Facts, Ifs, Buts, and Maybes

Libra: Facts, Ifs, Buts, and Maybes

Jeroen Houttuin

2019-12-23

ABSTRACT

This paper first presents the history and details about Libra, the Libra Association and the Calibra wallet. It then explores the 'Ifs, Buts, and Maybes' around those subjects, aiming to point out critical issues that may still hinder Libra from successfully launching as planned. The aim of the paper is to help the reader understand what the remaining hurdles and challenges for Libra are and make an assessment if Libra will launch early 2020, and if so, what the possible restrictions of such a launch could be.

This paper was originally written as the concluding 'written assignment' for the Certificate of Advanced Studies (CAS Blockchain) at the University of Zurich. The written assignment was submitted and approved on December 9 2019. This newer version includes some additions and spelling corrections.

1 DISCLAIMER

Libra is a very new project and is still in the process of being established. As such, many issues addressed in this paper are highly volatile, and some assumptions made in the early stages of writing this paper (mid-October 2019) may change before publishing it in December 2019. I will try to react to changes to reflect them as they become known, but the Libra environment is changing almost daily at the moment, so I cannot guarantee that all assumptions are completely accurate at the time of reading this paper.

2 INTRODUCTION

In 2009 the Bitcoin network was created and with it the world's first cryptocurrency, bitcoin (lower case b). A major advantage of this cryptocurrency is that anybody can use it without permission, and without trusted third parties, making Bitcoin a typical disruptive technology. Many similar currencies were created in Bitcoin's image, focusing on different areas: whereas Bitcoin's main focus is money, others focus more on fast payments, smart contracts, regional markets, or vertical markets.

A new era started in 2017 when Tether launched its USD-Tether (USDT), the first cryptocurrency pegged to a fiat currency, built on top of Omni and Bitcoin. It allows users to trade between cryptocurrencies and fiat value, without needing a bank account, and in some countries, without creating a taxable event. In the following years, many similar 'stablecoins' were created by various players, for example, USDC, TUSD, EURT, and xCHF. Stablecoins are typically backed by full fiat reserves (although there are other stability mechanisms as well, which are beyond the scope of this paper).

Tech-savvy early adopters are still the main users of cryptocurrencies and stablecoins, as the user experience is still too complicated for mainstream adoption. Some examples of complicating concepts are UTXOs (Unspent Transaction Outputs), gas, and transaction fees measured in Satoshis per byte. In addition, the risk of losing non-recoverable private keys is too high for non-expert wallet users. A further limiting factor is the small number of transactions that most blockchains can handle per second.

Facebook was not quite new to online currencies, as it had already introduced 'Facebook Credits' in 2010, but it had phased this out already in 2012, also because the credits were not widely accepted as a unit of account (note that Libra will face the same issues with acceptance, but probably in the Libra ecosystem prices will be shown in the equivalent amount in local currency).

In May 2018 it became publicly known that Facebook was preparing a cryptocurrency. Marc Zuckerberg had set himself a personal New Year's resolution to better understand decentralization and cryptography ("One of the most interesting questions in technology right now is about centralization versus decentralization. A lot of us got into technology because we believe it can be a decentralizing force that puts more power in people's hands.").

With its 2.4 billion monthly active users, simple user interfaces, 7 million advertisers and 90 million small businesses, it made sense for Facebook to try and tackle the problems that prevented mainstream adoption of cryptocurrencies.

David Marcus, then head of Facebook Messenger (and also former director at Paypal and board member of Coinbase) had laid out the main architecture for a new payment method, this time as a stable cryptocurrency, and convinced Zuckerberg to create a business unit to start building Libra. Libra's proclaimed ideology was to allow financial inclusion of the unbanked and underbanked and its first target applications would be remittances and other cross-border payments.

This culminated in the announcement of Libra, the Libra Association, and the Calibra wallet, in June 2019.

3 FACTS

This chapter presents some facts about Libra, the Libra Association and the Calibra wallet, before addressing the Ifs, Buts, and Maybes. The goal is to set a reference for aspects of Libra that are certain and to enable readers to easily separate them from the Ifs, Buts, and Maybes addressed in chapter 4.

3.1 WHITEPAPER

Facebook announced Libra in a whitepaper on June 18, 2019. The cryptocurrency Libra is scheduled to be launched by the Libra Association, founded in Geneva, Switzerland, at a yet unknown date early in 2020.

To give a brief overview of Libra's goals, I quote from the whitepaper: "Libra's mission is to enable a simple global currency and financial infrastructure that empowers billions of people. This document outlines our plans for a new decentralized blockchain, a low-volatility cryptocurrency, and a smart contract platform that together aim to create a new opportunity for responsible financial services innovation […] This is the goal for Libra: A stable currency built on a secure and stable open-source blockchain, backed by a reserve of real assets, and governed by an independent association. Our hope is to create more access to better, cheaper, and open financial services — no matter who you are, where you live, what you do, or how much you have. We recognize that the road to delivering this will be long, arduous, and won't be achieved in isolation — it will take coming together and forming a real movement around this pursuit. We hope you'll join us and help turn this dream into a reality for billions of people around the world."

Libra is designed as a stablecoin, and the economic power behind the members of the Libra Association is meant to enable wide market acceptance fast. Facebook already has monthly interactions with billions of users, and e-commerce platforms will have a large incentive to integrate Libra, as it will help them save on the current high fees.

3.2 DECENTRALIZATION

In order to become more decentralized, Facebook initiated the Libra Association, with a wide range of large organizations as members, with Facebook being just a regular member. An important reason for using an association was that Facebook considered that it did itself not have enough trust, and wanted to use the already established trust of existing large brands.

The founding members were a diverse group of businesses, non-profit organizations and academic institutions. These 'founding members' had only signed a memorandum of understanding at the time of the Libra announcement – the actual signatures and financial commitments were to follow in October 2019. Members take part in Libra oversight by running a validator node on the network and by participating in the governance of the project.

The founding members, i.e. the initial group of organizations that agreed to work together to finalize the Libra Association's charter, were divided into 6 categories:

- **Payments**
  - Mastercard
  - Paypal
  - PayU
  - Stripe
  - Visa
- **Technology and Marketplaces**
  - Booking Holdings
  - eBay
  - Calibra
  - Farfetch
  - Lyft
  - Mercado Pago
  - Spotify
  - Uber
- **Telecommunications**
  - Iliad
  - Vodafone
- **Blockchain**
  - Anchorage

    - BisonTrails
    - Coinbase
    - Xapo
- **Venture Capital**
    - Andreessen Horowitz
    - Breakthrough Initiatives
    - Ribbit Capital
    - Thrive Capital
    - Union Square Ventures
- **Non-profit and Multilateral Organizations, and Academic Institutions**
    - Creative Destruction Lab
    - Kiva Microfunds
    - Mercy Corps
    - Women's World Banking

Libra's declared goal is to have 100 members (initial list above counts 28) before launching in 2020.

The requirements to join the association can only be fulfilled by large legal entities, e.g. for business members, aspirants must have a market value of more than $1 billion USD or have greater than $500 million USD customer balances. The initial (one-time) membership fee is USD 10 million.

3.3 CRYPTOGRAPHY

On the protocol level, Libra makes strong use of cryptography, and for consensus, it uses a Byzantine Fault Tolerance protocol called LibraBFT. LibraBFT is based on HotStuff [3], a (delegated) dBFT protocol created by VMware Research in 2018. Libra has its own currency with the same name, which is pegged to a basket of fiat currencies, so it can indeed be called a cryptocurrency.

LibraBFT is a leader-based consensus protocol similar to the ones used in NEO and Binance Coin, in which 2/3 (a quorum) of all participating nodes have to agree to reach consensus.

Libra uses an account-based model, like Ethereum. A Merkle tree is used to link individual transactions, so instead of a blockchain, the Libra ledger should rather be considered a transaction chain. This would not scale in a completely decentralized blockchain, but since Libra uses a very limited number (maximum 100) of nodes in LibraBFT, this should scale well even on a global level.

3.4 NODES

The targeted scale of Libra is larger than any existing payment network, and all transactions will be settled on-chain. In the blockchain trilemma (Figure 1), decentralization will have to suffer, as the other factors are more crucial for Libra's success.

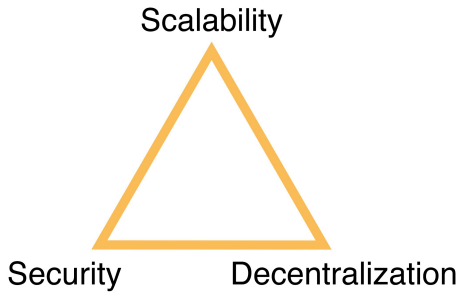

Figure 1. Blockchain Trilemma

The LibraBFT model will work well for this focus on scalability and security, especially if there are less than 100 nodes. Figure 2 shows that BFT protocols, in general, are well suited for Libra.

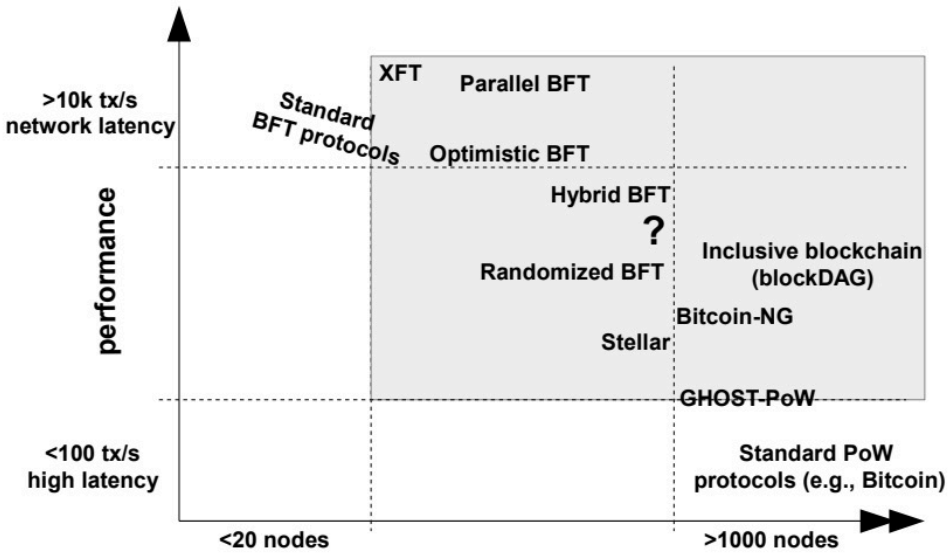

Figure 2. Node Scalability (source: [17])

3.5 LIBRA CURRENCY

The currency 'Libra' is designed to have a globally stable value by being pegged to a basket of stable assets of different kinds and origins. The idea behind this is that although it seems obvious for a US-based company to create a stablecoin that is based solely on the USD, this choice would make adoption more difficult within certain other countries. This is also one of the reasons why the Libra Association was founded in Switzerland.

Another apparent option would have been to peg the Libra to the existing SDRs (Special Drawing Rights), created by the IMF (International Monetary Fund) in 1969 to help balance international payments and prevent national liquidity or debt crises from destabilizing the global economy. Using this well established international 'paper gold' would give more legitimacy to Libra than pegging is to a more arbitrary basket defined by the Libra Association. However, SDRs can only be held by IMF member countries, not by individuals, investment companies, or corporations. Yet in order to keep the value of an SDR-pegged Libra stable, the Libra Association would have to hold its own SDR reserves. Also, SDRs are not backed by a physical reserve, and require trust in the IMF. These factors explain why pegging to the SDR was not a viable option for the Libra currency.

Libra is backed by bank deposits and government securities in currencies from stable and reputable central banks. The initial basket backing Libra will be composed as follows: 50% United States dollar, 18% Euro, 14% Japanese yen, 11% Pound sterling and 7% Singapore dollar. This is an initial proposal, and the Association is still working on the exact composition of the basket [15]. The basket is not planned to be actively managed after the launch of Libra.

3.6 FEES

The Libra Association plans to reduce user fees to a minimum. This fits in with Libra being an association registered in Switzerland, so it is not allowed to have economic goals. For remittances, low fees would mean lower than 3%. For e-commerce, the fees will typically be paid by the merchants and will have to be substantially lower than current credit card fees. This should make Libra more attractive than current online payments for both merchants and customers. Apart from those, Facebook estimates that it has roughly 90 million SMEs as registered users, many of which can currently not do e-commerce at all: they can neither pay for online advertising nor accept online payments. This is also an important target group for Libra payments.

3.7 MONETARY POLICY, ISSUANCE AND DESTRUCTION

New Libra will be minted when fiat money flows into the reserve and burned when fiat leaves the reserve. Libra plans to work with authorized partners and resellers to manage the frontend of this process.

Initially, the tokens will be distributed to the Libra Association members, who can sell or distribute them as they choose, e.g. through authorized resellers, which can themselves be association members.

The Libra Association is not planning to actively manage the mix of its reserves. However, to keep the reserve basket balanced, the reserve will have to trade forex, as different fiat currencies will be added to the reserves in unpredictable amounts. It is currently not clear how this will be done, and by whom. One possibility was mentioned by Christian Catalini from Calibra [15] and depends on the emergence of CBDCs (Central Bank Digital Currencies): if all currencies in the Libra basket are also available as CBDCs, they can automatically be traded against each other to maintain the mix of the reserves.

The association is also not planning to change its basket composition, except under exceptional circumstances. There is currently not a publicly available process for this, changing the mix will be possible as per any process the association sees fit. If one currency in the basket starts suffering from hyperinflation, Libra will not live up to its promises anymore, so the mix will have to be changed. It will even be possible to add different asset classes, such as gold or even bitcoin.

3.8 WALLETS

As Libra is open-source, there will be different wallet applications, both custodial and non-custodial. Initially, the most important wallet will be Calibra, a custodial wallet.

The company Calibra is a subsidiary of Facebook, Inc. It operates independently from Facebook and is headquartered in Menlo Park, CA, USA. Calibra was founded in 2019 with the mission of making money work for everyone globally. It plans to launch its custodial wallet Calibra in 2020. As well as being a standalone app available on iOS and Android, Calibra will be integrated into Facebook platforms such as WhatsApp, Instagram, and Messenger.

Calibra plans to perform full KYC (Know Your Customer) for onboarding users.

3.9 USE CASES

Apart from the apps and social media platforms that will integrate Calibra for payments between users, the following use cases are likely to be built:

- Remittances. Users can use Libra to send money to friends and family abroad.
- Ad payments. Platforms can accept Libra for advertising.
- Ad revenue sharing. Users can receive a part of the ad revenues if they view ads.
- Content paywalls. Micropayment may be required to read quality content.
- Attention rewards. Users can earn Libra in exchange for consuming content.
- Tips. Similar to Likes, users can send each other Libra micropayments as tips.
- P2P Payments. Users can pay each other for various reasons.

3.10 SMART CONTRACTS

Libra allows running smart contracts in a very similar way to Ethereum. It also uses gas as fees for running the contracts, with a specific fee for each bytecode operation. The fees can change depending on the load of the nodes. State variables are stored in the Libra distributed ledger.

One interesting possibility is the creation of stablecoins on top of Libra. Since Libra itself is stable against its basket, this will be easy. As a simplified example, suppose the Libra basket contains 50% USD; then we can accept one Libra to be locked up in a ‘USDL’ stablecoin contract, in exchange for two USDL tokens. The real stability of USDL will be against Libra, but as long as the Libra Reserve doesn’t change the mix of its basket, USDL will be stable against the USD as well. This will have to be explained in the fine print of the contract. The Libra Association could also easily offer such a USDL coin itself.

Smart contracts for DeFi (Decentralized Finance) applications, such as P2P fundraising and lending, are also likely to be developed soon.

3.11 MOVE

Move is a new Turing complete functional programming language, similar to Haskell, specifically developed for Libra. Move is compiled into bytecode, which is then run by stack-based interpreters running on the Libra nodes.

Not only can Move be used for smart contracts, but it was also used to program the management of coins, transaction processing, and validators in Libra.

Move is a language well suited for developing smart contracts and transactions, and since it is open-source, I expect there will be more blockchains built around Move, and even existing blockchains may integrate it. For instance, Ethereum could add it as a new language alongside Solidity and Vyper.

3.12 TESTNET

The Libra Testnet is already available and can be used through a number of wallets:

- Zengo (iOS)
- LibraVista (Web, iOS, Android)
- https://dev.kulap.io/libra (Web, Simulated hardware wallet)

The LibraVista web wallet is the easiest wallet to use for test purposes. Use the Mint function to receive some free coins, and then send them to the Kulap web wallet in order to test basic transactions.

A web-based Libra/Move IDE, similar to Remix for Ethereum, is available for developers: https://libraide.com/

There are also a number of transaction explorers (we cannot call them block explorers, as there are no blocks) for Testnet:

- https://libexplorer.com
- https://librabrowser.io/
- https://libraview.org/
- https://librachecker.com/

Of these explorers, Libexplorer is the most verbose and intuitive. My first tests with the wallets show that transactions are extremely fast, especially considering that each transaction is final, as there is no blockchain to provide block confirmations.

Basic transactions are currently free on Testnet. Gas prices may fluctuate, depending on existing demand; so on Mainnet transactions will probably not be free, although Libra aims to charge ‘low’ fees.

The availability of the Libra Testnet and various tools for it show that the Libra technology is ready and will not be a hindrance for a successful Libra launch early 2020.

3.13 REGULATION

Unlike Bitcoin, Libra is run by a legal entity, and will thus have to comply with laws and regulations in every country in which it operates. Libra is most actively seeking regulation within the US, which is demonstrated by the 2019 congressional hearings of both David Marcus and Marc Zuckerberg.

Apart from the US, Switzerland is also a top priority for Libra to seek regulation from, as the association is registered in Geneva. Here is a quote from the Swiss Federal Council addressing Libra: “The supervisory authority Finma announced on 11 September 2019 that, based on the information available, the project would be classified as a payment system and a corresponding licence would be required. Consequently, it would automatically be subject to the Anti-Money Laundering Act and international standards in this area.” Thus Libra is also actively seeking approval from Finma, which is well prepared to accept Libra, as in its 2019 supplement to the ICO guidelines [24] it added a new category for stablecoins, with a sub-category for stablecoins that are ‘linked to a basket of fiat currencies’.

Libra can be seen as part of a trend where big tech companies are moving into finance, such as the already existing Apple Pay, Samsung Pay, Amazon Pay (plus many other Amazon fintech services) and Google Pay, which are payment services that work together with credit card companies and banks. In November 2019, Facebook announced Facebook Pay (and Google announced that it will even go one step further and aims to become a bank). In diversifying, the above payment systems also start to threaten the existing banks, but regulators and governments have been accepting them so far. Libra is a step up from these services, in that it doesn't only provide financial services, but also a new currency, thus creating a larger threat to banks, central banks, and governments. Marc Zuckerberg explicitly called Libra a 'payment system' though at the congressional hearing, when asked about the need to regulate it as a bank. To which congressman Perllmutter replied ' I am not sure you guys understand what it is' [4].

Apart from the regulators in the US and Switzerland, all custodial wallets will have to comply with regulations in each country in which they operate.

One important issue that regulators are afraid of is how Facebook has handled user privacy so far [4]. Facebook has pledged that it would not share personal data of its users with Libra, but the sharing can still happen the other way around, i.e. Calibra can link KYC'd user identities to Facebook users, which will be valuable information, and may be a hidden incentive for Facebook to push Libra and Calibra.

3.14 KYC / AML

KYC and AML (Know Your Customer and Anti Money Laundering measures) will be done on the 'edges' of the network, e.g. by custodial wallets, authorized resellers and exchanges. The Libra Association is currently working on a framework to assist those edges in implementing the KYC/AML processes.

For areas where people often do not have the necessary paperwork for KYC, the Libra Association is working on new identity services, which could also be based on existing business relations such as cell phone contracts. In extreme cases, such as refugee camps, there may be a special role for NGOs (Non-Governmental Organizations) as trusted intermediaries to assist in KYC. NGOs can also help in educating people on how to use non-custodial wallets, which do not require KYC.

If KYC will always be done on the on- and off-ramps, Facebook and other association members can push adoption by handing out Libra to users without KYC, e.g. as reward tokens, which can be exchanged for Libra later. This way, Facebook can push mass-adoption of Libra very fast.

[Last minute addition 2019-11-14] On 2019-11-13 Facebook announced that it will integrate a new service 'Facebook Pay' in its Facebook and Instagram platforms. This service will initially only be available for US-based users, but it may be a step in the direction of the scenario described in the previous paragraph.

3.15 DRIVING BLOCKCHAIN ADOPTION

Libra has the potential to drive global acceptance of blockchain services at an enormous scale. Whereas there currently exist roughly 45 million Bitcoin wallets and 12 million active Bitcoin users, Facebook can reach 2.4 billion people through Facebook and Instagram (3 billion if we include Whatsapp). Libra will very likely also be tradable against other cryptocurrencies on exchanges, so the barrier for billions of people to start owning major coins like BTC or ETH will be lowered extremely. Even if a small percentage of Libra users would decide to try out Bitcoin, the number of active Bitcoin users would grow dramatically.

3.16 CENSORSHIP

According to the whitepaper, all Libra transactions stored in the ledger transactions are final, as they are tied into each other with a Merkle tree (although we will see in chapter 4 that transactions will not be as final as the whitepaper says they are).

3.17 FORENSICS

Anonymous Libra accounts can be made by anyone, anywhere, as with other cryptocurrencies based on public-key cryptography. As long as anonymous accounts are used for payments of goods and services that require no

KYC, an anonymous community can evolve and flourish within the Libra ecosystem, creating a Libra internal market.

Forensics will become important if this internal market is used for illegal goods and services. Libra is an account-based blockchain, so forensic tools similar to those used for Ethereum can be used. I expect that law enforcement agencies worldwide will use such tools to detect illegal use, and try to force Libra to take action where needed. As every jurisdiction has its own definitions of what is illegal, there will be many cases where Libra will not take such requested action. In these cases, such Libra accounts will probably be published on blacklists, which will imply a challenge for Libra to maintain fungibility.

4 IFS, BUTS, AND MAYBES

Whereas I listed facts about Libra in chapter 3, this chapter will present aspects of Libra that are still unknown, uncertain, ambivalent or problematic. Such information will be important for any party that plans to get involved with Libra: users, developers, association members, banks, payment gateways, exchanges, law enforcement, and regulators.

4.1 WHITEPAPER

The whitepaper as published on libra.org is neither dated nor versioned. When in doubt about changes, we'll have to use a web archiving service such as web.archive.org to compare to the original version. At the time of writing this paragraph (2019-10-28), the downloadable PDF version of the whitepaper does show a revision date 2019-10-13, so the whitepaper appears to be a living document, albeit in a hidden way.

Versioning would be of particular importance when seeking regulation, as regulators are unlikely to base their decisions on a 'moving target'.

It is hard to explain why Libra did not do this from the start, but probably versioning will be added retrospectively, possibly even before the publication of this paper.

4.2 LIBRA ASSOCIATION

The declared goal of the Libra Association is to attract 100 members before Libra launches (although Calibra's main economist Christian Catalini has said that 60 would also be sufficient [15]). At the time of writing, they have however lost a quarter of their founding members, and have not attracted new ones so far. The following members have left:

- **Payments**
  - Mastercard
  - Paypal
  - Stripe
  - Visa
- **Technology and Marketplaces**
  - Booking Holdings
  - eBay
  - Mercado Pago

Especially members of the Payments category have left Libra. These companies rely highly on good relationships with banks, and those same banks have reason to fear being disrupted by Libra, so it seems likely that the banks exerted pressure on those members to leave Libra, although this is difficult to prove. What is known for certain is that some politicians (probably subject to lobbying by banks – although it is again difficult to prove a direct correlation) applied pressure on those Payment members as well: US senators Sherrod Brown and Brian Schatz threatened Mastercard, Stripe, and Visa, in writing, with increased scrutiny unless they left Libra. Shortly after these threats, these companies did leave the Libra Association.

On 2019-10-15, the Libra Association announced that over 1,500 entities had indicated interest in joining the Libra project effort and that approximately 180 entities have met the preliminary membership criteria. Note that 'interest in joining the Libra project effort' does not mean they actually plan to join the association, and

'meeting membership criteria' does not mean they applied for membership. No new members have been added to the association since its inception. A major incentive for joining the association is that members can profit from the enormous reach of Facebook through Libra, yet so far no new membership applications have been made public.

As for Libra membership, it is currently not defined what will happen if a member does at some point not fulfill the membership criteria anymore, or how and under which circumstances the members could expel other members.

Facebook's huge role in Libra appears good for the project, but it is probably also its biggest weakness. Governments and regulators associate Libra with Facebook, and Facebook with privacy scandals such as leaks and the Cambridge Analytica affair. Facebook cannot count on enough goodwill, and the project might have had better chances if the main driver had been a different company. At the congressional Libra hearings with Marc Zuckerberg this became very clear. Zuckerberg opened with the following disclaimer: "We've faced a lot of issues over the past few years, and I'm sure people wish it was anyone but Facebook putting this idea forward". Members of congress only used roughly half of the time to ask about Libra, the other half was used to vent frustration about both Facebook and cryptocurrencies in general.

Facebook has declared that if one association member would become a single point of failure, i.e. Libra would be at risk if one member left, then the project would not have been designed right [15]. However, Facebook's role is still so central and crucial, that Facebook leaving would very likely make Libra fail. Libra's goal is to change this dependency as soon as possible, but this is not likely to happen before Q3 2020.

Another unknown factor is that the Libra association governs itself, and can thus change its consensus rules at any time. This may affect the rules and composition of the association itself, its partners, the protocols, and the mix of the Libra basket.

4.3 CRYPTOGRAPHY

There is no concept of a block of transactions in the ledger history. The consensus protocol batches transactions into blocks as an optimization and to drive the consensus protocol. However, in the logical data model, the transactions occur in sequence without distinction as to which block contained each transaction.

Strictly speaking, Libra does not use a blockchain, but it calls its database of transactions the 'Libra Blockchain', and since using the word Blockchain is not regulated, this is perfectly legal. The word 'blockchain' was first used to describe the Bitcoin ledger, but even in the Bitcoin whitepaper, that word is not used. Instead, it mentions a chain as a sequence of linked blocks.

As the word blockchain became very trendy in 2017, many companies started adding it to their brand names, often maliciously and malapropos. For Libra, using the word blockchain is not completely wrong, as they do validate blocks of transactions, but those blocks are not chained, so I do consider the word blockchain at least misleading. This explains why many experts consider Libra not a blockchain, and some even not a cryptocurrency.

4.4 DECENTRALIZATION

Facebook seems to be the Achilles heel of Libra, as it was crucial for its development, and it can onboard billions of users. If Facebook would leave the Libra Association, and removed Libra functionality from its user interfaces, it is hard to imagine that Libra could survive. Facebook is thus Libra-internally too big to fail. Yet there are some very likely scenarios that would force Facebook to leave. Consider the following example:

What happens if a so-called quorum (2/3 majority of nodes) approves a transaction that is illegal according to the regulation Facebook succumbed to in the US? This is very likely to happen sooner or later. As an example, consider sending a remittance to a relative in Iran, which may be perfectly legal in Switzerland, where the Libra Association is registered, and also in the home countries of a majority of the other Libra Association members, but for US-based Facebook and Calibra this would be illegal. The logical consequence for Facebook (Calibra) would be to either leave the association, force its will upon a quorum of the other members, or face the legal consequences in the US.

What can also happen is that governments, banks, or regulators exert pressure on a quorum of Calibra node operators in order to freeze Libra accounts. Since Libra is account-based, it is easy to block certain accounts. Even if users create their own accounts with independent Libra software, the nodes can still ban them from using Libra.

4.5 CALIBRA WALLET

Libra wants to supply payment services to billions of un- and under-banked people. One dilemma with this is that Calibra is a custodial wallet and will KYC its users, but many of the world's unbanked will not be able to pass the KYC process, due to missing identification papers.

Since Libra is an open-source project, it is to be expected that there will be third-party wallets as well, some of which will not enforce KYC. As a result, Libra's fungibility is not a given, as not all accounts are 'created equal'. As for other Libra Association members and authorized resellers, they may enforce strict KYC on exchanges and on- and off-ramps, but when an internal Libra market evolves, or P2P trading becomes more widespread, the association is likely to lose control of the effectiveness of its KYC.

Marc Zuckerberg has testified before US Congress that Facebook or Calibra will always reimburse its users if they lose money due to scams, hacks or extortions. It will, however, be impossible for Facebook and Calibra to do this for users who use other Libra wallets, e.g. on exchanges. This was not mentioned at the congressional hearing, but depending on the size of the Libra ecosystem outside Calibra, it can turn into a large problem, which Facebook is not responsible for, and neither are the other members of the association. Libra will work with authorized resellers and exchanges, but the conditions for this authorization are not yet published. Apart from that, there will also be users of non-custodial wallets and unauthorized exchanges, whom Facebook will not be able to assist in case of fraud.

4.6 NODES

All Testnet nodes but one are currently based on Calibra software. Bison Trails is running the first non-Calibra validator node since late October 2019. Theoretically, each association member could develop its own node software, but there is no immediate incentive to do this. The node software is open source, but this setup does leave a majority of power in the hands of Facebook, through Calibra. The latest published roadmap by Libra is shown in Figure 3 below. The roadmap does not show dates, but considering the Testnet is live, we should at least be in phase 2 at the time of writing. This means that the 'Calibra Involvement' should now be at most 25%. The Involvement metric itself is not defined and looking at the planned future numbers, it does certainly not represent Calibra's representation percentage among the members. If it means the percentage of Calibra nodes on the network, the number would also be way off. The same would hold true if it meant the percentage of Calibra engineers among all engineers working on Libra. From what we can see now, the power of Calibra within the Libra project, by any measure, is still very high.

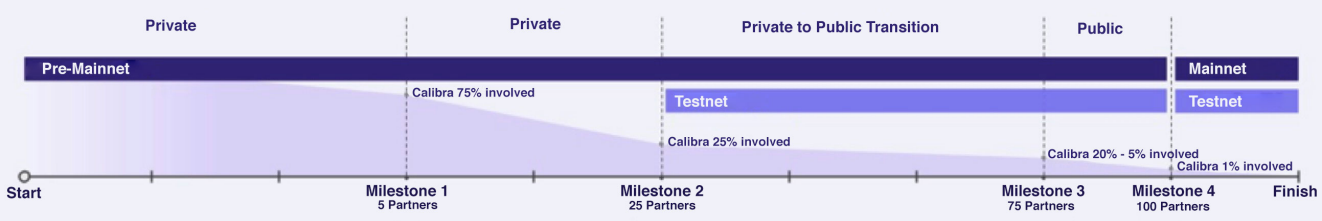

Figure 3. Libra Roadmap (source: [18])

Libra also encourages node operators to run nodes on AWS (Amazon Web Services). This could put 2/3 of the nodes under control of Amazon, which is itself not part of the association, but Amazon would then control a quorum and could censor transactions from being accepted by the network, potentially in a covert way, i.e. add delays to the elected leader node.

4.7 LIBRA AS MONEY

Libra is best compared to existing stablecoins, such as USDT or xCHF, but it is pegged to a basket of assets instead of one particular currency. As a result, it creates a new **unit of account**, which may be a hurdle for wide acceptance, although it is possible that merchants will show all prices in the local currency equivalents, and only show the corresponding Libra amount at the moment of payment.

As a **medium of exchange**, Libra is well suited, but only when its users are online, which will be an important handicap in especially those geographic areas where Libra aims to help the unbanked. It is possible that Libra will develop solutions that work on cheap smartphones per SMS as well, but no plans have been announced so far.

As for the **store of value** property of money, Libra is designed to be stable against a basket of stable fiat currencies. This sounds stable, but it also means it is as prone to inflation as the currencies it is stable against. This is an important distinction from major cryptocurrencies such as Bitcoin, which are often used as a speculative hedge against inflation. This is not a problem for the majority of potential Libra users, as they think in terms of fiat money anyway. I'm mentioning it here because Libra is often compared to Bitcoin when people first hear about this new cryptocurrency, in that they ask themselves (or me) if they should rather 'invest' in Libra than in Bitcoin, which is an irrelevant question - bitcoin can be used for speculation, whereas Libra is meant to not fluctuate in value, but is designed as a stable currency on the Libra payment network. If any fiat currency in the Libra basket suffers from inflation, so will Libra.

Competition comes from central banks planning to issue digital currencies, such as China's DCEP (Digital Currency Electronic Payments) and other CBDCs (Central Bank Digital Currencies), such as Fedcoin (nickname) by the US Federal Reserve. China has already announced that it will launch its DCEP before or during Q1 2020, whereas Fedcoin is only a rumor so far, but it could be implemented quickly, especially if the Fed sees a need to react to China's DCEP. Such currencies could be a threat to Libra, as they can easily be integrated into existing online payment gateways, but they will lack the global appeal and ease of integration into global social networks, so it is likely that they will rather be integrated into more regional apps only.

Bitcoin will also be a threat to Libra. It was not mandatory for Facebook to create its own cryptocurrency. They could also have chosen to integrate Bitcoin plus second layer solutions such as the Lightning Network, or even re-brand the old Facebook Credits as Bitcoin IOUs (I Owe You). Jack Dorsey, CEO of both Twitter and Square, is openly a fan of Bitcoin and has declared that Twitter will never integrate Libra. Square's Cash App has already integrated bitcoin.

4.8 LIBRA RESERVE

Libra is pegged to a basket of stable assets of different kinds and origins. This introduces a vulnerability to Libra in that it requires trust in the custodians of those assets, which will typically be banks, and in case of a bank collapse, Libra's value would collapse with it proportionally, which makes it less stable than the currencies it is pegged to. The only alternative will be to use a full reserve bank, which is hard to find, charges high fees, and will become a honey pot risk considering the amounts of fiat it would have to keep in vaults.

As mentioned earlier, Libra is designed to be stable, but all currencies in its baskets are currently inflating, so Libra can only be as stable as its basket currencies. In that sense, it would have been a logical step to add gold to the basket, as gold's buying power has made it the most stable asset for thousands of years. The fact that Libra did not decide to add gold shows that its focus is on being a payment network (medium of exchange) rather than a store of value.

4.9 REGULATION

Germany and France have already indicated in September 2019 that they plan to ban Libra, as they consider it a risk to the current financial and monetary systems. On October 31st, news broke that the 5 largest Eurozone economies (FR, DE, ES, IT and NL) will work together to ban Libra within their borders.

In the 2019 congressional hearing of Marc Zuckerberg, he pledged that Facebook would not help launch Libra anywhere in the world, as long as it was not fully approved by all regulators in the US. This creates a number of pitfalls:

- Regulators in the US are known for working slowly. The SEC has, on a number of occasions, postponed taking a decision about allowing a Bitcoin ETF. Some of them were denied by the SEC just before the final deadline, others were withdrawn just before the deadline. After more than 2 years, no Bitcoin ETF has been approved yet. As the scale of Libra is much larger than Bitcoin, it is unlikely that the SEC will wave it through before the planned launch in 2020.
- There are many regulators in the US, and they have partly conflicting interests. As an example, the IRS, the CFTC, and the SEC have been divided for many years on the simple question of whether bitcoin is a currency, a security, or a commodity. Depending on the answer to this question, different regulators may be responsible for Libra, possibly in parallel.
- Seeking full US regulation before launching Libra anywhere in the world may in some countries be perceived as US 'lawfare', hindering global acceptance.
- If Libra grows to a size that would make it of systemic importance, i.e. becomes a SIFI (Systemically Important Financial Institutions) or even a G-SIFI (Global SIFI), it would also have to be regulated by the Federal Reserve/OCC (Office of the Comptroller of the Currency) retrospectively. The main criterion for this regulation is a stress test, which should not be a problem for a fully backed SIFI though.
- 'Helping to launch' leaves a lot of room for interpretation. Smaller association member could launch Libra, without the help of Facebook, which could then start integrating Libra at a later stage.

For some countries, Libra will impose a threat (China in particular), especially if it becomes a widespread payment method, which would imply a free flow of capital. According to the Impossible Trinity (Figure 4), this means that such countries might lose either their fixed exchange rates or their sovereign monetary policy.

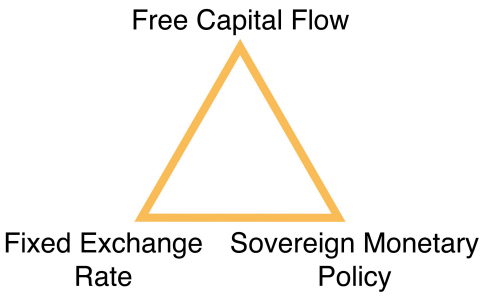

Figure 4. Impossible Trinity

For most developed countries, this will not be a problem, as they already have free capital flows, but in the case of China, it imposes a real threat for having control over their own money. Even though China does not allow its citizens access to Facebook and Instagram, Libra could still be used through non-custodial wallets. It should be noted that China is already slowly losing this control. So far, China has worked around the impossible trinity by creating two currencies - the offshore- and the onshore-Yuan - assuming they could block free capital flow for the offshore-Yuan. Tether, however, created a stablecoin called the CNH₮ in 2019, which is pegged to the offshore-Yuan, and this stablecoin can freely flow into China as well. Libra will be easier to ban than the more decentralized CNH₮ though, as the Chinese authorities would only have to block access to the shortlist of Libra nodes.

4.10 BANK RELATIONS

It is probably not a coincidence that there are no banks in the Libra Association, as Libra is planning to disrupt the banks.

ING CEO Ralph Hamers explained that institutions like ING have to guard the financial system to prevent criminal activity and may be bound to stop working with social media giant Facebook if the firm launches Libra. At this point, it is unclear what criminal activities Mr. Hamers is referring to. It seems likely though that most banks will be very reluctant to work with individual association members, Libra partners and resellers, and even the Libra Reserve.

4.11 PRESSURE ON SWITZERLAND

Larger countries and international organizations could put political pressure on Switzerland as the home of the Libra Association, in order to make Libra comply with their wishes, making the behavior of the Libra Association 'unpredictable'. Similar situations have happened before, e.g. in the case of the USA, UK and EU applying pressure on Switzerland to loosen its banking secrecy.

4.12 CENSORSHIP

Transactions sending Libra to a custodial wallet can easily be reversed, as the receiving custodian controls the private keys.

The Libra Association can also keep a blacklist of addresses, to which they will not allow Libra to be sent, or even to be sent from. Individual nodes can also keep their own blacklists, and block a transaction if they have a blacklist quorum for an address.

But even for transactions that cannot be reversed or stopped as shown above, the Libra Association still has technical means to reverse transactions. Since reaching consensus in LibraBFT is cheap compared to other consensus mechanisms such as Proof of Work, and the nodes are under the centralized control of the association, a quorum subset of the nodes can decide to undo an old transaction and reorg the ledger after that transaction. Depending on how long ago this transaction took place, it will take some time to rebuild the ledger after that transaction, which would lead to delays for current transactions in the mempool, but creating the reorganized ledger can be done in the background (similar to shadow mining in PoW systems), and once this is done, the reorganized ledger can be written to the database, and then the transactions that took place during the reorg calculations can be added again.

Although such reorgs are possible, it should be noted that they would completely undermine the trust in Libra, and therewith its usability in commerce.

It is currently not defined if and how the Libra Association will deal with independent smart contracts running on Libra. It is possible to create assets and services on top of Libra, using the Move language, and those assets and services may contain illegal aspects (e.g. unregistered securities or dark market goods and services).

Libra is thus not immutable or censorship-resistant, due to the centralization of the association and the nodes.

4.13 COPY CATS AND COMPETITORS

Considering the number of coins cloned off of Bitcoin, and with Libra being an open-source project, it is only a matter of time before people will create clones of Libra, probably trying to improve on certain aspects of it. Some possibilities for this would be:

- Integrate Proof of Work instead of LibraBFT and fork the ledger. This 'powLibra' would have its own unpegged currency, and free coins will automatically be given to all Libra holders at the time of the fork. It will be interesting to see how custodial wallets will deal with this situation. When this happened to Bitcoin through the creation of Bitcoin Cash, many custodians were reluctant to hand out the Bitcoin Cash to their users, but most did so in the end. In the case of Libra, they will be even more reluctant, as powLibra will be seen as an attack on the custodian and Libra itself, and it would result in loss of control regarding KYC/AML on the new chain.
- Another possibility will be to create a new chain with an airdrop, in which existing Libra holders, but possibly also holders of bitcoin or other coins, can claim free new coins.

There will also be competition for Libra from outside the crypto community, especially from central banks. This is what Marc Zuckerberg warned against in the congressional hearing in October 2019 [4], especially concerning China. Two days after the hearing China announced its CBDC. Tunisia has already launched its stablecoin E-Dinar (built on the Universa Blockchain), and Venezuela launched the Petro cryptocurrency in 2019 (not a fiat stablecoin). Other countries working on CBDCs and stablecoins are Sweden, Canada, Singapore, the Bahamas, the Marshall Islands, the British Virgin Islands, Uruguay, Ghana, Thailand, the UAE and again Venezuela. Different companies and agencies in the US, Hong Kong, Turkey, France, and Germany are also discussing CBDCs, but those countries have not announced concrete plans yet.

Even private bank JPMorgan Chase is planning its own JPM Coin, based on Ethereum and Microsoft Azure. JPM Coin is scheduled to launch late 2019. Private banks are threatened by cryptocurrencies, stablecoins, and even CBDCs (which will probably be limited in supply by the central banks, i.e. can not be created as needed by private banks), so it is likely that other banks are working on similar projects. Ripple's xCurrent is another example in which (more than 200) financial institutions are jointly aiming to build an alternative payment and settlement network.

As for the unbanked and underbanked, there is already competition from both m-pesa, a branchless banking service based on SMS, already operating in eight countries in Africa and Asia since 2007, and similar services like bKash in Bangladesh. In 2019, bKash started a partnership with Ripple to add remittances to its portfolio. Since 2018, there is also a cryptocurrency called Electroneum (ETN), designed specifically for the unbanked, that lets smartphone owners store, send and receive digital funds, without a bank account. Finally, the unbanked can also use any existing cryptocurrency wallet on their smartphones, without KYC. The wide range of existing stablecoin wallets will be a good choice for this, but also regular cryptocurrencies will work. All competitors in this paragraph lack the potential of fast mass adoption though. The reach of especially Facebook is a large advantage for fast adoption, but large central banks also have a large potential to drive adoption through CBDCs.

5 WILL IT LAUNCH?

It is hard to predict if Libra will launch, and even many experts disagree on it. However, there are different dimensions that can be considered about the launch: Will it launch as planned? If not, which factors can be changed to at least launch at all? This translates to the following questions: When will it launch? Will the Libra association have 100, or at least 60, members at the launch date? Will Facebook be involved? Where will it launch?

None of the above questions can, of course, be answered with certainty at this time, but they can be addressed separately, which is what I will do in this chapter. I will also add my own predictions, taking the 'Ifs, Buts, and Maybes' of the previous chapter as input.

5.1 LAUNCH AS PLANNED?

This is probably the easiest question to answer, and my clear prediction is no. It is very unlikely that Libra will launch as planned, early in 2020, integrated in Facebook and Instagram, worldwide, with the Libra Association having 100 members, and with full approval from all US regulators (let alone from all regulators worldwide).

The easiest part for launching as planned is probably the technology; looking at the technical documentation and the tools already available for the operational Libra Testnet, this will not be a bottleneck. Regulation will be the most difficult part and will have influences on timing, the association and its members, and the jurisdictions in which Libra can be launched.

5.2 LAUNCH WHEN?

With the amount of CBDCs and other stablecoins currently under development, it is important for Libra to be launched as soon as possible, which can probably be in the first half of 2020, as originally planned, depending on the concessions Libra is willing to make.

5.3 LAUNCH WITH HOW MANY MEMBERS?

Libra aims to be as decentralized as possible at the launch date and to decentralize even further after the launch. To make this claim credible, the Libra Association urgently needs at least 40 new members. As no official membership applications have been announced yet, I expect the association to lower the bar for membership soon (e.g. from 10 to 5 million USD, or introducing new types of membership), and to be able to reach a total of at least 50 or 60 members by mid-2020, which it will consider enough for a launch.

Facebook (Calibra) itself is crucial for the credibility of Libra, so it cannot realistically leave the association.

5.4 LAUNCH INVOLVES FACEBOOK?

Marc Zuckerberg pledged in he US congressional hearings that under certain extreme circumstances, Facebook would leave Libra. As mentioned above, I think this would be fatal for Libra's credibility and success, but it is worth looking at Zuckerberg's exact words. His main pledge was that 'Facebook will not be part of launching the Libra payments system anywhere in the world until US regulators approve' [25]. These words offer an important loophole. Facebook itself is not a member of the Calibra Association (although its subsidiary Calibra is), so Facebook can stay passive and let the association launch Libra, and then integrate Calibra into its services later. I expect this will be the way that Libra will launch, allowing Zuckerberg to remain true to his pledge, and still let Libra launch.

5.5 LAUNCH WHERE?

A typical success formula for start-ups is: 'first dominate a small market; then scale and expand. This is the way that Facebook itself started, and Facebook also uses this strategy for other services, such as the new Facebook Pay, so I think it is likely that Libra will start this way as well. New services are typically introduced in a small number of countries. For Libra, the US and Switzerland are important countries. The US is difficult to get fast approval from the regulators, and will probably have to wait until the pressure from citizens becomes high enough, but Switzerland will be easy, as the new stablecoin supplement from Finma ([24]) seems tailor-made for Libra. I thus expect Libra to launch in Switzerland first, followed closely by other crypto-friendly jurisdictions, such as Malta, Japan, and a number of countries in Africa and Asia.

6 CONCLUSION

Libra currently acts as a catalyst for the entire blockchain ecosystem. It raises awareness of cryptocurrencies, stablecoins, corporate coins, and CBDCs, and also brings attention to the shortcomings of the current monetary and financial systems, especially toward the unbanked and underbanked. As Libra has the potential to become a disruptor of those current systems, it will keep facing stiff opposition from those who have the most to lose: banks and governments, especially those in the western world.

Potential Libra users should be aware that Libra will not be playing the same role as cryptocurrencies such as bitcoin: Libra will not be censorship-resistant and can be frozen at the will of the association (possibly under pressure of banks and governments), and it will not be a hedge against inflation, let alone a speculative store of value.

Concerning the launch, I will conclude with my personal prediction, which is that Libra will launch in a small number of countries, one of which will be Switzerland, before Q3 2020, with Facebook initially playing a passive role. It will then quickly expand to more countries, and Calibra will be integrated into Facebook and Instagram for users in those countries, with the USA not being among the first. This is a personal prediction based on my research for this paper, and I expect some readers to reach different conclusions.

I do hope and expect that Libra will launch in some form in 2020, and I think it will be an important boost for the entire blockchain, FinTech, and DeFi ecosystems.

7 REFERENCES

[1] Libra Association, 2019: "Libra White Paper - An Introduction to Libra".

[2] Basel Committee on Banking Supervision, 2011: "Global systemically important banks: assessment methodology and the additional loss absorbency requirement".

[3] M. Yin, D. Malkhi, M. K. Reiterand, G. G. Gueta, and I. Abraham, 2019: "HotStuff: BFT consensus in the lens of blockchain".

[4] US Congress and Marc Zuckerberg, 2019-10-23, "Mark Zuckerberg Testimony Transcript".

[5] Satoshi Nakamoto, 2008: "Bitcoin: A Peer-to-Peer Electronic Cash System".

[6] Zachary Amsden, Ramnik Arora, Shehar Bano et al, 2019: "The Libra Blockchain".

[7] Shehar Bano, Mathieu Baudet, Avery Ching, Andrey Chursin et al, 2019: “State Machine Replication in the Libra Blockchain”.

[8] Sam Blackshear, Evan Cheng, David L. Dill, Victor Gao et al, 2019: “Move: A Language With Programmable Resources”.

[9] Calibra, 2019: “Customer Commitment”.

[10] Calibra, 2019: “Commitment to Compliance and Consumer Protection”.

[11] Libra Association, 2019: “How to Become a Founding Member”.

[12] Christian Catalini, Oliver Gratry, J. Mark Hou, Sunita Parasuraman, Nils Wernerfelt, 2019: “The Libra Reserve”.

[13] Swiss Federal Council, 2019-10-15: Press Release: “Federal Council informed of current status of stablecoin debate”.

[14] Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner, 2019: “Regulating Libra: The Transformative Potential of Facebook’s Cryptocurrency and Possible Regulatory Responses”.

[15] Christian Catalini on Laura Shin’s Unchained Podcast, 2019-11-05: “A Libra Co-Creator on How Facebook Will Make Money From Calibra”.

[16] Kevin Helms, 2019-08-15: “Central Banks Worldwide Testing Their Own Digital Currencies”.

[17] Marko Vukolic, IBM Research Zurich, 2016: “The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication”.

[18] Libra Association, 2019-10-02: “September Libra Developer Update - Roadmap #1”

[19] CNBC, 2018-05-08: “Facebook shakes up its execs and adds new blockchain group”.

[20] IBM & OMFIF, 2019, “Retail CBDCs - The next payments frontier”.

[21] Board of Governors of the Federal Reserve System, November 2019: “Financial Stability Report”.

[22] fortune.com, 2019-11-20, “PayPal CEO Dan Schulman Reveals Why He Withdrew From Facebook’s Libra Project”.

[23] Eric Wall, 2019-11-20, “Privacy and Cryptocurrency, Part IV: Stablecoins— Blacklists and Traceability”.

[24] Finma, 2019-09-11: “Supplement to the guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)”.

[25] Marc Zuckerberg, 2019-10-23: “Testimony for the Hearing Before the United States House of Representatives Committee on Financial Services”.