of a recomposed financial ecosystem.

Legacy

Beyond the project, this announcement is significant for the emergence of global financial and payment systems. The project is based on the idea that technologies can now guarantee properties of integrity and transparency, paving the way for new institutional infrastructures. By proposing a resounding but still incomplete solution, this project stimulates the already advanced work of public and private actors on the subject.

The perceived political threat can also lead to regulatory harmonization. As we have seen with the phenomenon of public sales of tokens, the difference between the time of standard development and that of private innovation encourages regulators to be mutually inspiring[147]. It is not excluded that this threat could also lead to complete bans locally.

Finally, current players in the cryptoassets market, such as exchanges, wallets, and custodians, will benefit from the development of new asset classes based on similar models. The development of security tokens is already an example of this synergy, relying for instance on players who have been able to set up rigorous compliance processes. Conversely, public and private projects based on these models will benefit from an adoption facilitated by the maturity and diversity of solutions proposed by these actors, adapted to different use cases and markets.

[147] Xavier Lavayssière, The ICO regulatory competition, Rethinking Law, June 2018

Glossary

Address

An address is an identifier that identifies a user or a smart contract on a network. The address is usually derived by hashing a public key (see hash).

Public Key and Private Key

Terminologies used in the context of asymmetric cryptography. A user generates a pair consisting of a public key and a private key. The public key is transmitted over the network. A correspondent can use it to encrypt a message that can only be read by the user. Conversely, the owner of the private key can also use it to sign a message. The signature can then be verified utilizing the public key. This signature process is used for transactions.

Cryptoasset

Digital financial asset represented on a distributed ledger. The system guarantees possession and transfer of the asset. We can distinguish several categories of cryptoassets:

- Cryptocurrencies, generally refer to native units of a network. The best known are Bitcoin and Ethereum,
- Utility tokens, to be used as payment for a particular service,
- Stable Coins, representing a stable value in an existing currency
- Securities tokens, representation of existing securities or a similar set of rights

Exchange

Exchanges are marketplaces where supply and demand for cryptocurrencies meet. These are essential elements of the ecosystem in that they are the main gateway for cryptoassets. It is also the main actor that can be supervised by the regulators.

Hash

One way process giving a result of fixed size from a data set. The most commonly used methods are SHA (Secure Hash Algorithm), a suite of standards established by NIST, a U.S. agency.

Node

A node on a peer-to-peer network refers to a software instance connected to the rest of the network. Each node relays the shared information on the network (for example blocks and transactions).

Merkle Tree

A Merkle tree is a data structure that guarantees the integrity of information and facilitates proofs of inclusion. Data that must be included in the tree is hashed, then each pair of hashes is hashed again, until reaching a singleton, the root. In Bitcoin the root of a Merkle tree of a block's transactions is included in its header. In Libra, Merkle trees are used to guarantee transactions history and store data (state and events).

Module

Generic term used in computer science to designate a reusable part of a computer program. In the context of Libra, it is a program in *Move* interpreted by the nodes to add features such as the minting and transfer of libras.

Move

Language designed for resource management in Libra. The term refers to the binary level, the intermediate language, and the high-level programming language. It is expected to provide flexibility and security properties (including verifiability).

Remittance

Regular transfer of money from a migrant worker to his family. Remittances (ḥawāla in Arabic and hundi in Hindi) are sent through regular financial institutions, startups or informal networks[148].

Resource

Term for a value associated with an address on Libra. A resource is linked to a module that defines how it can be updated. The Libra currency is itself implemented as a resource on user accounts and controlled by a module.

Peer-to-peer (*P2P*)

In computer science, a peer-to-peer network is a network of computers or software that exchange information without predefined roles. It differs from the client-server model where the role of the server is to provide services or resources to the client.

In finance, a peer-to-peer payment or transfer is a transfer directly between individuals, usually within the same application. This model differs from a bank transfer or a regular payment.

Bitcoin and cryptocurrencies allow peer-to-peer financial exchanges between individuals and rely on a peer-to-peer network.

[148] US Treasury, Hawala and its role in The Hawala Alternative Remittance System and its Role in Money Laundering, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/FinCEN-Hawala-rpt.pdf

Validator

In the context of a consensus mechanism, a validator is a node proposing (*leader*) or validating transactions. Its role consists in verifying transactions, signing them, and relaying them. In the context of Bitcoin, validation is ensured by miners that must additionally solve a computationally intense puzzle.

Wallet

A wallet is a program, device or service that enables the management of the user's private keys and the creation and sending of transactions over the network. An important distinction in the context of Libra:

- *Custodial Wallet,* where the service provider manages the private keys on behalf of the user or manages funds in an aggregated address. Exchanges (See exchanges) of cryptocurrencies and Calibra are two examples of Custodial Wallets
- *Non-Custodial Wallet,* where only the owner of the cryptoassets has access to the private keys. On the software side, most clients, including the Libra client, are non-custodial wallets.

Author

Xavier Lavayssière

Xavier Lavayssière is an independent researcher on blockchain and regulation, with a particular interest in infrastructures compliant by design. With a background in Computer Science (Claude Bernard Lyon University) and Public Law of the Economy (Panthéon-Assas University), experience in high-level public administration (General Commissariat for Investment, European Investment Bank, Embassy of France in the United States), he has been working since 2014 on issues (see publications), technical projects (Cryptotux.org, Nanti, Forest as a DAO) and the structuring of the ecosystem around these technologies. He co-founded the Smart Contract Academy, Le Blockfest, Chaintech, ECAN and The Block Café. Xavier Lavayssière teaches at higher education institutions (Ecole des Ponts, Paris Bar School, EM Lyon ...) and leads the pedagogy of a dev bootcamp (Alyra). He regularly participates in the Blockchain Perspectives Chair at Louis Bachelier Institute.

Publications

- *The emergence of a digital order, AJ Contrats, n ° 2019_7, 2019*
- *Blockchain and financial securities: minimalist decree for ambitious reform, RLDA, n ° 144, 2019 [FR]*
- *The ICO regulatory competition, Rethinking Law, June 2018*
- *Smart Contracts : Case Studies and Legal Analysis, Collective Work, 2018 [FR]*
- *Blockchain Legal Issues, Legal Subgroup Report, France Strategie, 2018 [FR]*
- *Regulatory Framework for Token Sales: An Overview of Relevant Laws and Regulations in Different Jurisdictions, 2018 [EN]*
- *Bitcoin cryptocurrency could help to secure financial transactions, 2014 [FR] [EN]*

Email: xavier@libracpd.com
Twitter: @XavierLava

Acknowledgments

Many thanks to Mark Zeller, Lucas Verra, Camille Rouge, Maxime Evrard and Thiebald Cremers for their comments, information and advice.

Annex I: Founding Members

Company	Area	Headquarters	Country
Iliad	Telecom	Paris	France
Vodafone Group	Telecom	London	UK
Anchorage	Cryptoassets	San Francisco	USA
Bison Trails	Cryptoassets	Brooklyn	USA
Coinbase	Cryptoassets	San Francisco	USA
Xapo Holdings Limited	Cryptoassets	Palo Alto (main activity center)	USA
Andreessen Horowitz	Venture Capital	Menlo Park	USA
Breakthrough	Capital Venture Capital	NYC	USA
Capital	Venture Capital	Palo Alto	USA
Capital	Venture Capital	NYC	USA
Mercy Corps	Social / NGO	Portland	USA
Union Square Ventures	Venture Capital	NYC	USA
Creative Destruction Lab	NGO / Social	Calgary	Canada
Kiva	NGO / Social	San Francisco	USA
Women's World Banking.	NGO / Social	NYC	USA
Mastercard	Payments	Purchase	USA
PayPal	Payments	San Jose	USA
PayU (Nasper)	Payments	Hoofddorp	Netherlands
Stripe	Payments	San Francisco	USA
Visa	Payments	Foster City	USA
Facebook / Calibra	Payments	Menlo Park	USA
Booking Holdings	marketplace	Delaware	USA
Farfetch	marketplace	London	UK
Ebay	Marketplace	San Jose	USA
Lyft	Marketplace	San Francisco	USA
Mercado Pago	Marketplace	Buenos Aires	Argentina
Spotify Technology	Payments	Sweden	Stockholm
Uber	Marketplace	San Francisco	USA

Appendix II: Etymology

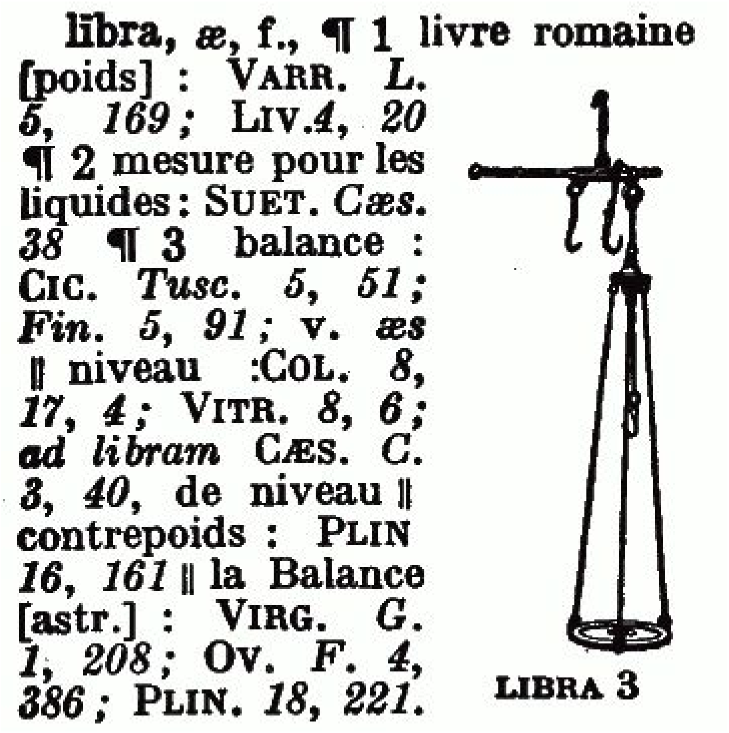
Libra is a Latin feminine word (plural librae) meaning:

- A Roman pound (329 grams)
- A measure of liquid (hence *liter*)
- A balance or counterweight
- The astrological symbol Libra

The term has a legal dimension, per aes and libram[149] means an act performed during a formal procedure.

It should be noted that the word does not have a common origin with:

- Liber, libera, adjective designating free from proto-european "people"
- Liber, libri, name designating a book or the living bark of a tree



libra, æ, f., ¶ 1 livre romaine [poids] : VARR. *L. 5, 169* ; LIV. *4, 20* ¶ 2 mesure pour les liquides : SUET. *Cæs. 38* ¶ 3 balance : CIC. *Tusc. 5, 51* ; *Fin. 5, 91* ; v. æs ‖ niveau : COL. *8, 17, 4* ; VITR. *8, 6* ; *ad libram* CÆS. *C. 3, 40*, de niveau ‖ contrepoids : PLIN *16, 161* ‖ la Balance [astr.] : VIRG. *G. 1, 208* ; OV. *F. 4, 386* ; PLIN. *18, 221*.

LIBRA 3

Illustration from the illustrated Latin-French dictionary of Félix Gaffiot, 1934

[149] See above Gaius quote

hello@libracpd.com

https://libracompendium.com