Monday, July 8, 2019

AtonRā Partners

Libra... And Now What For Fintech and Mobile Payments?

This research report aims to explain the potential as well as the technical and economic challenges of the new Facebook-backed cryptocurrency. We clarify what Facebook's Libra might change in the crypto world as well as the possible implications on some other sectors that we follow closely, such as mobile payments and fintech.

On June 18th 2019, the Libra project was officially announced to the public after more than one year of development. The plans are for a live deployment during the first half of next year. High expectations are being built on Libra as its primary stated objective is to allow a cheap and immediate exchange of "money", supported by the making of a global and stable currency based on blockchain technology. When sending $200 around the world the commission costs hoover at around 7%[1] on average: this makes clear the need for a cheaper alternative.

Being backed by the likes of Facebook, Visa, Mastercard, Vodafone, Uber, Andreessen Horowitz, and many others, gives Libra credibility. However, due to Facebook's history of privacy violations and the threat that a global, unregulated private coin might have in the world's economies, critics have stepped-up in the last few days. Private companies, by definition, are not philanthropic. Is there any other reason rather than "banking the unbanked" behind Libra?

We believe that to understand the real incentive for Libra, we need to go back in time. Indeed, Facebook first floated the idea of having a payment system within its social platform back in 2010 with the launch of **Facebook Credit** (FC), which was thought to be the killer app of PayPal. The main advantages for Facebook would have been twofold: on the one hand, they would have got 30% of all revenue made by developers that would have used FC, on the other hand, they would have enabled users to seamlessly pay within their platform, thus getting precious consumer's data for their advertising system.

Even though the main goal is tremendously ambitious, available details are currently very scarce. The "white paper" states three main points about the coin:

[1] https://www.worldbank.org/en/news/press-release/2019/04/08/record-high-remittances-sent-globally-in-2018

1) “Built on a secure, scalable, and reliable blockchain”,

2) “Backed by a reserve of real assets”,

3) “Governed by the independent Libra Association”

Conclusion

We believe that as of today, Libra has not the technical capabilities, regulatory backing, economic acceptance, and financial infrastructure empowering billions of people, to become a global currency. The impossibility by Libra for secured, large-scale, and fast transactions without a central authority is a clear indication of where the coin would have to make concessions. The coexistence of scalability, security, and decentralization in governing the money flows is not possible at the same time because of how a blockchain works; an impossible trinity characterizes the three elements.

Furthermore, authorities are reluctant in trusting systems that might potentially facilitate money-laundering, terrorist financing, and tax evasion activities. Central banks are vital in governing the current financial system, controlling inflation and sustaining economies. Shifting the economic power from public authorities to private entities like the Libra Association would have a profound impact. Central banks around the world won’t likely accept to be taken over by an individual player as his interests would not align to those of the public.

We can foresee two kinds of users for Libra:

- Cryptocurrency/technical users:

  People that do not care about anonymity but who are looking for a low-risk asset or willing to use a stablecoin (e.g., crypto traders). Those needing anonymity and censorship resistance will never transact with Libra but rather stay with Bitcoin/Monero and the likes instead.
- Non-cryptocurrency/non-technical users:

  Libra will certainly attract users in developing countries (namely, the unbanked), who search low costs, fast transactions, and a way to escape from hyperinflation. However, the strong know-your-customer (KYC) requirements, the lack of internet connectivity (75% of the 1.7 billion who are unbanked do not have access to the internet) in addition to the unfriendliness by some governments over cryptocurrencies will likely **slow down** - **if not completely stop** his **adoption**. Users in developed countries which are searching for **low transaction fees** and **high speed** will likely use **platforms such as Revolut** or **their e-banking platforms**. Fees from traditional banks will get under pressure while transaction speed is to improve, which is already the case for international payments made within the EU, for example.

In the "white-paper," it is reported that the backers of the Libra association will get rewarded by the dividends Libra will generate in the future. We believe that the reality might be a bit different, as we see the gathering of data (spending habits) by Libra users, as the main reason behind their support in the project. Such companies would see their services and goods one click away from the ads. By allowing the purchase of products directly from advertisements on the apps, they could incentivize, if not restricting, such purchases through their coin.

	TPS	Openness	Centralization	Censorship resistant	Anonymity	Stable	Access
Bitcoin	4.7	Open	None	Yes	Partial	No	On/off ramps
Visa	1'736	Private	Complete	No	None	Yes	Trival
Monero	10	Open	None	Yes	Complete	No	On/off ramps
Libra	***1'000***	***Private***	***Semi***	***Not really***	***None***	***Almost***	***On/off ramps***
PayPal	200	Private	Complete	No	None	Yes	Link to a bank account

AtonRâ Partners - *Fig 1: summary of different international digital payment methods*

One thing is evident to us, the launch of Libra is going to speed-up, and likely change once and for all, the perception of bank's CEOs that technology so far didn't move a needle in their businesses. We believe that the entry from Facebook into the digital currency world is just the premise of what's next to come: the massive entry of the tech giants into the banking space as it is currently happening in China.

Tech giants such as **Alibaba** and **Tencent** bundled digital payments (linked to a bank account) with their apps and offered a seamless mobile payment experience to their users. With the take-off of mobile payments, the same Alibaba and Tencent gather vast amounts of data, giving them insights into customer's preferences. This was possible as the penetration of credit/debit cards in China was extremely low. Facebook (and the Libra association) want to go one step further. By disrupting the mean of payment and by having access to precious data on the circulation of money, the Libra association would have an insight into consumers behaviors like no one else.

Whether Libra take-off or not it comes as a wake-up call for the banking and financial industry that has to react or take the risk of being wiped out. We believe that Libra acts as a catalyst for our Fintech and Mobile Payment themes as it would speed-up the ongoing digitalization of payments and increased spending from legacy banks, neobanks, and fintech of any sort into financial software products.

White Paper Analysis

In this section, we provide our analysis of the Libra white paper.

Basics of Blockchain Networks

Nowadays, the word "blockchain" is used to designate all cryptocurrencies. However, the correct term is **Distributed Ledger Technology (DLT)**, where "blockchain" is only a subcategory. Another subcategory is the family of Byzantine Fault tolerance, where Libra stands. Thus, Libra is not a blockchain (for more information, check the technical explanation in the Appendix). A distributed ledger is a rather simple concept. Through decentralization, it eliminates the need for a central authority or intermediary, to process, validate, or authenticate a transaction.

The first constituent of a DLT is a network of **nodes** (computers, servers, smartphones) that connects using a peer to peer (P2P) protocol. These nodes must perform several actions:

✓ Receive and broadcast transactions.

✓ Verify such transactions.

✓ Store the current (and previous) state of the ledger (Blockchain or database).

✓ Agree on the next (future) state of the ledger.

Depending on the subcategory of DLT, the ledger structure and algorithms used to agree on the next state of the ledger might be completely different. In Bitcoin or Ethereum, the nodes responsible to maintain the network are called **miners** and they can be anyone while in Libra they are called **validators** and their real-world identities are known and fixed (i.e., Uber, Mastercard, Spotify, etc.).

Let’s assume that *Bob* wants to send coins to *Alice* (i.e., move coins to a different address in the ledger):

1. *Bob* will use a software (e.g., Calibra) that connects to one of these “nodes.”
2. The software will sign the transaction with *Bob*’s private key and send it to the node.
3. The node will verify *Bob*’s transaction (i.e., that the signature belongs to *Bob*) and broadcast it to the network.
4. The node in charge to decide the next ledger state will gather transactions (i.e., *Bob*’s and other’s).
5. If the transaction is successful, the ledger updates with *Bob*’s transaction: *Alice*’s ledger account gets credited with *Bob*’s coin.

The mechanism of electing who will decide the next state, and how is done, is called **consensus**. We explain this concept in details in the Appendix of this research report.

Is This Cryptocurrency Something New?

The idea of stablecoins is nothing new in the crypto space. **Tether** from Bitfinex, the biggest and most known of these coins, was first created in 2014 to give stability to cryptocurrency users. By backing 1 to 1 with real-world assets, the value is pegged to be always equivalent to the actual asset (1 US Dollar in the case of Tether). Even though Tether went through several scandals and suspicions of not having the backing of its assets[2], it is still the most traded stablecoin in terms of volume and has today a market cap of $3.5 billion.

Since the creation of Tether, several other centralized stablecoins emerged[3], backed by other currencies or assets such as gold or real estate. However, a new kind of stablecoins, the decentralized ones, truly revolutionized the space by providing stability without authoritative control[4]. Even though technically impressive, these coins can handle only a few transactions per second (i.e., low capacity), suffer from high volatility, and are very difficult to use. Therefore, as of today, Tether is still widely used despite the scandals and opacity surrounding its network.

Other cryptocurrencies known as high-performance blockchains emerged to tackle the problem of scalability. Such Distributed Ledger Technology (for instance, **EOS** in the family of delegate Proof-Of-Stack

[2] https://www.theblockcrypto.com/2019/05/21/tether-admits-in-court-to-investing-some-of-its-reserves-in-bitcoin/

[3] https://coinsutra.com/best-stablecoins/

[4] https://hackernoon.com/a-comprehensive-guide-to-decentralized-stablecoins-22f66553c807

(dPOS)),￼ or **Cosmos** in the family of practical Byzantine Fault Tolerance - pBFT￼) can achieve (theoretically) hundreds of transactions per second (TPS). However, their prices are not regulated or backed by real-world assets and thus fluctuate freely.

The Libra "Blockchain"

- ✓ Libra is not a blockchain, and the coin is not a cryptocurrency.
- ✓ Libra **will not be anonymous** (see Figure 2). Users are going to be under **pseudo-anonymity** (like Bitcoin), meaning that their identity hides behind a unique deterministic identifier. As KYC will be mandatory, the pseudo-anonymity would disappear.
- ✓ **1000 Transaction Per Second (TPS)**. This performance is only possible because the network is centralized/permissioned/private. If the network becomes decentralized, the TPS will go down drastically. (see Section *Trilemma of distributed systems and the concept of scalability* in the Appendix). **All validators are known by each other** (as opposed to Bitcoin). Twenty-eight members are already onboard with a target of 100 validators at launch. The centrality and the corporate nature of the validators make **Libra not resilient to censorship**.
- ✓ Even though Facebook does not claim any control over Libra, the validators do. The possible cooperation of **at least 1/3** of validators would lead to a compromise network. If this happens, the rewriting of the database would be possible at near zero cost. Libra is thus **much less secure than networks such as Bitcoin,** where dozens of thousands of nodes manage the network with a 51% resistance failure (it would cost several billions of dollars to conduct[5]).
- ✓ Libra will use a **new programming language called Move**. History shows that modern programming languages, even though designed with security in mind, do not necessarily lead to higher security. Solidity, the smart contract language built for **Ethereum**, had flaws that led to the Decentralized autonomous organization (DAO), allowing for the theft of 3.6 millions of Ethereum[6].
- ✓ Libra will allow smart-contract ability. Cambridge data Analytica leakage shows us that Facebook has a bad history of letting developers (that might be crooked)[7] build on top of its platform.

[5] https://cryptoslate.com/analysis-bitcoin-costs-1-4-billion-to-51-attack-consumes-as-much-electricity-as-morocco/

[6] https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee

[7] https://techcrunch.com/2019/06/18/libra-analytica/

The intention by the Libra association to completely open up the network is a utopia in our view: all the promised performances require the network to be permissioned ("private"). A DLT that claims to provide decentralization, security, and speed has either bent the laws of physics or it has discovered a breakthrough method that solves the major DLT scalability problems that have puzzled top mathematicians and computer scientists for the past decade (like the Ethereum Foundation).

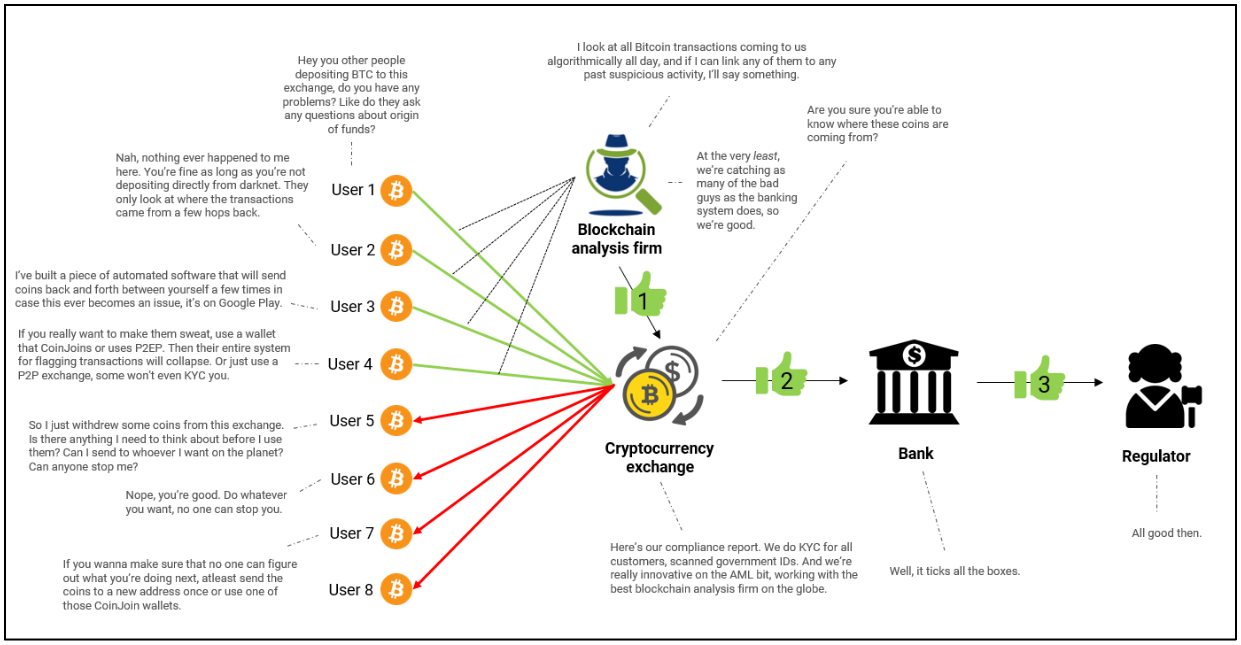

Hey you other people depositing BTC to this exchange, do you have any problems? Like do they ask any questions about origin of funds?
I look at all Bitcoin transactions coming to us algorithmically all day, and if I can link any of them to any past suspicious activity, I'll say something.
Are you sure you're able to know where these coins are coming from?
Nah, nothing ever happened to me here. You're fine as long as you're not depositing directly from darknet. They only look at where the transactions came from a few hops back.
At the very *least*, we're catching as many of the bad guys as the banking system does, so we're good.
User 1
Blockchain analysis firm
User 2
I've built a piece of automated software that will send coins back and forth between yourself a few times in case this ever becomes an issue, it's on Google Play.
User 3
1
If you really want to make them sweat, use a wallet that CoinJoins or uses P2EP. Then their entire system for flagging transactions will collapse. Or just use a P2P exchange, some won't even KYC you.
User 4
2
3
So I just withdrew some coins from this exchange. Is there anything I need to think about before I use them? Can I send to whoever I want on the planet? Can anyone stop me?
User 5
Cryptocurrency exchange
Bank
Regulator
Nope, you're good. Do whatever you want, no one can stop you.
User 6
User 7
All good then.
If you wanna make sure that no one can figure out what you're doing next, atleast send the coins to a new address once or use one of those CoinJoin wallets.
User 8
Here's our compliance report. We do KYC for all customers, scanned government IDs. And we're really innovative on the AML bit, working with the best blockchain analysis firm on the globe.
Well, it ticks all the boxes.

Fig 2: Pseudonymous of Bitcoin privacy unveiled

Libra's Ecosystem Key Points

The key points to retain from the white paper surrounding the ecosystem is summarized as follow:

✓ Libra reserve: they want to build a **geographically distributed** and regulated group of **global institutional custodians**. Because of the diverse regulation, the distribution of custodians will make things difficult.

✓ To meet law and regulation, **KYC will be mandatory**. However, this is tremendously difficult (impossible?) to achieve in an open network (a.k.a. Current crypto space regulation).

✓ **Centralization**: the fact that the network is centralized and that a user would need to trust two third of the validators would equal to shift the trust from the well-known banks (and their regulatory space) to a cluster of big technology companies.

✓ Private key: the way Calibra (the Libra wallet) plans **to manage identities is unclear**. If the user has control over it, then the private key issue and its implications are close to cryptocurrencies' ones (losing control of the key means losing control of funds). If the key, for instance, derives from the user's Facebook account, then privacy is indeed violated and, most importantly, the oversight control over the funds goes to a big tech company instead of an allowed bank.

✓ Despite the technical limitations of Libra, access to **2 billion Facebook users** might significantly push Libra adoption.

✓ Governance and management on DLT projects were found to be difficult in the blockchain. With collaboration coming from numerous big tech companies, the Libra Association can get things done. Moreover, critical financial and technical resources might enable Libra to achieve more dazzling results than those shown by other existing cryptocurrencies.

Economic And Macroeconomic Analysis

In contrast to the previous section where we highlighted the technical difficulties faced by Libra, in this part of our research, we accept the fact that Libra can support international payments while ensuring enough the security and anonymity of its users. Consequently, scenarios depicting the economic potential and possible macroeconomic consequences, due to the broad adoption of Libra, are described.

Economic impact

Migrants Remittances

The World Bank estimates the global the **annual remittance flows at $689 billion** in 2018 ($633 billion in 2017). The most substantial flows came from low-to-middle-income countries ($529 billion in 2018, up of 9.6% vs. 2017). Remittance inflows growth has been robust in East Asia and Pacific (7%) and South-East Asia (12%).

On average, **the transferring of $200 costs around 7%**, surging to 10% and above in many African countries and small Pacific islands. Reducing the percentage of the fees to 3% by 2030 is a global target under the Sustainable Development Goal (SDG). Banks are the most expensive remittance channels (average cost of 11% in 1Q19). Such data shows that the first potential application of Libra appears clear: money movement between borders needs to be available at lower costs.

Medium Of Exchange

Money finds its use as a mean of exchange, a unit of account, and store of value. Libra would best fit the first category but could expand into the more ambitious role of a store of value such as the US Dollar or the Euro today. Since Libra aims primarily at being the mean for **transactions**, markets involving large flows (Forex markets notably) are those that will be affected the most, even more, if the corporate world would embrace it.

Platforms converting fiat currencies into Libra will probably keep transaction costs, including bid/ask spreads, as low as possible. Since tangible and liquid assets back Libra, any mispricing would be temporary, as a real arbitrage opportunity exists. With this in mind, the threats around Libra's stability are unfounded.

Although far and just a theoretical prediction, only regulation would prevent it from being employed as a real alternative to current currencies, potentially wiping out the need of being pegged to other currencies' values.

Digital Payments

Digital payments applications are rapidly expanding worldwide. The benefits they provide in terms of speed, reliability, and low costs are propelling their growth. Mobile payments services in "unbanked" countries are still very successful as they have been able to adapt to existing infrastructure without requiring any significant upgrades by end-users.

Payments and money transfers will be the most affected by Libra. Such activities are estimated to be worth between 10-15% of today's total banking revenues.[8] Libra would be partially competing with the digital payments world too. Indeed, on the one hand, Libra may need the infrastructure to allow people exchanging fiat currency for Libra; on the other hand, Libra aims to eliminate the need of moving money back and forth from different currencies by channeling everything into a universal medium of exchange, that the Libra Association wants to set.

[8] *The Future Of Banking: Regulators To Decide If The Crypto Stars Align For Libra*, S&P Global Ratings, Jun 2019 (https://www.allnews.ch/sites/default/files/files/20190625_SP_Libra_Regulators___Decide.pdf)

Comparing the transaction capacity permitted through several means of payment helps to understand their adoption potential. Multiple users will need to execute their payments simultaneously. A system supporting a high number of transactions must nowadays allow for close-to-immediate execution. Then, looking closely at the maximum number of transactions per second gives us a more in-depth insight into the system ability to process numerous transactions at the same time.

Payment method	Transaction per second (TPS)		
	Maximum theoretical	Maximum practical	Average
Bitcoin	27	7	4.7
Visa	> 65'000	Unknown	1'736
Ethereum	25	15	15
Libra	1'000	Unknown	1'000
PayPal	Unknown	450	200
Hedera Hashgraph	500'000	Unknown	Unknown

AtonRâ Partners

Macroeconomic Impact

A tough choice is to be made by the Libra association in deciding which assets are to be part of Libra. Do they follow systems in place such as the IMF's Special Drawing Rights (SDR) or do they take the risk of being politically exposed by their preferences in including one asset vs. another one that is backing Libra?

The SDR, an international reserve asset created by the IMF in 1969, is aimed at supplementing member countries' official reserves. For example, the Chinese renminbi was added to the SDR basket on the 1st October 2016 and was an essential milestone for integrating China within the global financial system, hence supporting the use of renminbi all over the world.

Deciding to hold specific currencies while excluding others impact the way such currencies or assets are perceived and used worldwide. How would the Libra association choose which assets to include or not into the backing of the Libra? How would one make sure that personal and commercial interests do not dictate their decisions?

Central banks hold foreign exchange reserves for a variety of purposes: keeping own currency value at a fixed rate with respect to foreign ones, maintaining liquidity in case of economic turmoil, balancing outflows/inflows of foreign currencies, curbing or controlling inflation, providing confidence to international markets, diversification (also other assets such as gold and interest-bearing investments are held). All these functions would be lost if Libra were to be freed from maintaining reserve assets after having reached wide deployment.

The Future Role Of Central Banks

Central banks mainly use three tools to carry out their monetary policy: discount rate, reserve requirement, and open market operations. Those are valid until the current system, built on fiat currencies and network among banks, holds. The management of the amount of money circulating in the economy and its costs have been the primary tools through which economies have survived the 2008 financial crisis. The removal of such instruments from the hands of central authorities or making it ineffective are the two dangers posed by the rise of another coin which is able (and willing) to compete in providing other means of payment. It would represent the end of central banks as we know them today.

Macroeconomic Consequences

Firstly, the amount of money invested in low-volatile assets (bank deposits and short-term government securities) would likely have a remarkable impact on them. As (if ever) Libra adoption expands, more and more assets have to be bought. The massive positions held by Libra would **undermine governments' freedom** and potentially influence yields.[9]

Choosing which countries' securities will back Libra brings up another problem. If the Libra Association independently decides the parameters without solely relying on credit ratings or other commonly-used indicators, it might bias governments decisions.

To illustrate the problem, we take the example of the Norwegian Government Pension Fund, a $1 trillion investment fund capable of steering corporation policies towards values shared by such a deep-pocketed entity: not respecting its values would mean seeing a reduction or total cancellation in the stake it invests[10].

[9] Forbes estimates bond market size as being close to USD41 trillion

[10] https://www.theguardian.com/business/2019/jun/12/worlds-biggest-sovereign-wealth-fund-to-ditch-fossil-fuels

An S&P research[11] poses the question of Libra becoming a **reserve currency**, disagreeing with this possibility in the foreseeable future. As the report states, "investors are unlikely to rush to the Libra as a source of stability" as they would do to the U.S. Dollar. In volatile times a credible central bank will not back it. The unknown is how the Libra Association will manage the reserve during market turmoil. Also, the low-interest environment in which we are in would not foster its establishment since low-risk assets won't be able to contribute to Libra's development costs. Nowadays, roughly $12 trillion of investment grade corporate and government bonds have negative yields, according to recent data from Barclays.

We believe that Libra will be hindered by two pivotal issues: **trust** and **interests on deposits**. If the former refers to the doubts posed towards a private entity issuing money, the latter denotes the opportunity cost faced by (likely) not receiving interests on one's account.

Credit creation in the Libra system would imply cross-border lending, which in our view is unlikely to be well received by governments, unless under severe and strict regulations. If this were not the case, monetary sovereignty would phase out, and central banks role blurred; indeed, monetary authorities' task is to maintain stable prices while ensuring financial stability, goals diverging from private sector ones. Losing their power would cost central banks their monetary tools and independence.

Libra would need custodians to hold related reserves; thus, exposure to private entities would imply that the new asset will be dependent also on corporations' reliability. As stated in the white paper, "the reserve will be held by a geographically distributed network of custodians with investment-grade credit rating to limit counterparty risk"[12]. Limiting the **counterparty risk** would not eliminate risk.

The fundamental mission of Libra is to help the unbanked, referring to the portion of the population which is not able to access to the banking system for a variety of reasons (costs, KYC, etc.). Significant users of this new coin are therefore expected to be people from undeveloped countries which are now struggling to make transactions and to get loans because of their inability to access the banking system.

[11] *The Future Of Banking: Regulators To Decide If The Crypto Stars Align For Libra*, S&P Global Ratings, Jun 2019 (https://www.allnews.ch/sites/default/files/files/20190625_SP_Libra_Regulators__Decide.pdf)

[12] https://libra.org/en-US/about-currency-reserve/#the_reserve

Although the goodness of the proposal is hardly arguable, for people to transact Libra will require an internet connection, dedicated apps (WhatsApp, Facebook, Messenger), a smartphone[13] and access to a digital exchange to get the desired coins, at the same time granting the access of personal data to the counterpart.

The credit consequences, from people withdrawing deposits from their bank's accounts to convert them in Libra, would be significant in our view. It is through deposits that banks can purse lending activities; a sharp decrease in that amount would pose tight limits to financial players.

The Regulatory Hurdles

Banking System

If Libra goes beyond enabling a single global currency used to execute a transaction, the whole banking system is up for a complete reshaping.

People not having access to banks are usually those having bad credit histories, not owning an official identification or lacking a permanent address. The know-your-customer (KYC) procedures are in place to prevent frauds arising precisely from these lacks. 1.1 billion people do not own any ID (which is part of the KYC requirements) according to the World Bank data.[14]. Governments should introduce policies to force mass adoption of ID documentation, among others.

Libra does not plan to offer interest on accounts, a lost opportunity for users that decide to store value through it. Moreover, if it were to provide financial services, the Association behind it would need to offer **deposit insurance**, a critical factor for end users. The deposit insurance is an instrument apt at fostering stability and trust within the system.

[13] GSMA data states that 66.53% of the world owns a cell phone (https://www.bankmycell.com/blog/how-many-phones-are-in-the-world)

[14] *1.1 Billion 'Invisible' People without ID are Priority for new High Level Advisory Council on Identification for Development*, World Bank, Oct 2017 (https://www.worldbank.org/en/news/press-release/2017/10/12/11-billion-invisible-people-without-id-are-priority-for-new-high-level-advisory-council-on-identification-for-development)

If no lending activities were possible for Libra, the company could work according to the narrow bank model; that is, it would invest all the money in exchange for the coin in safe assets without being involved in other financial activity. Therefore, the money earned through interests (in a non-negative interest environment) could be given back to coin holders, once all the costs are paid out, and depositors would bear no risk with the narrow bank model. The zero interest and no deposit insurance issues would be then overcome all at once. A severe threat would remain unsolved in our view: are we ready to deal with a too-big-to-fail global entity as it could be Libra?

Money-Laundering, Terrorist Financing, And Tax Evasion

Many initiatives are already enacted to oversee cryptocurrencies:

- ✓ "Under Anti-Money Laundering Directive 5 (AMLD5), virtual currency exchange platforms and custodian wallet providers become obliged entities and cryptocurrencies – via the concept "virtual currencies" – are brought in scope. So, insofar cryptocurrency is held through a custodian wallet provider or transactions occur via a virtual currency exchange platform, there will be information available for the tax administration as the case may be brought to the attention of the tax administration by an FIU reporting a suspicious transaction linked to tax evasion."[15]
- ✓ Financial Action Task Force's (FATF) – an intergovernmental organization that focuses its efforts on fighting money laundering – is strengthening its control over digital currencies to require heightened regulation. New measures will need crypto assets service providers to comply with anti-money laundering and to combat the financing of terrorism.[16]

Some Additional Interesting Information

- ✓ David Marcus, Head of Calibra: founder of Zong (mobile payments company) sold to PayPal in 2011, later President of PayPal and therefore joining Facebook as VP of Messaging Products in 2014. He was also Member of Board of Directors for Coinbase.

[15] *Cryptocurrencies and blockchain – Legal context and implications for financial crime, money laundering and tax evasion*, Robby Houben, Alexander Snyers, Jul 2018, p. 72 (http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf)

[16] https://cointelegraph.com/news/fatf-to-strengthen-control-over-crypto-exchanges-to-prevent-money-laundering

- ✓ Hedera Hashgraph: Libra Governance system's idea is close to theirs, they met Mr. Marcus in early 2018 to speak about their project (full WSJ page to ironically thank Facebook because they say it copied them)[17]. Hashgraph is the only **private** distributed ledger mathematically demonstrated to be Asynchronous Byzantine Fault Tolerant (ABFT), better-protecting from DDoS attacks, network manipulations, and other attacks. This excellent article explains (and demystifies) the facts around Hashgraph.

- ✓ JPM coin is a stablecoin launched in February 2019 that will start trials in 2H19 and pegged 1:1 to USD dollar (fiat currency held by JPMorgan, aimed at speeding transactions). It will run on their Quorum[18]. The token will be transferred via a permissioned distributed ledger, with the possibility to redeem the token for cash through JPMorgan. The coin could serve to settle bonds and commodities transactions.

- ✓ "Another effect of being backed by assets is that it may help lower the risk of high inflation in countries across the world". Nobel Prize-winning economist Friedrich Hayek made this very point in his book "The Denationalization of Money". Hayek believed everyone would be better off if people could pick among distinct types of private money, like Libra, instead of using government-issued money. Hayek believed issuing private money would banish inflation from the world since people would only use the currency most stable in value".[19]

Q&A as a conclusion

1) Will Libra make the ideal coin for those consumers looking to avoid traditional banks and to bypass high transfer fees?

- ✓ It depends on the user's feature - two types of real-world users are depicted in the *Conclusion* section.

2) Will Libra give access to the unbanked around the world?

[17] https://cryptonomist.ch/it/2019/06/24/libra-facebook-hedera-hashgraph/
[18] Enterprise-focused version of Ethereum
[19] https://www.fool.com/investing/2019/06/19/facebook-claims-libra-offers-economic-empowerment.aspx

- ✓ No. Lack of connectivity, KYC documentation, opposition by local governments will hinder the path.

3) Will Facebook be able to overcome the technical and physical challenges of permissionless (open) blockchain?

- ✓ No. The technical capability is missing as of today.

4) Will Libra destabilize central banks?

- ✓ If it reaches wide adoption, yes.

5) Will Libra backers make money out of it? How? A non-profit association should not make money

- ✓ Interest from asset backing will go to the Association. Dividends will be paid to early investors in tokens. More interestingly, non-monetary benefits (e.g., data, customer purchasing through platforms) will go to companies participating in the project, thus "eluding" non-profit rules.

6) What about the "brokerage" fees to convert money in and out of Libra?

- ✓ Calibra is going to be a wallet. The money will trade through other platforms (with fees). Spread may be applied; likely to be reduced to zero because the final aim is to get customers into Libra.

7) What if rules are changed once Libra establishes? Could it print money without any reserves backing it?

- ✓ If the regulated becomes the regulator, public authorities will be overwhelmed by private companies. Once people rely upon your coin, your aim is not to lose their confidence. Everything is theoretically doable until you do not miss the support from the users and do not break legal rules – the key here will be to know by which law Libra is subject to.

8) Why not having a system like WeChat Pay and Alipay where bank accounts are linked to the digital wallets, and the costs range in the 0.1%?

- ✓ Having a unique coin accepted worldwide saves time and costs. Integrating Libra and marketplaces within widely diffused apps (Facebook, Instagram, WhatsApp) would make purchases more immediate. The network of companies behind the project is an invaluable asset.

9) Libra-denominated IOUs might be created (for sure it will as the temptation of doing so would be too strong) that aren't backed by hard assets, eventually creating all the conditions for the next financial crisis

- ✓ Debt instruments and stocks might be issued in Libra, thus creating a new market. If the system is not considered safe, nobody will want to accept it. If it is thought as safe, while being unstable in reality, this could bring to a deep crisis when pitfalls start showing.

Technical Appendix

Some technical explanations are needed to understand what lays behind the newly proposed coin. This section is purposely technical as we believe that to understand what Libra has to offer, one would need to know where it situates concerning vs. the other cryptocurrencies.

The Transaction Models

While consensus in cryptocurrency platforms is necessary to secure the network and validate the state of the blockchain, the transaction model employed by a platform is used to prove ownership of tokens. In other words, it is the mechanism explaining how the ledger must be updated after someone spent coins.

The easiest to understand is the **Account based model** (used in Ethereum and Libra, for instance) which is similar to how traditional banking ledger works: each user has an account with an amount, and this amount is updated once the transfer, deposit or withdrawal is done.

The other model is called the **Unspent Transaction Output model** (used by Bitcoin): instead of having an account, the state of user fund is computed using the history of spent transactions. Going further into its details is not the goal of this research report.

Principle Of Finality

After the number of Transaction Per Second (TPS), the finality describes the time at which a block is considered immutable/reversible. In Bitcoin, there is no finality (i.e., any block could be rewritten), but because the cost of rewriting the entire chain is prohibitive, it is considered probabilistically unfeasible after six confirmations (about 1 hour).

Permissionless And Permissioned

The network of processes participating in the consensus procedure can be configured in permissioned or permissionless setups.

1. **Permissionless network:** in a permissionless network, neither the node identities nor their numbers are known to by other nodes. **In these types of networks, an incentive mechanism must be set up in order**

to avoid cheating, and most particularly, **to resists again Sybil attack**[20]. In Bitcoin, it is called Proof of Work (PoW): by rewarding miner for good behavior, the system protects itself against fool plays.

2. **Permissioned network:** in a permissioned network, the identity and the number of nodes in the network are known to all nodes. Thus, **a node can trust the messages originating from another node** in the same network, and there is **no need for protection against Sybil attacks.** To interact with the network as a client (e.g., user), permission must be granted by a central authority. Such authorities will grant cryptographic material allowing users to send transactions, similar to a basic login system for web apps.

The Libra blockchain will be configured as a permissioned network at launch with a known set of nodes called **validators**. This means all validators in the Libra network know each other's identities.

Consensus

Basic Of Consensus

The consensus is the process for achieving agreement on the next state of a data value within a distributed network. In DLT, the Nakamoto (e.g., bitcoin) and the classical consensus are to be distinguished:

1. **Nakamoto style algorithms**: in this consensus, nodes do not know each other, and therefore, there is no trust among them (the network is then permissionless). Thus, an incentive not to cheat must be set up. This incentive is an "effort" (work, resource, asset, etc.), by which a network member (node) must "invest" to create a new block. At the same time, other network members should be able to verify that the work is done. The presence of this "difficulty" or spent resources, as well as its verifiability, must guarantee the security of the network by increasing the price of the possible attacks. Because of the "longest chain rule," the finality of the block (its immutability) is not immediate. Therefore, confirmations (i.e., blocks) must be waited upon before considering a block immutable/irreversible.
2. **Classical consensus algorithms**: in this class of algorithms, the nodes are known to each other. As such, there is no need for an incentive not to cheat, and the leader is selected randomly, using multiple rounds of message exchanges carrying votes. This type of consensus is well known since the 1980s and implemented in most current decentralized database systems.

In the case of distributed systems, failures may occur. They can be voluntary (cheating) or involuntary (machine or network failure) but, anyway, this will lead to information being not broadcasted, altered or

[20] A single user generates multiple entities to influence the consensus process and for instance, mounts double spend attacks.

deleted; consensus algorithms tolerating this failure up to a certain point are named **Byzantine Fault Tolerance (BFT)**.

The Different Families Of BFT Consensus

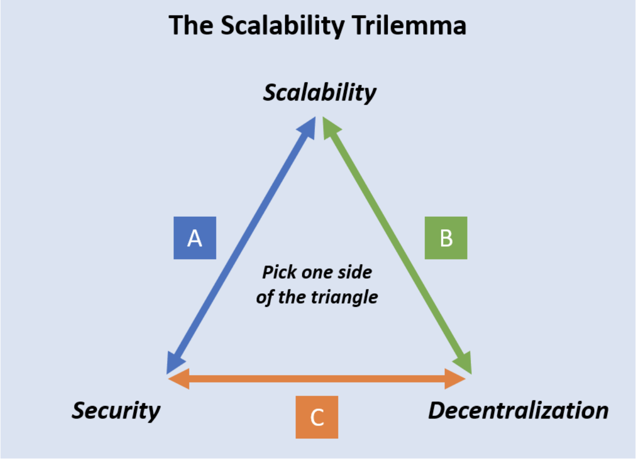
To dig further into the consensus algorithm, **LibraBFT's belongs to the family of classical BFT.** It is based on another consensus algorithm called HotStuff, which in turn borrows some of its consensus logic from another well-known classical BFT algorithm called **Practical Byzantine Fault Tolerance**. What needs to be kept in mind here is that HotStuff offers better performance.

The selection of the leader (i.e., validator that can create and validate the next state) is like the well-known BFT algorithm Tendermint, already in use in cryptocurrencies such as Cosmos. The main difference is that Tendermint assumes that the leader election step can fail whereas Libra does not. In other words, if the validators are reliable, Libra will perform better; otherwise, it will be as performant as Tendermint.

Given the high-cost barrier entry to act as a validator (i.e., the 10 million registration fee to the Libra association and requirements imposed by the Association), we can expect the node (validator) to run in private and highly reliable data centers. As a consequence, Libra will likely perform within the best scenario case (i.e., fail-safe node).

The Trilemma Of Distributed Systems And The Concept Of Scalability

The scalability is the capacity to be changed in size or scale. In regards of distributed systems, it is the capacity of a network to maintain performances (latency, TPS, etc..) while the number of nodes increases.



However, a solution that is scalable in a single dimension (such as the number of transactions or size of the network) may not be well-suited for a use case that requires scaling in a different dimension.

An important concept to keep in mind is that **no consensus algorithm is perfect and suitable for every application**. It goes back to the trilemma of distributed systems stating that you cannot have a network that is scalable, decentralized, and secure, all at the same time. A blockchain that claims to have solved this trilemma has either bent the laws of physics, or it has discovered a breakthrough method that addresses the major blockchain scalability problems that have stumped top mathematicians and computer scientists for the past decade.

This is a very important fact: by design, a BFT consensus algorithm can achieve high scalability and low latency while being secured because of the permissioned (which leads to centralization) nature of its network. In other words, pBFT consensus cannot be implemented efficiently in open networks.

A coin needs to be at least secure and scalable to be used as a mean of exchange. In the current state of distributed system: **Libra has, therefore, no choice than to be centralized,** and it will likely never be otherwise.

To Summarize

Libra is, then, a **permissioned network** running a variant of pBFT (a.k.a. HotStuff). As such, the network promises to achieve 1000 transactions per second. The Libra association want to shift from close to open, which is something never done before.

Libra is different from Bitcoin because of the absence of a chained block: Libra is a cryptographically authenticated database, and its history is a Merkle tree. **There is no "blockchain" in Libra** (blockchain is necessary for a permissionless network where nodes can freely join or leave the network). It is an account-based data model, like Ethereum, and in opposition to the transaction-based data model proposed by Bitcoin. Libra is closer to a **distributed database system** (a signed "snapshot" of Libra account) **maintained by known validators**.

Submitting a transaction and paying a fee, such as the Gas[21] for Ethereum, are required to modify the ledger. Such fee is designed to be low under normal situation and to increase drastically in case of high network usage (e.g., to prevent attacks by the exhaustion of resource also known as Denial of service – DoS attacks); nonetheless, the entity of the fee's smallness is not given.

[21] Unity of fee

Glossary