Master Thesis

The Digital Transformation of Payment Systems - Libra's Impact on the Global Economy

Enzo Mesanovic

2013-054-499

Submission date: 06 January 2020

Supervised by:
Prof. Dr. Fabian Schär
Credit Suisse Asset Management (Schweiz) Professor for
Distributed Ledger Technologies and Fintech
Center for Innovative Finance, University of Basel

Abstract

This master thesis examines the conceptual and technical specifications of Facebook's Libra project, which provides a comprehensive understanding of the fiat-backed digital currency, the payment system and financial infrastructures for billions of people to be launched in the first half of 2020. The results demonstrate that Libra could potentially accelerate financial inclusion and improve services within the network, but current drawbacks such as the permissioned blockchain and centralized network limit user participation, and resistance from governments, regulators and legislators underlines the disruptive nature of the project, which, if accepted globally, could have a significant impact on the global economy.

Keywords: Blockchain, Digital Currency, Facebook, Libra
JEL: E42, E58, G28, L86, O33

Contents

Plagiarism Declaration

With my signature, I certify that the information I have given about the tools used in the preparation of my work and about the assistance I have received is true and complete in all respects. I have read the information sheet on plagiarism and fraud of 22 February 2011 and am aware of the consequences of such action.

Enzo Mesanovic

List of Figures

List of Tables

List of Abbreviation

AML	Anti-Money Laundering
BFT	Byzantine Fault Tolerance
CHF	Confoederatio Helvetica Franc
CFT	Combating the Financing of Terrorism
DAO	Decentralized Autonomous Organizations
DLT	Distributed Ledger Technology
DoS	Denial-of-Service
DPOS	Delegated Proof-of-Stake
EdDSA	Edwards-curve Digital Signature Algorithm
EU	European Union
EUR	Euro
EVM	Ethereum Virtual Machine
GBP	British Pound Sterling
JPY	Japanese Yen
KYC	Know Your Customer
PoS	Proof-of-Stake
PoW	Proof-of-Work
TPS	Transaction Per Second
TBTF	Too-Big-To-Fail
Tx	Transaction
USD	US Dollar
VM	Virtual Machine

1 Introduction

The evolution of blockchain and crypto assets was certainly a countermeasure to the inefficiency of financial markets, as well as to the inability of governments and central banks to mitigate the effects of crashes on those markets. The collapse of Lehman Brothers and the subsequent global financial crisis of 2008, which can be identified as catalysts, marked the worst financial catastrophe since 1929; however, the history of financial markets has also taught us about the procyclicality of such events. In the same year, Bitcoin (Nakamoto, 2008) was introduced as a pure peer-to-peer (P2P) electronic cash system based on cryptographic proof mechanisms, which enabled the trustless transmission of transactions among users as well as prevented double-spending attempts. The use of distributed ledgers allowed the synchronization of data among participants, making the system highly secure and replacing trusted third parties—this ultimately laid the foundation for blockchain technology. The very first explorations of electronic money and decentralized monetary systems started with B-money (Dei, 1998) and Bit Gold (Szabo, 2005), which were considered the early pioneers but were not implemented. Thus, it could be argued that blockchain was a natural product of technological progress and was probably accelerated by the distress and turbulence in the financial markets, which created the need for efficient ownership protection based on the skepticism of government-dependent banking systems.

The last decade was marked by several developments and new blockchain and crypto-asset platforms, of which some of the most significant were Ethereum, Ripple, Litecoin, Dash, and the subsequent 4,992[1] listed coins. Nevertheless, blockchain-based currencies have experienced lower market acceptance throughout the volatility, no intrinsic value, and a lack of commercial use. This is because they have not been able to provide the key characteristics of traditional money, such as a medium of exchange, unit

[1]For the list of all crypto assets visit; `https://coinmarketcap.com/all/views/all/` (retrieved 01.01.2020).

of account, and storage of value, preventing them from becoming global means of payment. For example, Bitcoin has seen bull runs in a short period with enormous price fluctuations based on market expectations and short-term profits based on speculations, followed by subsequent price drops. Ethereum and Litecoin were mainly used for transactions on the platform, whereas Ethereum focused on the deployment of smart contracts and decentralized applications (DApps), neither of which—because of the volatility in daily price—were suitable for day-to-day operations, and therefore received less acceptance in the market.

Since then, the further development of crypto assets has raised the need for stability and low volatility, leading to the emergence of stablecoins such as Tether[2] or Digix Gold Token[3]. The advantages of stablecoins are their constant price level and intrinsic value that not only facilitate daily transactions and value preservation, but can also serve as a hedge against the volatility of other crypto assets on the market because of the low correlation. However, even stablecoins have not been able to offer perfect protection because their reference assets (e.g., the US dollar) are not resistant to market declines and inflation.

The next expansion toward the global acceptance of crypto assets may arrive with the announcement of Facebook's Libra, a global digital currency, which will be backed by a basket of major fiat currencies to allow a stable value and to build a financial infrastructure based on a consortium of international companies. Libra promises a revolution of the Internet of money, with the financial inclusion of billions of people to empower efficient money transfers and cross-border transactions with minimal fees; furthermore, it promises to attract companies with its programmable platform and the ability to define custom-based transactions in the Libra network.

[2]Tether (USDT) is pegged at a 1:1 ratio with the US dollar. For further information visit; `https://tether.to/`

[3]Digix Gold Token (DGX) is valued at the rate of one coin/gram of gold. For further information visit; `https://digix.global/`

From the analysis, it can be deduced that the Libra network will face a high level of centralization and be marked from the permissioned nature of the Libra Blockchain. Further, the Libra Association, as gatekeeper, is based on leading and mostly for-profit companies that can reach approximately 2.3 billion people only through Facebook; this is without mentioning the other members of the Libra Association and their overarching link between the industries that emerge on the platform, which exclusively will earn interest from the user‘s deposits in the Libra Reserve. In addition, the results demonstrate that Libra‘s disruptive nature could lead to the destabilization of the financial system, leaving governments and central banks motionless in their fiscal and monetary policies, which are essential instruments for ensuring economic stability and growth, unless regulators successfully address the inefficiencies of the Libra project using appropriate regulatory measurements. Finally, the potential risks arising from the project's current specifications can be highlighted, which in the worst-case scenario could lead to a surveillance system that would allow Facebook and other members to control the digital identities of billions of people and their sensitive data.

The remainder of this thesis is structured as follows: Chapter 2 identifies the basics of blockchain technology to evaluate essential features for the functionality of the system. Chapter 3 describes the conceptual structure based on the Libra White Paper, and Chapter 4 examines the technical specifications of the Libra Blockchain to assess the potential functionality of the network. Chapter 5 formulates predictions according to the results of the analysis and existing statistics to predict the impact of Libra. Chapter 6 identifies potential risk factors that could have serious consequences on the environment. Chapter 7 addresses shortcomings based upon the technical specifications, and finally, Chapter 8 provides the conclusions to the thesis.

2 Theoretical Framework

This chapter highlights the fundamentals behind crypto assets and the underlying technology that plays an essential part in their functionality.

2.1 Blockchain

The term blockchain can be described through the use of distributed ledger technology (DLT), defined from its first implementation in Bitcoin, as a public and distributed ledger that stores all transactions and allows every participant to hold a copy of the ledger history. This provides the integrity of the data in the blockchain to be verified, as transactions are transparently stored in the ledger and visible to all participants in the network (Berentsen and Schär, 2017). In this decentralized system, participants must agree on transactions to update the ledger, which is determined using a consensus algorithm that uses computing power to solve mathematical problems (e.g., mining). Furthermore, it eliminates double-spending attempts through the use of cryptographic proof, allowing P2P verification without the need for trusted third parties (Yli-Huumo et al., 2016). However, the data are stored in blocks, which form a continuous chain of chronologically and timestamped transactions that are added to the blockchain—they can no longer be changed, falsified, or deleted (Crosby et al., 2016).

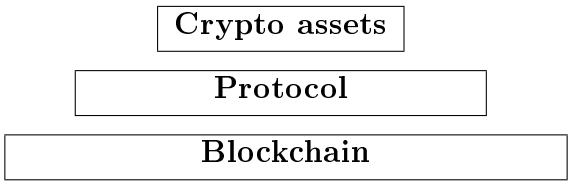

Figure 1: Technology layers. Source: Own illustration

As shown in Figure 1, the blockchain builds the basis of the system that will be implemented through the protocol, which defines the rules between participants; from there, the crypto assets only account for the top layer in the network, which depends on the first two components.

2.1.1 UTXO vs. Account

In the Unspent Transaction Output (UTXO) model, transactions contain several inputs and outputs, where the full state comprises the total number of UTXOs that can be spent in the network, which is analogous to the individual balance of the user being derived from the UTXOs available under the account address (Akcora et al., 2018). In the Bitcoin network, users can transmit transactions by signing the last hash value and attaching the recipient's public key to the transaction (Nakamoto et al., 2019). However, users do not own the coins but the output with the number of coins that can be signed as input in the transaction and forwarded to the recipient, which then controls the output (Ray et al., 2013). The first condition for transactions under the UTXO scheme is that the input must exceed the output or the transaction will fail (Berentsen and Schär, 2017). Second, the received input can be spent in one or several separate transactions, but if the quantity of coins received is not integrally issued in the following transaction, the remaining amount will be considered the transaction fee (e.g., reward) for the miners who will create new blocks (Akcora et al., 2018). Third, any coin payment must have a valid reference to the previous output, otherwise it will account for double-spending attempts, but this also allows users to retrieve past transactions (Delgado-Segura et al., 2018). In general, it is impossible to link accounts to the coins' origin because users create new addresses for new transactions, thereby providing parallel processing throughout the independence of transactions, but suffering from the lack of state for more complex programs because they can either be spent or not (Buterin et al., 2013).

The Account Model relies on balance sheet management, similar to accounts in the traditional banking system, where the full state can be directly determined from the accounts locally in the network (Ray et al., 2013). In Ethereum, users can spend any fraction of existing or received coins in their account, because transactions are defined by one input and one output (Akcora et al., 2018). However, accounts will be directly affected by state transitions—transfers of value and informa-

tion—because each address can be linked to an account based on the verification/signature key pair generated when a new account is created (Ray et al., 2013). With programmable abilities, the data and values are necessarily stored on the blockchain, which allows multi-stage smart contracts and DApps that could allow for reusable behavior as well as scripts with internal state storage for more complex processes (Buterin et al., 2014). In this context, there are externally owned accounts, which are controlled by users' verification keys, and contract owned accounts, which are autonomously managed accounts that store the contract code from the specified smart contract and can perform transactions and update internal states based on the conditions (Buterin et al., 2013). Enhancement can be achieved with space storing because of smaller byte amounts from the single-state tree storage and simple transaction output, which only requires a reference and a signature (Ray et al., 2013). Disadvantages arise from the publicly visible nonce in transactions, whereby the accounts store the nonce in a sequential order required for transaction execution to prevent double-spending attempts, but this limits the parallel processing of transactions.

2.1.2 Permissionless vs. Permissioned

Public blockchains are defined from the public and distributed ledger with the P2P network, which is based on cryptographic proofs and economic incentives defined from the consensus mechanism of the underlying protocol (Buterin, 2015). Any participant with the appropriate computer and open software who is willing to contribute can participate in the verification process, which includes transaction validation, ledger state updating, and system maintenance—this is also referred to as *permissionless* (Bashir, 2018). The most common implementations of public blockchains are Bitcoin and Ethereum, which are based on the Proof-of-Work[4] algo-

[4]Hashcash was invented by Adam Back 1997 that was used to avoid email spam and denial-of-service attacks. The Hashcash protocol introduced to PoW mechanism, which created stamps using computational effort from the recipients to deter threats or spam. Further readings; `https://nakamotoinstitute.org/static/docs/hashcash.pdf`

rithm. The PoW mechanism is required to solve mathematical problems with computational power incorporated from the miners in the validation, where the verified block is timestamped and added to the blockchain (Berentsen and Schär, 2017). The advantages are the decentralized network, few entry barriers, high-level privacy, no central authorities, and the anonymity of the participants (Buterin, 2015). Oppositely, they suffer from slow transaction throughput due to the resource-intensive mechanism and illicit activities such as shadow banking and money laundering.

Private blockchains belong to an entity and are primarily used for internal business case solutions such as projects, control, and database administration (Bashir, 2018). Activities such as writing or validating data belong to the owner, and furthermore, the ability to read data can be restricted as well, which can be classified as *permissioned*. Consortium blockchains are recognized as hybrid-variants, where the network is private only to a certain extent because several selected participants can be approved to participate in the validation process based on predefined rules (Buterin, 2015), which also accounts for a *permissioned* system. A common implementation is Hyperledger Fabric, which provides cross-industry blockchain solutions at the enterprise level, defining the consensus mechanism based on the predefined roles of nodes. For instance, the peers maintain the ledger, the orderer communicates the information, and the endorser ensures the validity of the transactions in the network (Valenta and Sandner, 2017). The consensus mechanism often relies on crash fault-tolerance or Byzantine fault tolerance protocols, with a focus on the resiliency of the system to ensure faultless processing (Bashir, 2018). The advantages arise from the minimal resource requirements of the consensus mechanism, higher scalability, faster transaction processing, and efficient consensuses among a smaller number of trusted validators (Buterin, 2015); however, limitations are the centralized nature of the blockchains with limited user involvement, where the decision-making and voting rights belong to predefined owners or selected members, thereby leading to lower privacy and a higher possibility of network attacks.

3 The Libra Concept

This chapter examines the foundation of the Libra project and identifies crucial characteristics for the technical analysis.

3.1 Libra

"The mission for Libra is a simple global currency and financial infrastructure that empowers billions of people."[5]

With the Libra project, Facebook has unveiled the development of a unique digital currency to be launched in the first half of 2020. The Libra coin should enable financial operations over the network, with a stable value that will be supported by a consortium of international companies—the Libra Association—which ultimately lays the foundation for the Libra Reserve, the aims of which are to actively preserve the coin from unexpected changes in the financial market and to guarantee its operability (Association et al., 2019*a*). The Libra network builds on the self-developed Libra Blockchain, which will be maintained throughout the rules defined in the Libra protocol, using the new programming language Move to define custom assets and user-defined transactions to be carried out, which all together forms a complex ecosystem (see Figure 7) (Association et al., 2019*a*).

3.1.1 Association

The Libra Association is an independent nonprofit organization comprising 21 companies from different industries with strategically distributed locations; these companies are involved in the development of Libra, which is headquartered in Geneva, Switzerland (Association et al., 2019*b*). To participate, members must meet certain conditions for approval; one requirement is to stake a part of the network in the form of initial entry costs amounting to 10 million US$ or an arbitrary amount for

[5]Statement from the White Paper, S.1. Source: (Association et al., 2019*a*)

international members (Association et al., 2019*b*). Members will represent validators in the network, who are responsible for transaction validation and database maintenance based on members' collective agreement, as defined in the LibraBFT consensus protocol (Amsden et al., 2019), as well as receive decision-making rights for policy changes and updates that will be considered in the council (Association et al., 2019*c*). The verification process will rely on these validators, who are also the only bodies authorized to mint or burn coins, and from there, authorized resellers and exchange platforms will be responsible for daily operations with users (Catalini et al., 2019). Due to demand, the Libra Association will perform large quantities of coins, and ultimately represent the buyer of last resort, who can buy the coins back when the demand decreases (Catalini et al., 2019).

Industry	**Company**
Blockchain	Anchorage, Bison Trails, Coinbase Inc., Xapo Holdings Limited, Ribbit Capital, Thrive Capital
Non-profit and multilateral organizations	Creative Destruction Lab, Kiva, Mercy Corps, Women's World Banking
Payments	PayU
Technology and marketplaces	Booking Holdings, Calibra, Farfetch, Lyft, Spotify AB, Technologies Inc, Uber
Telecommunications	Iliad, Vodafone Group, Union Square Ventures
Venture Capital	Andreessen Horowitz, Breakthrough Initiatives L.P

Table 1: The Founding Members of the Libra Association
Source: Adapted from (Association et al., 2019*a*)

3.1.2 Reserve

The Libra Reserve will be responsible for the stable value of the digital currency, which is comprised of the members' participatory investment of 10 million US$ or an arbitrary amount for international investors (Catalini et al., 2019). In addition, the variable part will be based on users' deposits in several fiat currencies, which means that the collateral will dynamically respond to the number of users and the demand. Users are required to cover the value of the coin at a 1:1 ratio to prevent an inflationary model in the network (Catalini et al., 2019). The value of the coin must be predictable for any given time and circumstances in the market, where P_t should equal P_{t+1}, which will be actively maintained throughout the investments of the reserve (Catalini et al., 2019). The composition of the reserve is the result of bank deposits and riskless government debt from reliable central banks, with a strong focus on major currencies such as the USD, EUR, GBP and JPY (Catalini et al., 2019).

In fact, a small deviation in the value of Libra can be expected from specific changes in the government-issued currencies. To minimize the likelihood of such events, diversification will be achieved over long-term government debt, bonds with t $>$ 1-year duration with low default and inflation probability, such as Switzerland, which holds its inflation rate between 0 and 2% (BFS, 2019); furthermore, it will consist of short-term governments securities such as U.S. Treasury bills with t $<$ 1-year duration, which should provide liquidity to mitigate the effect of market downturns and abrupt changes in demand (Catalini et al., 2019). Notably, assets will not be managed actively, which implies that the outcome after withdrawing can deviate from the value in the network because of unexpected changes in the foreign exchange market (FX) (Catalini et al., 2019). Therefore, users are not protected against market risks, such as changes in the domestic currency and exchange rates, where the outcome from two different users may differ depending on the economic situation of the countries.

3.1.3 Token

The Libra network relies on a two-token system, which efficiently separates the governance and validator management from the native currency in the protocol.

The *Libra Investment Token* defines the participation of companies as contributors to the system with the function of validating nodes, which represents the security unit in the protocol. To be approved, companies must meet certain predefined conditions that ensure the credibility of participants as well as prevent malicious activities due to social reputations (Amsden et al., 2019); In return to the investment, participants not only receive proportional decision-making and voting rights in the network but also benefit from the interest yield generated from the collateral in the reserve (Amsden et al., 2019). On this basis, the Libra Investment Token can be classified as an asset token[6], because the participants are eligible for dividend payments and other income streams of the network.

The *Libra Coin* represents the native currency unit in the protocol that will be backed by the basket of fiat currencies and government securities, which endows the properties of a stable coin with a constant price level (e.g., asset-collateralized token), which qualifies it for a medium of exchange. The Libra coin can be classified as a payment token[6] because it will be used as means of payment for cross-border transactions, money transfers, and financial services in combination with the financial infrastructure (Association et al., 2019*a*); however, it can be argued that the Libra coin could also be classified as a hybrid token[6]—a payment and asset token—because the value will be defined from several low-volatile assets, which enables the digital representation of real-world assets and thus represents a financial claim.

[6]The specifications are adapted from the FINMA ICO Guidelines; `https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en`

3.1.4 Calibra

Calibra, an independent subsidiary founded by Facebook, will be used as a digital wallet to facilitate coin management and conduct regulated transactions over the network, and moreover, it will represent a full member of the Libra Association (Association et al., 2019*a*). In this case, Calibra will be integrated into the interface of Facebook's core products such as Facebook Messenger and WhatsApp, as well as be a standalone application with which users will be able to send money with the same ease as sending messages (Association et al., 2019*a*). The need for an independent institution was raised by the recent charges against Facebook in the Cambridge Analytica[7] scandal. Cambridge Analytica was accused of misusing confidential data of Facebook users to capture consumer behavior with the intention of placing customized ads that match their preferences to increase the accuracy of ads and thus maximize profits. In this context, Calibra was founded with the primary objectives of ensuring the efficient separation of users' social media data and financial data for a higher level of privacy (Association et al., 2019*a*).

3.1.5 Incentives

To attract companies to the network, there must be certain incentives that make it profitable for them to participate. However, although explicit incentives exist, several statements might indicate that additional instruments will be implemented for the welfare of members. From the Libra documents following incentives can be extracted:

Dividends

Members of the Association will benefit from the investments of the funds based on interest-bearing deposits. The dividends will be used to maintain the system, but the remaining amount will be paid out to members as a reward for early participation—users will have no claim on the re-

[7]Further readings on the Cambridge Analytica incident; `https://www.theguardian.com/news/series/cambridge-analytica-files`

turns (Catalini et al., 2019). The amount heavily depends on the returns of the investments because they are invested in less volatile assets that match low return profiles, and it also depends on external events such as market expectations.

Transaction fee

The network will be based on the gas model, which charges a fee for the execution of transactions, and smart contracts that serve as protection against spam and system congestion (Amsden et al., 2019). However, no statements have been made about the final installment of fees during normal and higher workloads. Even if the fees will be small, this could yield a significant amount if mainstream adoption can be assumed.

Storage fee

Currently, members can release data after execution based on the expiration time approach, which will be determined by the VM. This could be achieved from the size of an account and time it is stored in the ledger, which would cause fees until the data can be released by the virtual machine (Bano, 2019). Higher transaction loads and data can burden the memory capacity, which necessitates a rent-based system being implemented that will be perfectly compatible with the account-based model and increase members' profits.

Conversion fee

To improve efficiency, the Libra Association will only conduct transactions with larger amounts of coins in response to demand in cooperation with the authorized resellers and exchange platforms (Catalini et al., 2019). However, it can be expected that any fiat-to-Libra or Libra-to-fiat exchange will cause a conversion fee, which will belong to the merchants, but there are no definite statements to be found in the documents.

4 The Libra Blockchain

The Libra Blockchain, which relies on a decentralized and cryptographically authenticated database, builds the foundation of the system that will be managed throughout the pool of validators—the consortium—who are involved in the verification process (Amsden et al., 2019). The implementation of the blockchain will be derived from the Libra protocol, which defines the rules and communication between the validators to collectively maintain the database. Based on the transaction validation, the consensus mechanism will determine the manner in which validators can reach an agreement on the sequential order of the transactions to uphold the state of the database, thereby forming authenticated data structures that ensure the integrity of the Libra ecosystem (Bano, 2019)

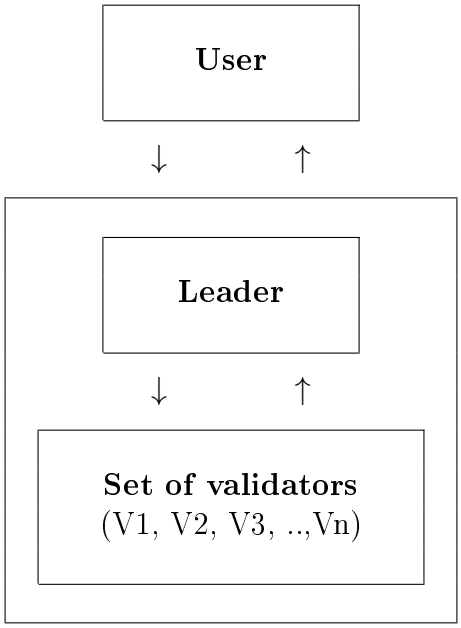

Figure 2: The user and validator faucet process
Source: Adapted from (Amsden et al., 2019)

As shown in Figure 2, the interaction in the Libra protocol will be based on two parties, the users who issue transactions and the leader who processes transactions among the validators to reach a consensus, which will be elaborated in the further course of the analysis.

4.1 The Account Model - State

To encode the ledger state, the Libra protocol uses an account-based model because the state can be identified as a key-value store (i.e., public-key cryptography), which authenticates user accounts and allows account address keys to be linked with account values (Amsden et al., 2019). Hypothetically, the account values are a collection of resources and modules stored under the users' account addresses, and can be interpreted as a map of the access path to byte array values (Amsden et al., 2019). Resources are declared by the modules, which contain the name and account address to define access control, as well as enable reusable behavior and multi-stage actions with respect to the bytecode, which ultimately will promote token standards (e.g., ERC-20[8])(see subsection 4.5.1).

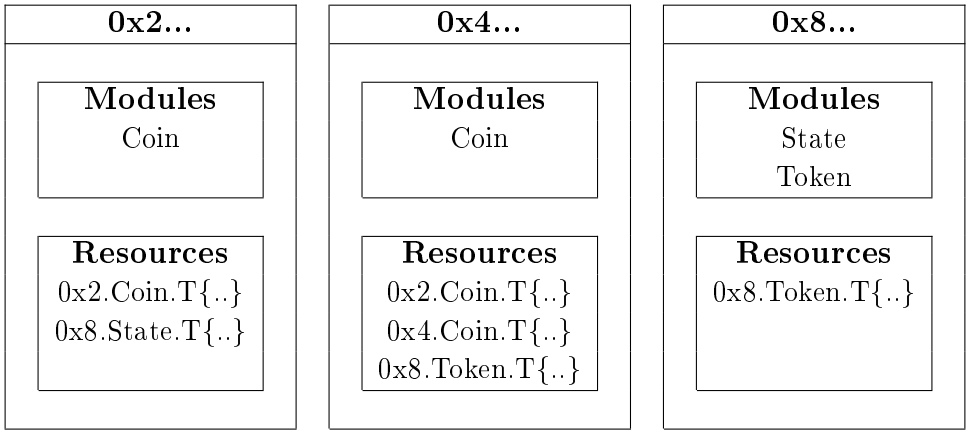

Figure 3: Storage inside the accounts
Source: Adapted from (Amsden et al., 2019)

Figures 3 shows the storage process of the resources and modules in three different accounts, where each address can contain resources, which store data values such as the number of coins owned or the state, and modules, which store the bytecode (Amsden et al., 2019). However, each address can store multiple modules as long as they have different names; otherwise, modules can have the same name under different account addresses because the resources generally differ from each other. Furthermore, the

[8]The Ethereum Request for Comments is a guideline for creating tokens on the network. See; `https://eips.ethereum.org/EIPS/eip-20`

account system will allow transactions to be conducted directly from users' accounts because the transmission of values and information will be processed and stored in the accounts, which will lead to direct state updates of the accounts (Amsden et al., 2019). Changes in the state of an account will lead to the computation of new hash values (e.g., authenticator keys) for the entire account history, which belong to a serialized sequence of transactions from which the cost *O(n)* is derived from the length of the bytecode n that increases with the number of transactions submitted from the account (Amsden et al., 2019).

4.1.1 An Address

A unique account address will be produced within the creation of the account, which will generate the verification and signature key pair. The verification key will represent the user's account address, derived on the basis of the Keccak-256 algorithm (also known as SHA-3[9]), based on the cryptographic hash function and the corresponding signature key that will be used to sign transactions (Amsden et al., 2019). To request an account address, an existing account must invoke the *CreateAccount* command with a transaction that transfers coins to the new account to pay the creation fee, which will only then enter the ledger state (Amsden et al., 2019). Libra users can optionally change their signature key while maintaining the verification key (e.g., their account address).

Compared with Ethereum, which also uses the account-based model and similar key-pairs, users cannot rotate or change their individual signature key because the accounts are always assigned to a specific account address authenticated from the corresponding verification key (Buterin et al., 2013).

[9]Compared with SHA-2, SHA-3 allows for preventing collusions with sponge functions (Bertoni et al., 2013) via EdDSA555, which in this context uses the specifications of the Curve25519 (Poddebniak et al., 2018). Bitcoin uses the ECDSA, as well as others, which is based on the elliptic curve that generates the private key from where the point of origin takes another computational step, producing the public key as a one-way function and especially in Bitcoin with two hash functions, SHA256 and RIPEMD, for additional security.

4.2 The Transaction System - State Transition

This section explains the relationship between the transaction system and state transitions when attempting to update the ledger state.

4.2.1 Prerequisites

Conditions that must be fulfilled before execution are that the validators agree on the initial state (i.e., the genesis state). The reason for this is that all the components of the blockchain system, such as the account logic, the transaction validation, validator management, Libra coins etc., will be defined from the modules, whereby the initial state must also be included (Amsden et al., 2019). This will be configured through a first transaction T_0 that defines resources and modules to be created in the initial state S_0, identified by a hash function, which will be added to the ledger history to form the overall status quo of the network (Amsden et al., 2019). Secondly, transaction outputs must be predictable depending on the information in the transaction and the ledger state; moreover, they must be hermetic to ensure that transaction execution will not lead to external effects, allowing validators to separately execute the same transactions to agree on the order (Amsden et al., 2019). Finally, the transaction will cause fees (e.g., the gas model (Wood et al., 2014)), which is an crucial instrument for preventing spam and reducing system congestion; the fees will adapt dynamically to the system capacity and be charged from senders' accounts in the denomination of Libra coins (Amsden et al., 2019). According to demand, the system will charge low fees during periods of moderate use of the system's capacity and higher fees with increasing transaction loads to reduce demand and system disruption, which could lead to DoS attacks (Amsden et al., 2019). To this background, validators will also have the option of privilege transactions with higher gas prices in times of higher system congestion, which also means that some transactions will not be processed.

4.2.2 A Transaction

Transactions are the only operation that can invoke changes to the ledger state, which will lead to state transitions and updates of the database.

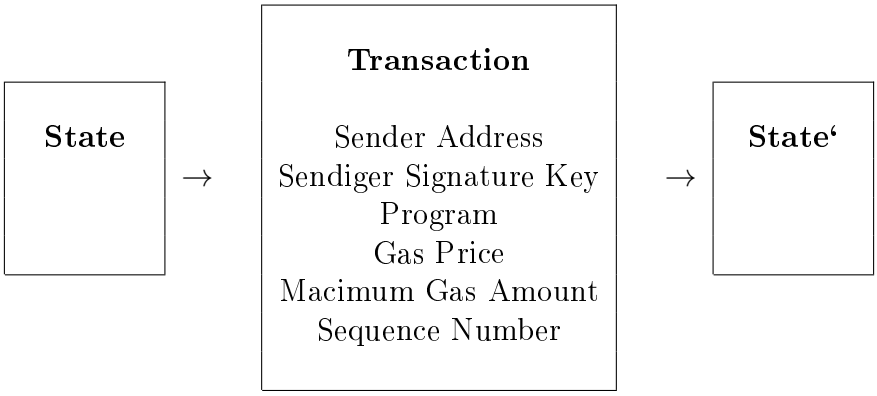

Figure 4: Transaction structure
Source: Adapted from (Amsden et al., 2019)

Figure 4 indicates the transaction structure, which can be described as follows (Amsden et al., 2019): The sender address belongs to the user's account address, which indicates the sequence number (e.g., the authentication key) and the balance of the *Token.T* resource (see Figure 3) stored under this account address. The sender‘s signature key used to sign transactions must match the verification key of the sender, and the hash of the signature key must also match the authentication key retained by the sender‘s *Token.T* resource. The program contains a transaction script written in bytecodes, which contains the arguments for the procedure such as the number of coins to be transferred and the recipient's address, or the optional list for modules to be published. The gas price indicates the gas amount per unit that users are willing to pay for the execution of the transaction by the VM. The maximum gas amount defines the upper-limit that can be consumed by the transaction, where the VM counts the gas units and the transaction fails if the gas limit exceeds this value. The sequence number must correspond to the sender's *Token.T* resource that keeps track of the sequential order, which is incremented by one after execution to ensure that transactions are not reused.

4.2.3 Transaction Execution

The transaction's execution proceeds before the validators reach a consensus to achieve an efficient agreement on the sequential order as a speculative attempt. Therefore, the VM must undertake several steps, which are described as follows (Amsden et al., 2019). (1) The VM compares the signature with the transaction data and the user's verification key. (2) The VM runs prologue with the admission control, which confirms the sender's identity and sufficient account balance to cover the gas units caused by the VM, as well as verifies that the transaction has not been issued already by comparing the sequence number (e.g., nonce) of the transaction with the sequential order of the number in the user's account. (3) The VM controls the transaction script or module with the Move bytecode verifier, which controls for type safety, reference safety, and resource safety to detect failures and bugs as soon as possible, mostly for smart contract codes. (4) The VM publishes modules under the account address of the sender, which then avoids duplicates, because modules with the same name in the account will fail (see Figure 3). (5) The VM runs the transaction script, which in case of success will be added to the full state; however, if it fails because the sender runs out of gas or unexpected runtime duration, no changes in the full state will occur. (6) Beyond step (2) the VM runs the epilogue, which charges the maximum gas amount for the execution process even if the user's gas ran out at some point.

The execution translates data into a new authenticated data structure to represent the full state of the database, since the transactions are deterministic and hermetic, which produces a temporary ledger history (e.g., authenticator) with the transaction appended (see subsection 4.3.2) (Amsden et al., 2019). The authenticator will then be forwarded to the consensus protocol where the leader will use it to reach an agreement among the validators to update the ledger state, resulting in a new version of the database (see subsection 4.4.1).

4.3 The Consensus Protocol

This section introduces the consensus protocol that allows the set of validators to achieve a logical representation of the single database.

4.3.1 Byzantine Fault Tolerance

The origin of BFT can be derived from the Byzantine Generals Problem (Lamport et al., 1982), which was introduced in computer science, because the distributed systems were unable to synchronize the same information, leading to disruption of the network and system errors. The intention behind BFT is to achieve the preservation of distributed systems against colluding and faulty nodes; the remaining honest nodes would still be able to agree on the same information to achieve faultless processing, as well as prevent DoS attacks without interrupting the system. The BFT consensus defines the process through which the set of validators reaches a consensus on the same information, such as the current ledger state in the network (Amsden et al., 2019). The mechanism ensures the reliability of the validators throughout collective decisions, where the communication between nodes must lead to efficient transaction validation (Bano, 2019). Therefore, the underlying consensus protocol must be fault-tolerant to enable the network to continuously function, even if there are nodes that fail to respond or act maliciously.

Alternative solutions to the problem of Byzantine generals have been introduced in Bitcoin and Ethereum, where the underlying consensus protocol is based on the PoW algorithm and cryptographic proofs related to the hash function, which uniquely assign the integrity of the data to the computing power of the miners in the network (Wood et al., 2014). In this context, the Byzantine failures cannot pose a threat to the system, but the resource-intensive process (e.g., energy consumption) weakens the overall attractiveness of the mechanism (Buterin et al., 2013).

4.3.2 LibraBFT

The consensus protocol replicates the submitted transactions of users, executes them in the current database and reaches an agreement on the binding commitment of the transaction order (Amsden et al., 2019). The LibraBFT belongs to the HotStuff[10] consensus protocol variant, which enables efficient state machine replication (Amsden et al., 2019). This implies that validators can reach an efficient consensus on transaction information to maintain the database, even if colluding or deviating nodes exist among the set of validators (Amsden et al., 2019). Persistence is ensured throughout the global stabilization time, which provides the necessary conditions for validators to continually process the transactions and coordinate among the remaining honest nodes within the maximal delay of δ, also known as partial synchronization[11] (Bano, 2019). In addition, the pacemaker provides liveness in LibraBFT, which will cause timeouts that allow validators to synchronize during the rounds and move to the next round (Amsden et al., 2019). The fundamental aspects of LibraBFT that protect the system from bugs are as follows: the validators do not have to sign the sequence of the transaction, but the transaction block will be formed by quorum certificates (QCs), whereby the aggregation of the signatures ensures the verifiability of the validators, but also secures the identities of the validators that are not displayed (Amsden et al., 2019).

A consensus shall be reached in LibraBFT, where two-thirds of the nodes act honestly and one-third of the nodes can be malicious (e.g., Byzantine nodes) among the set of validators (Bano, 2019). The voting rights of Byzantine nodes with the intent to deviate from the protocol should never exceed the threshold f, which defines the faultless processing among the other honestly acting nodes, to reach an agreement on the transactions and maintain the ledger state, which is described as follows (Lamport et al., 1982):

[10] For explicit information on the HotstuffBTF paradigm with the BFT consensus, see; `https://arxiv.org/abs/1803.05069`

[11] For the technical implication of partial synchronization in the consensus protocol, see; `https://groups.csail.mit.edu/tds/papers/Lynch/MIT-LCS-TM-270.pdf`

$$N \geq 3f + 1 \tag{1}$$

$$N \geq 3 * 6 + 1 \qquad if \quad f = 6 \tag{2}$$
$$N \geq 21$$

$$N \geq 3 * 33 + 1 \qquad if \quad f = 33 \tag{3}$$
$$N \geq 100$$

Equation (2) represents the condition for LibraBFT to remain safe when most f votes are Byzantine nodes that apply to the relation of all validators N in the network. In equation (3), the current status quo of the Libra Association can be observed, which in the case of six Byzantine nodes requires at least N $\geq$ 21 validators, where the remaining 15 nodes can reach a consensus on transactions. With the planned expansion of the Libra Association to 100 members, equation (3) implies that in the case of 33 Byzantine nodes, a total of N $\geq$ 100 validators must be present to absorb the malicious nodes and ensure the efficient processing of transactions between the remaining 77 honestly acting nodes in the network.

The main procedure is as follows (see Figure 2). Users issue transactions by signing them, and a validator forwards the transaction to the mempool and shares it with the other validators. LibraBFT proceeds in rounds, and in each round a leader will be selected, which will be triggered by a built-in function of the last leader that randomly assigns a new one to reduce the likelihood of counterfeit and DoS attacks from the unpredictability of the next leader (Bano, 2019). The leader takes a sequence of a transaction from the mempool and broadcasts it to the other validators who control voting rights and the commitment of the transaction (Bano, 2019). However, when the validators vote in favor, the transaction execution produces an authenticator of the database (see

subsection 4.2.3). In response, the validator will sign the transaction block and the authenticator, and the leader will gather all the votes to form a QC, which proves that votes for the block are $\geq$ *2f+1* and will be broadcasted to the other validators (Amsden et al., 2019).

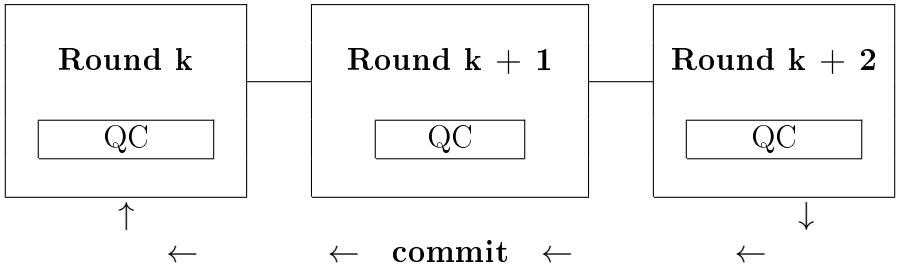

Figure 5: The continuous 3-chain commit rule
Source: Adapted from (Amsden et al., 2019)

As shown in Figure 5, a transaction block will be committed based on a continuous 3-chain pattern, which describes a transaction block at round k with the corresponding QC needing to be confirmed with the following two transaction blocks, *k+1* and *k+2*, and their corresponding QCs. Finally, the validators will sign the authenticator to produce a new authenticated data structure that will be updated with the latest ledger state, which represents a full state of the database (Amsden et al., 2019).

4.4 The Database

All data will be stored in the single-version database, which encodes the entire ledger history and current ledger state with the number of coins available on the network (Amsden et al., 2019). The version of the database is always determined by the number of executed transactions denoted by an unsigned 64-bit integer. Applying transaction *Ti* to the ledger history *Si-1* will generate the new ledger state *Si* and analogously produce the transaction output *Oi*, which aggregates the execution code, gas usage, and events (Amsden et al., 2019). In general, at each versioni, the full state of the database is composed of a tuple *(Ti, Oi, Si)*.

4.4.1 Ledger History

In the Libra protocol, the authenticated data structures for the ledger history will be formed by the Merkle tree (Merkle, 1987) after transaction execution. This includes the representation of the entire database and simultaneously creates a short authenticator based on transaction T_i, which will be signed by the validators used to agree on the transaction order in the consensus protocol (see subsection 4.3.2) (Amsden et al., 2019). The ledger history keeps track of all transactions executed over the network, which are sequentially ordered upon the latest ledger stated, and determined by a cryptographic hash function that must indicate the initial state S_0 with the first transaction T_0 as well as all subsequent transactions, thereby ensuring the integrity of the database in each version$_i$ of the network (Amsden et al., 2019).

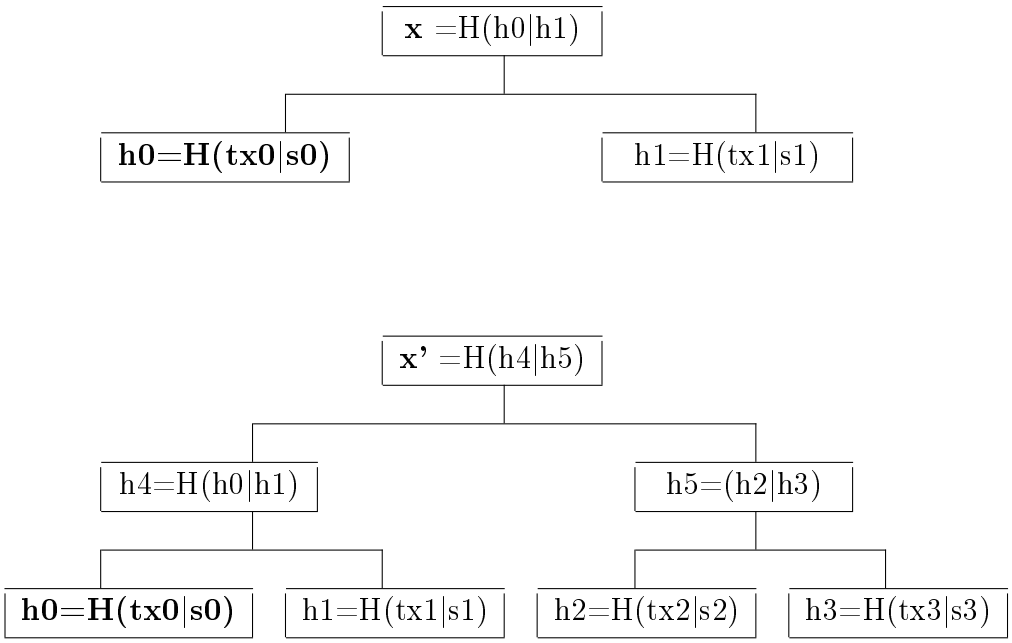

Figure 6: The Merkle tree storing process
Source: Adapted from (Amsden et al., 2019)

As shown in Figure 6, the Merkle tree provides the authenticated data structure for the ledger history, which will be automatically updated when new transactions are executed (Amsden et al., 2019). In this context, users can always observe the accountability of the validators by sending queries on any specific state, which enables users to re-execute transactions to compare the specific $state_i$ of the corresponding $version_i$ of the $database_i$ (Amsden et al., 2019). The accumulator of the Merkle tree performs only append-only operations because the data structures are deterministic, and furthermore, when new data enter the database, a new root hash $x \rightarrow x'$ will automatically be executed, which indicates the full state with the authentication path of sequentially ordered transactions (Reyzin and Yakoubov, 2016). This allows the mapping of all data as an authentication path of sequentially ordered transactions (e.g., hash values) from an ever-growing Merkle tree, which always includes the first transaction T_0 in state S_0 and with hash value h_0 (Amsden et al., 2019). The hash function H is a mathematical representation, which assigns the hash value h to each input m, with the designation $H(m) = h$ ensuring the integrity of the data, because the smallest deviation in the archetype leads to different hash values and thus to an invalid outcome (Berentsen and Schär, 2017).

The full data structure of the database will be differently managed with a focus on efficient proofs and storage optimization. In general, for every new version of the database, the validators will sign an authenticator, also known as the root hash x, which indicates the full state with the entire ledger history. However, as the ledger history increases, each leaf obliges the so-called $TrasactionInfo_i$ structure (Amsden et al., 2019). From here, the structure inherits aggregated components such as the signed transaction T_i, the event list E_i produced from transaction, and the state S_i after executing the transaction, which is a sparse Merkle tree that includes an account blob for each leaf (Amsden et al., 2019).

4.5 Move Programming Language

The Move programming language will facilitate programming through reducing complicated code structures to prevent false specifications with executable bytecodes. Move will enable custom transactions and user-defined contracts, as well as provide the ability to define and implement core components of the blockchain (Blackshear et al., 2019). In the spotlight are the custom resource types, which are used to encode programmable assets to interact as values, and thus achieve the representation of real-world assets with the appropriate measurements throughout Move, which are defined as follows (Blackshear et al., 2019):

- *Create* resources when real-world assets enter the network
- *Modify* resources when the digital assets change ownership
- *Destroy* resources when physical assets depart from the network

Flexibility will be provided by transaction scripts, which contain the procedure and the bytecode that allow customization, because scripts can invoke one-off behavior and multi-stage actions in the modules as well as run local computations (Blackshear et al., 2019). The Move programming language inherits two programs:

- *Transaction scripts*, which are single-use codes to submit transactions
- *Modules*, which are long-life codes that define the access control

Safety is ensured throughout the bytecode verifier that controls programs in terms of type safety, reference safety, and resource safety, which will then be forwarded to the bytecode interpreter. This provides a higher level of security because the code will not be compiled within the transaction's execution, which could cause several failures (Blackshear et al., 2019). Verifiability will be provided with the aforementioned static on-chain verification tools, which also control runtime failures such as integer overflow and program correctness, because poorly defined resource specifications could provoke loopholes and bugs (Blackshear et al., 2019).

4.5.1 Resources and Modules

In the Libra protocol, remarkable improvements have been made to the specification of resources and modules to enable the efficient representation of real-world assets, assignment of ownership, and contract-based transactions. However, the entire database will be described from resources defined as data values and modules as code values (Blackshear et al., 2019).

The programmable resource types can be individually customized, and are stored as data structures, including the arguments for the procedure that ensure resources cannot be copied or replicated, only moved within the storage (Amsden et al., 2019). Resources are characterized by their name and contain the name and address of the module, allowing users to efficiently stake coins and store the resource in the account, which also provides the possibility for smart contracts and token standards (e.g., ERC-20) in the network. Within the resource, values will be stored under named fields that can be integers or more complex types of values, such as resources within the resource (Blackshear et al., 2019).

Modules are code units that store the Move bytecode published in the ledger state, which can be characterized by the name of the declared account address (Blackshear et al., 2019). In comparison, smart contracts in Ethereum store the codes and values together, whereas in Libra the modules and resources are separated in the protocol (see Figure 3). However, within the modules, the bytecode defines the structure and argument procedure, and therefore secures the resource values and determines access control for users (Blackshear et al., 2019). Intuitively, modules are used as instructions for creating resources, which will provide functions such as simple ownership as well as complex financial services to be defined (Blackshear et al., 2019). In addition, modules cannot be changed or deleted once they have been declared in the account address, a feature that serves as security for users yet does not prevent human failures where the only option—for now—will be a hard fork to undertake changes (Amsden et al., 2019).

4.5.2 Move Virtual Machine

The Move VM is instructed to combine individual components, such as the implementation of the bytecode verifier and bytecode interpreter, which can be described as an execution model capable of processing a set of bytecodes with a stack-based architecture (Amsden et al., 2019) that is crucial for the execution of smart contracts in the protocol. In the stack VM, the operand is expressed through the stack pointer, where no address is explicitly required, and the operations are performed via *push* and *pop* operations to simplify transactions and customize assets. For the Move VM to verify and run the bytecode, transaction scripts are currently written in Move intermediate representation (IR), which compiles the codes into bytecodes, where the execution can be performed without translating the codes into low-level components (Amsden et al., 2019). With a focus on contracts, the Move VM supports state variables such as booleans, unsigned 64-bit integers, 256-bit addresses, and byte arrays of fixed size according to the runtime and memory model, as well as structures that include resources and references (Amsden et al., 2019).

Compared with Ethereum, where smart contracts are written in Solidity[12], the EVM is not able to read the codes until they have been compiled into opcodes and subsequently stored as bytecodes to be executed (Hollander, 2019). However, problems occur after the EVM performs specific transactions or tasks because multiple errors can occur within the compilation process that remain undetected, leading to bugs and false specifications or enabling actors to circumvent the compiler from directly written bytecode scripts (Buterin et al., 2013).

[12]Solidity is a high-level contract-orientated programming language, which takes several characteristics from JavaScript as well as C++ and Python, see; `https://solidity.readthedocs.io/en/v0.5.12/`

4.6 Performance

The performance will be a critical aspect for the protocol to provide a global financial infrastructure in which Libra strives to meet all the abovementioned components above to maximize efficiency based on the following three main drivers (Amsden et al., 2019):

• The *throughput*, which defines the maximum number of transactions per second that the blockchain can process

• The *latency* period, which determines the time between submitting transactions and another party determining that the transaction has been executed

• The *capacity*, which describes the number of accounts that can be stored in the blockchain

Because the Libra protocol is still under construction, it is assumed that it will be able to process 1,000 transactions per second (TPS) within 10 seconds of submission and confirmation of the transaction (Amsden et al., 2019). Technical requirements for a validator to support the performance are a 40 Mbit/s[13] Internet connection. In addition, each node requires only one CPU to support 1,000 TPS and memory storage must be backed up with a 16TB[14] SDD storage server to store and process information (Amsden et al., 2019). Components such as the single Merkle tree for authenticated data structures improve the performance, where users can verify data more easily instead of calculating single hash values for specific transaction blocks. The accumulator automatically leads to updates when new information enters the ledger history, allowing for automatic execution and efficient proof that x is a prefix of x' (see Figure 6), thereby preventing any counterfeits and responding with invalid outcome, as information is deterministic (Amsden et al., 2019).

[13]The 40 Mbit/s are derived from a single transaction generating 5KB of traffic, where the 40 Mbit/s converted to kilobytes per second correspond to 5,000 KB/s, resulting in 1,000 TPS.

[14]4 KB traffic generated by an account where the 16 TB converted to kilobytes corresponds to 16 billion KB, providing a capacity of 4 billion accounts.

4.7 Transition

Libra will be governed by the Libra Association, where the validators are engaged in the transaction validation and database maintains to keep track of the transactions and uphold the state of the blockchain. The participation relies on predefined rules that companies must adhere to in order to be approved to contribute to the network. The consensus protocol is based on the collective agreement of validators with the underlying BFT mechanism, which aims to reduce the computational effort associated with alternatives such as the PoW mechanism, achieving efficient transaction throughput through a consensus being reached among a smaller number of trusted validators in the network. This means that users will have restricted capabilities in the network, which ultimately rests on money transfers and the transmission of transactions based on the services and goods offered.

The transition toward permissionless with the PoS mechanism, which includes the full decentralization of the network, should involve users actively participating in the transaction validation process with distributed decision rights on protocol modifications; furthermore, it will probably provide the ability for all parties to define custom assets and smart contracts (Bano et al., 2019). With a brief review of the PoS mechanism, which relies on economic incentives that ensure the security of the network, validators must stake coins, and in case of manipulation, they will become obsolete (Buterin et al., 2014). Therefore, voting rights will be distributed proportionally to the stack owned by users and the time of possession, which determines the probability of users being selected, to purpose new block units where validators will receive a transaction fee (i.e., reward) in return (Li et al., 2017). From this, an inference can be drawn that users with a significant number of tokens seem to have much more influence on the network; for example, User A owns 15% of the coins, which increases his or her probability compared with User B who owns 2% of the coins, enabling User A to then propose 15% of new blocks in the network (Li et al., 2017).

4.8 Overview

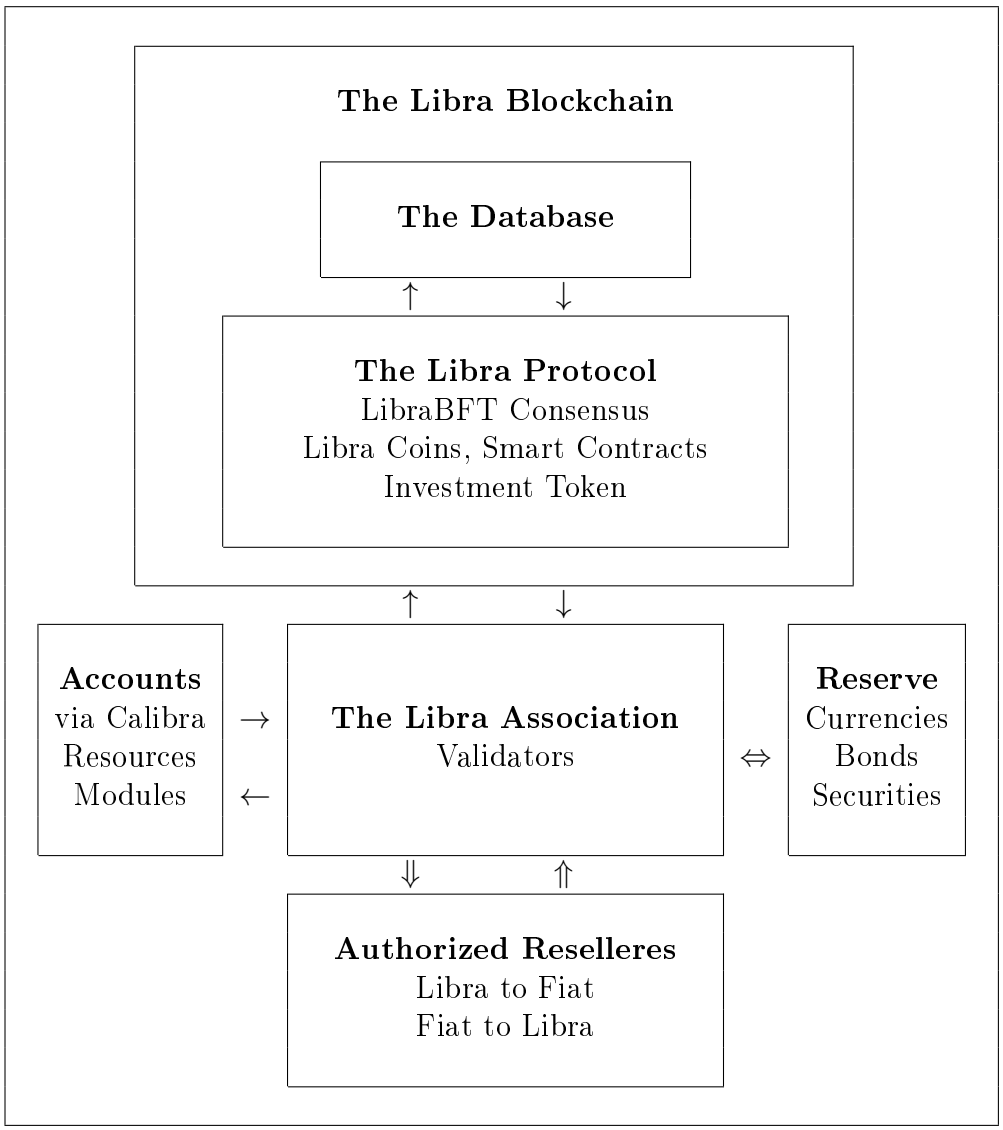

Figure 7: The Libra ecosystem. Source: Own illustration

Figure 7 presents a simplified holistic representation of the information channels (thin arrow) and monetary channels (thick arrow) in the Libra ecosystem. The Libra Association will process users' transactions based on the rules in the LibraBFT, uphold the database and respond to user's queries with authenticated data structures. Further, the Libra Association will be involved in the management of the Libra Reserve and, in cooperation with authorized resellers, will deposit money into the Reserve due to demand and create Libra coins in return, and vice versa.

5 Potential Impact

This chapter combines results from the analysis with the existing projects and company statistics in order to derive the impact of Libra.

5.1 Short-term

The digital currency, Libra, will attract different types of investors, as seen before, underpinned by the fact that it will be backed by the collateral of low-volatile assets, ensuring its stable value and relatively constant price level. With the integration of Calibra into the interface of Facebook and its core products, Libra will find its way into daily transactions for some users, which can be used as a means of payment rather than a type of investment opportunity referred to common blockchain-based currencies that are driven by market expectations and speculations and, in return, experience low persistence and large price fluctuations.

With the ability to transfer funds and submit transactions based on low fee structures and efficient settlements will be particularly crucial for some countries, as the minimal entry barriers and few technical requirements will encourage new actors to enter the financial market. Libra will overcome skepticism of citizens, which can be strengthened by the trust built up in the network, as reputable companies ensure regulated transactions and actively preserve the value of the digital currency. In terms of statistics (see Appendix), it can be deduced that the driving force will be Facebook, as its core products together can reach approximately 2.9 billion users. In combination with the other members, it becomes apparent that mega-merger of companies in the network has potential synergy effects (Vizjak, 1994), which are driven by the industry expertise and the interlocking of the services and products on the network. Therefore, global acceptance will ensure that Libra is viable as a means of payment, bearing in mind that almost 1.7 billion adults today are without a bank account (Demirguc-Kunt et al., 2018).

China	225 million	**Nigeria**	70 million
India	190 million	**Mexico**	55 million
Pakistan	100 million	**Bangladesh**	55 million
Indonesia	95 million	**Rest of the World**	910 million

Table 2: The global share of the unbanked
Source: Adapted from (Demirguc-Kunt et al., 2018)

Digitalization and constant development have led to the widespread availability of financial services alongside traditional institutions, enabling customers to manage their accounts ad hoc via e-banking or banking apps. In relation to the aforementioned 1.7 billion without a bank account (see Table 2), an estimated 1.1 billion adults show evidence of mobile phone ownership, with the above countries showing at least 50% with mobile phones except Pakistan, while China even showed 82% mobile phone ownership (Demirguc-Kunt et al., 2018). This illustrates the current discontinuity with traditional institutions, together with increasing access to the Internet, which shows the importance of advancing toward digital payment systems. There are, however, some indications of a strategic orientation, which can be observed in the strong focus on the desired financial integration in emerging countries like India, thus explaining the possible expansion of international dominance by Facebook and the other members.

Nevertheless, Libra will certainly find acceptance as a store of value because the majority of the underprivileged belong to developing and emerging countries, which are often exposed to hyperinflation and poorly protected property rights due to governmental instability. Thus, Libra will also offer the characteristics of a unit of account and means of exchange, which will be critical when bootstrapping new services into existing operations. Compared to common crypto-asset platforms, which suffer from a high degree of system abstraction and complexity,

Libra can accelerate the inclusion of financial services into already well-established communication and messaging applications, justifying its successful adoption.

Take Facebook's attempt to integrate financial services into its messaging approach with WhatsApp Pay (2018) in India as an example: the project was successfully adopted into the daily operations of approximately 1 million Indians who performed financial operations through the application, which facilitated the transaction process, bank transfers, bill exchanges, and receipts by simply transmitting the amount to the recipient via a message. The response to WhatsApp Pay was positive and well received by users, who took advantage of the effortless handling of transactions, but most importantly, it was reinforced by users' already habitual use of WhatsApp for messaging and communication, making it less difficult to adopt (Times, 2019). Accordingly, the estimates of Credit Suisse[15] have shown the following relationships: the digital payment market in India is expected to grow from 200 billion US$ in 2018 to approximately 1 trillion US$ in 2023, and WhatsApp, with an average of 230 million users per day, is the most widely used application today, demonstrating a positive correlation with plans to move toward a global digital currency.

Against this background, the Libra Association as the protagonist will actively use the digital currency in payment operations with the involvement of its members. For instance, Uber, which operates in a purely cashless manner based on credit card payments, can integrate Libra as an optional payment method or even replace all other payment options on the platform. Assuming that Libra's acceptance increases over time, this could force other companies to either incorporate Libra into their payment operations for the global purchase of goods and services, as the digital payment industry has reached a significant level of importance for the current financial system and is expected to grow steadily until 2021 (Bansal et al., 2018).

[15]For further information on the digital payment market and the development please visit; `https://www.financialexpress.com/industry/technology/digital-payments-to-grow-to-1-trillion-by-2023-credit-suisse/1055252/`

5.2 Mid-term

In terms of innovation, the Libra network also provides a complete platform, offering programmable resources that enable the deployment of smart contracts and DApps, for which various financial service providers could emerge on the network, offering different types of applications and encouraging active engagement. The importance of smart contracts is demonstrated by Ethereum, which has enabled contract-based transactions with programmable capabilities on the network amounting to an estimated increase from 200,000 executed smart contracts in June to 1.5 million in November 2018, with 49 million unique addresses on the Ethereum platform[16]. In terms of DApps, the Ethereum platform has an estimated 2,637 DApps[17] deployed with approximately 20,000 daily active users, 61,380,000 transactions per day, and a transaction volume of 2,963,573 US$ per week, indicating an alignment toward decentralized applications and the growing trend of decentralized autonomous organizations (DAOs). Trending DApps on the platform are Compound.finance, which offers crypto loans and the ability to earn interest; Ethlance, which offers a decentralized job search marketplace; CryptoKitties, which offers unique crypto-collectibles in the form of kittens; Aragon, which enables the establishment and management of DAOs; and Prism, which can be used as an asset management platform for investments. However, the relevance of programmable capabilities symbolizes the need for publicly manageable smart contracts on the Libra network, as it drives competition and innovation between companies and start-ups (Agrawal, 2019).

More crucially, the widely discussed public threat that Libra might pose to other crypto-asset platforms can be denied from this perspective. The Libra network assumes a superior role as an intermediary between the mainstream market and crypto market, which is increasing due to growing acceptance at enterprise-level and further scalability improvements by Bitcoin, Ethereum and others that leverage the importance of

[16]Ethereum by the numbers, for more information visit; `https://media.consensys.net/ethereum-by-the-numbers-3520f44565a9` (18.10.2019)

[17]For the list of all DApps in the Ethereum blockchain, see; `https://www.Stateofthedapps.com/de/platforms/ethereum` (18.10.2019)

greater participation in the crypto market. One of many examples is Moon[18], which offers an Internet browser extension that ultimately enables the purchase of services on leading e-commerce platform Amazon using crypto-assets such as Bitcoin, Ether, and Litecoin. This demonstrates the relevance of including crypto-assets and digital payment systems in the financial market's further development. However, the current options for buying crypto assets after setting up a wallet are basically based on three types[19]: first, one can buy certain amounts directly via credit card; second, one can purchase via bank transfer, once by an automated clearing house process or with wire transfer, which is faster but charges higher fees; or third, one can buy certain amounts through deposits via debit card. This highlights the current requirement for users to either have a bank account or to use arbitrary financial services as an on-ramp option. In this context, Libra could facilitate entry barriers and accelerate participation in the crypto market, which would lead to an increasing demand for crypto assets. This would also mean that users of Libra would not be obliged to convert any coins into fiat money because all operations will be available over the network, from different services and goods among various markets.

In relation to this, the link between everyday users and companies to the crypto market can be accelerated by the industry expertise and established services of the members, which also offers the possibility of direct transfer from Libra-to-crypto and crypto-to-libra without the involvement of an external facilitator. For example Coinsbase, one of the most widely used crypto-exchange platforms and a member of the Libra Assocation, which includes 50 different crypto assets, including Bitcoin, Ether, Ripple, Litecoin, Dash and others. It is expected that Coinbase will likely offer the buy, sell and trade Libra coins on its platform, which is a direct on-ramp to the crypto market for users.

[18]For more details on the Internet browser extension and possible improvements of the crypto assets, visit; `https://techcrunch.com/2019/10/21/moons-browser-extension-lets-you-pay-with-bitcoin-on-amazon/`

[19]The payment options were retrieved from one of the largest crypto-exchange platforms; Coinbase (2015): `https://www.coinbase.com/buy-bitcoin`. Bitstamp (2013): `https://www.bitstamp.net/market/order/instant/`. Kraken (2011): `https://www.kraken.com/`

5.3 Long-term

In the long run, expectations about Libra's impact can be difficult to anticipate because of uncertainties, as it depends on the development of the Libra ecosystem. Operational risks such as system failures or outages can occur inside the network, and furthermore, market expectations and downturns can occur from the outside that require dynamic interventions for value preservation—all of these are considered in the further development of the Libra.

However, the digital payment system within the Libra network symbolizes strong competition and the potential to polarize the payment industry with a broad of financial services and mobile access, as well as the ability to ensure Libra's operability and provide a financial infrastructure for billions of people. As consequence, Libra could lead to disruptions in various industries and sectors, which can be described as follows:

(1) A universal unit of account could be achieved through the global acceptance of the digital currency.

(2) Traditional payment facilitators such as PayPal, ApplePay, and AliPay may lose importance, and thus face the decision to either apply for membership or be outperformed by the interconnected Libra network.

(3) Stablecoins might experience difficulty in following up because Libra will be backed by the collateral of different currencies and government securities, thereby achieving superior value preservation compared with stablecoins per se, which are tied to a single reference asset such as the US dollar.

(4) In line with the digital payment system, the Libra network holds the potential to achieve a superior position as a programmable platform with the use of smart contracts and DApps growing into a new marketplace, which also lays the foundation for DAOs, but requires further improvements before being opened up to the public.

6 Risk Factors

This chapter identifies potential risk factors based on the impact of Libra, which are divided into three main dimensions.

6.1 Economic Aspects

By combining the capabilities of central banks embedded in the hypocritical use of blockchain technology, the Libra Association inherits two powerful domains. This could lead to obscurity because of little comprehensive knowledge, and therefore promote economic freedom under false pretences. In relation to central banks, the Libra network contains assets represented by the initial investments of members, deposits in the form of fiat money from users purchasing coins, and liabilities from issued coins that represent a financial claim on real-world assets (King, 2004). The difference between assets and liabilities results in equity, which, in contrast to central banks, will be exclusively owned by the Libra Association (King, 2004). In this context, any increase in the value of the collateral or the interest generated by the deposits will be used to pay dividends to the validators, followed by system maintenance, where users are not entitled to the generated surplus from the reserve. Notably, the Libra Association can conduct monetary policy measures with the ability to create coins when users make deposits and burn coins when users withdraw from the network; additionally, the coins are covered at a 1:1 ratio, which prevents inflationary manifestations in the network (Sims, 2016).

Another critical implication is that Libra could take control of government-issued currencies, such as the US dollar, which depends on foreign governments holding US Treasuries with the promise of repayment; this enables the United States government to maintain operability without sinking into budget deficits (Beltran et al., 2013). Note that Libra is supported by short-term securities and long-term government bonds from different countries, which allows some strategic investment decisions based on the management of the reserve that could jeopardize governments' mone-

tary sovereignty as well as the national security of the domestic market. Therefore, Libra could exert pressure on governments that refuse to cooperate and support those that comply with the network. For example, potential risks could arise if foreign governments decide to hold Libra instead of the US dollar (e.g., US Treasuries), which on the one hand would heighten the U.S. federal budget deficits[20] that must be offset, probably from printing money[21], but on the other hand it would displace the US dollar as the leading global reserve currency, which historically makes up 60% of central bank reserves (Choi and Park, 2009).

As an illustration, assume that 1% of the approximately 2.3 billion Facebook users decide to hold Libra, which is equal to 23 million Libra users. Furthermore, expect Libra to be valued at $1 and monthly demand for the coins to be approximately 1,000, resulting in $23 billion US$, from which an average demand of 12,000 coins can be derived that equals 276 billion US$ per annum (or arbitrary currency from international investors). The assumption of only 1% already indicates the enormous amount of fiat money that would enter the network, which only accounts for a fraction of existing users. This should also highlight the potential outflow of fiat money, which in the worst case could lead to possible capital flights (Alesina and Tabellini, 1989), thereby possibly destabilizing the financial system and being responsible for the devaluation of certain currencies. Then, governments and central banks would not be able to control the outflow anymore and be limited in the possibilities for an intervention, because fiscal and monetary policy would be ineffective (Josh, 2018) if the majority decides to hold Libra instead of US dollars, pound sterling, euros, or other currencies, entailing significant risk factors for the financial and monetary system, which would expand to a global perspective.

[20] Current budget deficits result in 1.109 trillion US$. For further information visit; `https://www.thebalance.com/current-u-s-federal-budget-deficit-3305783`

[21] The Fed has printed an additional 210 billion US$ since mid-September, which has entered the economy, see; `https://cointelegraph.com/news/the-fed-just-printed-more-money-than-bitcoins-entire-market-cap`

6.2 Regulatory Aspects

The rejection of Libra by regulators implies that regulatory requirements may represent the greatest burden, because regulators (mainly from the US, but also from the European Union and Switzerland) have expressed concerns about the effective regulatory instruments for blockchain-based currencies with regard to know your customer (KYC), anti-money laundering(AML) and combating the financing of terrorism (CFT) standards. The new technology implies several problems for governments in relation to tax evasion, fraud, and illegal activities by unauthorized persons that may be circumvented by individuals through these networks. The Swiss Financial Market Supervisory Authority (FINMA) is an independent financial market regulator that has published directives on regulatory requirements for the use of blockchain technology in Switzerland. In response to the increasing growth of blockchain-based business models over the past decade, FINMA has committed to protecting the domestic market from unexpected shocks that may result from poor regulatory standards on blockchain technology. FINMA also addresses service providers in Switzerland who are subject to the Anti-Money Laundering Act, which requires transparency and verification of the identity of clients suspected of being subject to unconventional conduct or money laundering (FINMA, 2018).

In addition, the Financial Action Task Force[22](FATF), which also deals with AML and CFT measurements, has issued standards stipulating that information from token transactions of clients and beneficiary clients must be published for transparency like a traditional bank transfer. Article 10 of AMLO-FINMA requires stakeholders to publish a complete list of suspicious clients on the network with their transaction report (FINMA, 2018), and if a client wishes to submit a transaction with blockchain-based currencies, he or she must prove the relationship between the external wallet before acting by technical means, as set out in the official report.

[22]For further information on FATF visit; `https://www.finma.ch/en/finma/international-activities/policy-and-regulation/fatf/`

The borderless spectrum of the network implies that regulation will either be ineffective or inadequate because the digital currency will operate globally, thereby affecting several governments, or even lead to sanctions that may affect the continuity of the Libra network. However, this is only the beginning of an extensive process of regulatory approval and licensing where the obligation exists to disclose the company's objectives and purposes, which could be successful from the point of view of regulators but will ultimately compromise the privacy of users on the network.

Evidence of the circumvention of regulatory requirements can be expected from the testimony from Facebook CEO Mark Zuckerberg in front of the House Financial Services Committee, in which he said: "Facebook will not be part of launching the Libra payments system anywhere in the world until US regulators approve."[23] Facebook was originally included as a member of the association in the Libra White Paper after the announcement of the project; however, since the official formation of the Libra Association on October 15, Facebook is no longer included—it will operate indirectly through Calibra, suggesting the potential problems and complexity behind the Libra project. Both international and U.S. regulators will have difficulty addressing Libra's responsible stakeholders because the Libra Association is a nonprofit organization based in Switzerland that depends on a global consortium of equal rights. At some point, Libra may even be subject to the regulatory requirements of Basel III/IV[24], which sets the international capital requirements for financial institutions that impose a systematic risk to the global economy with a too-big-to-fail (TBTF) intervention in the event of a default, which would trigger a financial crisis. The unique form of the project must be defined with custom rules that will be exclusively adjusted for the Libra Association as it is not a bank per se.

[23]For the full report on Mark Zuckerberg's Libra testimony in front of the HFSC, visit; `https://docs.house.gov/meetings/BA/BA00/20191023/110136/HHRG-116-BA00-Wstate-ZuckerbergM-20191023-U1.pdf`

[24]The Basel Committee on Banking Supervision has published the Basel III, which sets the global regulatory framework for more resilient banks and banking systems with the finalizing of the post-crisis reforms. Further reading; `https://www.bis.org/publ/bcbs189.pdf`; `https://www.bis.org/bcbs/publ/d424.pdf`

6.3 Privacy Aspects

The Libra project is faced with several privacy concerns, not only because of Facebook's involvement but also regulatory pressure based on AML and CFT standards, which will most likely be achieved over KYC authentication requirements. Moreover, technical specifications such as the governance of the Libra Association—and thus of the centralized network—supports the presumption that it could not only filter data to comply with regulatory requirements, but also use the information for other purposes.

"An additional goal of the association is to develop and promote an open identity standard. We believe that decentralized and portable digital identity is a prerequisite to financial inclusion and competition.". [25]

Next to the need for a global digital currency and financial infrastructure, Libra exhibits evidence for a rather hidden objective with the increasing relevance of digital identities (DIDs) in the financial market's current development. The statement above leads to the question of what the true objectives should be, will they improve the payment industry, or—with control over DIDs and enhanced visibility of users' financial information—lead to transparent monitoring of citizens' sensitive data in the digital sphere. Notably, Facebook has positioned itself as gatekeeper with its subsidiary Calibra committed to the authentication of users who want to join the network, which ultimately allows the company to take the next step toward building a surveillance state (Khan and Goodell, 2019). An emerging market that has been ongoing for several years, better known as the transparent citizen (Reidenberg, 2015), is already highly competitive, with some of the leading companies such as Google and Microsoft working on decentralized personal identity solutions. The current estimates on the DID market imply that the market is expected to reach 34 billion US$ in 2024 (Insight, 2019).

[25] Statement from the Libra White Paper, S.8 (Association et al., 2019*a*)

7 Discussion

"The Libra project shows 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."[26]

Certainly, several lessons can be drawn from the disclosure of the technical specifications that allow Libra's current drawbacks to be highlighted. From this perspective, the Libra project can be identified as a profitable business case cleverly wrapped in some common terminologies of blockchain technology, which can easily lead to obscurity among the bright mass. In contrast to the abovementioned statement, Libra will rely on a permissioned blockchain with the Libra Association as the gatekeeper and the members as validators, who must be approved based on predefined conditions to participate in the verification process. Thus, users will not have any decision-making or voting rights in the network. Moreover, Libra will not have the characteristics of traditional crypto assets[27], as no cryptographic incentives can be identified, but will rather be classified as digital currency secured by the collateral of real-world assets, which represents a financial claim.

"Unlike previous blockchains, which view the blockchain as a collection of blocks of transactions, the Libra Blockchain is a single data structure that records the history of transactions and states over time."[28]

Apparently, the Libra Blockchain will neither contain blocks nor a chain, but will rather be defined by a single-version database that stores sequentially ordered transactions in the ledger history. The ledger will be managed by the consortium, which rather resembles book-keeping instead of a cryptographically secured blockchain. From the current perspective,

[26] Statement from the Libra White Paper, S.1 (Association et al., 2019*a*)

[27] According to the ECB an crypto-asset is recorded in digital form enabled through cryptography with no financial claim on, or a liability of, any identifiable entity. See; `https://www.ecb.europa.eu/paym/intro/mip-online/2019/html/1906_crypto_assets.en.html`

[28] Statement from the Libra White Paper, S.6 (Association et al., 2019*a*)

it can be concluded that the network will be centralized in every respect, where any advantages of public and decentralized blockchains will disappear from the users' perspective.

Technically, several distinctions within the specifications can be highlighted in the Libra documents, such as the two-tier management by the association for investment decisions and by the protocol for the rules of validators in the verification process. This questions the efficient allocation of decisions in different stages, as well as presents difficulties for implementing regulatory measurements. Furthermore, risks from the decisions in reserve management and asset allocation should be considered; however, no statements have been made on how the association will actively absorb changes in the collateral's value on a larger scale. These changes could simultaneously invoke liquidity risks if users decide to collectively withdraw funds from the network, similar to a bank run, which could lead to system failures of the Libra network as well as to risks to central banks and influence over interest rates in the financial market. Furthermore, the regulatory pressure raises concerns about how users' confidential data will be calibrated in the already highly afflicted network, because the Libra Association will most likely be forced to initiate KYC requirements to comply with AML and ATF standards. Therefore, Calibra, as a custodial wallet, will represent a target for members because it is the gateway between users and the Libra network; users will most likely need to identify themselves to enter the wallet function. The consensus protocol with LibraBFT provides faultless processing and system integrity; however, deviating nodes will be penalized, yet the ambiguous identity of validators in the QCs will make it difficult to determine who has followed the rules. This leads to the assumption that the consortium will most likely suffer from collective reputation costs because sanctions against single nodes will be impossible. Authenticated data structures are used to represent the database, where users who send queries can receive a replica of the database with their entire transaction history. This is found in public blockchains, and therefore, how validators will secure the information in the network is unclear. Furthermore, Move will enable programmable resources and modules for custom assets

and contract-based transactions, but because the options will not be initially public, only validators will be allowed to deploy smart contracts and DApps, which will ultimately limit the users' ability in the network. It can be argued that the Libra Association probably wishes to prevent smart contracts being deployed by users in order to avoid hackers abusing loopholes in the poorly specified codes, which could lead to terrible consequences for users, such as Ethereum's DAO Hack[29]. Currently, users have two options to enable smart contracts, either throughout a hard fork or the transition of the network.

From the current perspective, however, the rather poorly formulated plan for a transition towards permissionless with the PoS algorithm can be disproved. First, this transition would ultimately weaken the influence of the validators and allow users to take control of the network's development, which would only be feasible if the members manage to withdraw their investments while keeping the system running based on a sufficient amount of user deposits. Second, the PoS mechanism can scarcely be applied in a permissionless network because long-range attacks and nothing-at-stake problems are common limitations. More specific, if a fork occurs, validators will build on each branch to increase their probability of receiving the transaction fee because it is impossible to anticipate which will be accepted by the peers in the network (Buterin et al., 2014). As an aside, splitting the computing power in the PoW mechanism would decrease the profits of miners because of the higher cost of mining, whereas it would increase the likelihood of obtaining rewards without additional cost to the validators in the PoS mechanism. Possible solutions were proposed such as the Slasher algorithm, which is based on punishing miners who divide their computing power into several branches; however, because mining is based on probabilistic outcomes, validators can hold back a block for seconds and still maximize their likelihood of receiving the reward (Buterin, 2014). Therefore, Libra will most likely run into the same problems as

[29]Next to the Dao Hack, which led to a loss of 3.6 million Ether, there were others such as Parity's Multi-sig Wallet Hack and the Parity User-triggered Wallet Freeze Hack, which also led to significant losses caused by loopholes and vulnerabilities in the code. For further information visit; `https://medium.com/firmonetwork/3-famous-smart-contract-hacks-you-should-know-dffa6b934750`

Ethereum, which took the first step with the Casper protocol[30] and the Istanbul hard fork toward the transition; however, various inefficiencies still remain for the PoS mechanism in permissionless blockchains, which require more sophisticated solutions before efficiency can be guaranteed. In general, the network could perhaps shift to the PoS mechanism, but the stable value of Libra—which is backed by real-world assets—implies that some nodes will be required to have a foothold in the financial market, thereby making the permissionless consensus rather implausible.

The scope of the project's overarching network implies that Libra requires an international agreement between governments and responsible institutions committed to monitoring the financial stability. In this context, uniform guidelines and regulatory frameworks must be applied to ensure global operability, which in consideration of the technical specifications are hardly discernible from today's perspective. There are few arguments that support the need for a rather failed attempt to integrate blockchain technology into a digital payment system, which other companies such as PayPal, AliPay and WeChat Pay have successfully achieved without the use of blockchain. Nevertheless, the potential impact behind the Libra network should not be underestimated because it is about to build a borderless monetary system—a digital central bank—run by private companies outside of national governments and borders.

Should the Libra Association still decide against all odds to launch the project, there could be a divided impact, as the functionality and operability will be banned in some regions [31]; others will accept Libra in some of their daily operations, such as buying memberships for Spotify or pay for the Uber rides; as well as people from emerging countries who can use Libra to protect their money from depreciation due to instability of the government and benefit from the advantages of the network, which offers efficient transaction operations and value preservation.

[30]For an insight in the various problems and limitations of the PoS mechanism in the permissionless blockchain, visit; `https://medium.com/belem-blockchain/the-ethereum-casper-project-part-2-3-e6e746c40baa`

[31]France and Germany announced to ban Libra. Further information; `https://www.reuters.com/article/us-facebook-cryptocurrency-france-german/france-and-germany-agree-to-block-facebooks-libra-idUSKCN1VY1XU`

8 Conclusion

In conclusion, the Libra project exhibits several differences to conventional blockchain and crypto-asset platforms. The Libra Association will follow its vision to provide an efficient global payment system and financial infrastructure for billions of people. However, Libra can neither offer short-term profits according to its stable value nor ensure the anonymity of users throughout the governance of the consortium in the thoroughly centralized and permissioned blockchain network. However, it will provide the necessary characteristics of traditional money that allow efficient money transfers and cross-border transactions to be processed within seconds under minimal fee structures in people's daily financial operations. Furthermore, the programmable platform holds the potential to evolve into an international marketplace for smart contracts and DApps, allowing companies and start-ups to integrate ideas and promote innovation to become a serious competitor to platforms such as Ethereum; however, since this option will not be publicly available, only validators will be allowed to conduct this task. Against this background, the current opposition of regulators, policymakers, legislators, governments, and crypto experts has indicated the potential risks from external effects from a macroeconomic perspective, such as the threat to government sovereignty and national security, as well as the destabilization of financial markets throughout the monetary shift in the economy associated with the immense size of the project.

Libra can be expected to be accepted much faster and have more users than other blockchain-based currencies because it is focused on intuitive use with the bootstrapping of financial services in existing applications, and also because the digital currency will provide key characteristics such as a medium of exchange, a medium of account, and a store of value, enabling efficient money transfers, value preservation, and the purchase of goods and services. If the mass adoption of Libra leads to increasing participation and global acceptance, the Association will have enormous inflows of government-issued currencies in the reserve, and the ability to apply monetary policy measures implies that Libra could become sys-

tematically relevant in a short period. Consequently, the question arises of whether a network of private and mostly for-profit companies should be allowed to gain such influence over the global economy, where fluctuations or the collective withdrawal of funds by users could lead to defaults in and interruptions to the Libra system, which could also necessitate bailouts or TBTF packages that will be carried by the tax payers and therefore the citizens of various countries.

As the project is still in the development phase, the final impact of Libra could not be estimated at the time of the analysis, where the paper has tried to develop a differentiated perspective on the assessment of Libra, as the dynamics of the project are likely to change over time depending on the environment. However, it can be assumed that even if the Libra Association manages to adapt to all requirements, Libra will not replace traditional fiat money, as it is itself dependent on a basket of different fiat currencies that define its value, which will be affected in the event of a financial crisis and other events in which Libra will not provide an optimal solution. It will be interesting to follow the further development of the Libra project in order to assess whether the benefits will outweigh the current constraints that will be observed during the introduction of Libra in the first half of 2020.

Critical Appraisal

The following master's thesis was written in the context of the development of the Libra project, which in the meantime can differ in numbers and content, as it only covers the period up to 1 December 2019. In addition, implications were formulated based on predictions from the available data and research of existing business statistics to predict the magnitude of Libra. Therefore, no guarantee can be given for the accuracy of the information contained in this analysis.

Appendix

Facebook (2004) has an estimated 2.41 billion active users per month, with 1.58 billion active users per day, which represents approximately 66% of monthly users. In terms of demographics, India accounts for 270 million users, followed by the United States with 190 million, Indonesia with 130 million, Brazil with 120 million, Mexico with 82 million, the Philippines with 68 million, Vietnam with 58 million, Thailand with 46 million, and smaller shares among other countries. Facebook benefits from the integration of services in its messaging approach, such as Messenger, WhatsApp, and Instagram, which reflects Facebook's presence on the market. In 2018, Facebook's estimated annual return amounted to 55.84 billion US$, which was mainly from advertising; however, key findings suggested that 92% of its revenue comes from mobile phones, demonstrating Facebook's integration of mobile devices (Celement, 2019*a*). Facebook acquired WhatsApp in 2014, which enables instant messaging and online chats over the Internet worldwide; users can communicate, make phone calls, and share pictures and videos. WhatsApp has an estimated 1.6 billion active users per month and 500 million active users per day, making it the most widely used mobile chat application. Facebook Messenger ranks second in global mobile chat app ratings with an estimated 1.3 billion active users per month (Celement, 2019*c*). Note that an overlap in users is expected because both apps can be used simultaneously, but WhatsApp users do not need to have Facebook accounts and vice versa. The last application is Instagram with an estimated 714 million active users per month, which is expected reach 989 million users over the next 3 years (Celement, 2019*b*).

Uber (2016) is a global ridesharing app, which is mainly active in public transport but also offers food delivery services through Uber Eats. In 2018, Uber had an estimated 95 million active users per month, resulting in net sales of 11.3 billion US$ from approximately 5.23 billion trips booked. An expected increase of 15 million users by the first quarter of 2020 will lead to a total of 100 million active users per month, with an increasing trend over the next few years (Mazareanu, 2019).

Lyft (2012) is also a ridesharing app that competes in the transportation sector, which focuses on the Canadian and U.S. markets. In 2017, Lyft had an estimated net sale of 1 billion USD, which was achieved from 375.5 million rides booked via the app. The following year, net sales increased to an estimated 2.1 billion USD with approximately 551 million trips, making it the second-largest public transport application

Spotify (2013) offers a global music streaming platform based on monthly subscription fees via the Spotify App, which creates audio content that allows the streaming of almost any mainstream musician/group and features multiple music labels such as Universal, Sony, and Warner Music Group. In 2018, the streaming platform generated net revenues of 5.26 billion EUR, with 225 million active users in total, which grew to an estimated 232 million in the second quarter of 2019. This makes it one of the most popular streaming applications for the music industry (Watson, 2019).

The Vodafone Group (2008), as a global telecommunications provider, is based in India, South Africa, Germany, Italy, Spain, Great Britain and the United States. In 2019, Vodafone achieved an estimated total revenue of 43.67 billion EUR, of which 10.9 billion EUR was generated in Germany. Vodafone benefits from its distributed locations, where the total number of mobile phone users is estimated at 468.2 million, of which 334.1 million are exclusively located in India (Horst, 2019).

Coinbase (2012) is one of the leading crypto-exchange platforms, which includes crypto assets such as Bitcoin, Ether, Litecoin, Dash and many others. In the first half of 2018, an estimated 7.1 million users on average were actively trading on the platform, reaching a peak in January with 11.1 million users and the lowest number of 5.6 million users in June (Szmigiera, 2019). The fluctuations in users were determined by observing market expectations and news related to regulations and policy changes.

References

Agrawal, H. (2019), '9 best dapps on ethereum platform that you can use right', *Coinsutra* . https://coinsutra.com/ethereum-dapps/.

Akcora, C. G., Dixon, M. F., Gel, Y. R. and Kantarcioglu, M. (2018), 'Blockchain data analytics', *Intelligent Informatics* p. 4. http://www.comp.hkbu.edu.hk/~cib/2018/Dec/iib_vol19no2.pdf#page=6.

Alesina, A. and Tabellini, G. (1989), 'External debt, capital flight and political risk', *Journal of international Economics* **27**(3-4), 199–220. urlhttps://www.nber.org/papers/w2610.pdf.

Amsden, Z. et al. (2019), 'The libra blockchain'. https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf.

Association, L. et al. (2019*a*), 'An introduction to libra'. https://libra.org/en-US/white-paper/.

Association, L. et al. (2019*b*), 'The libra association'. https://libra.org/en-US/wp-content/uploads/sites/23/2019/08/TheLibraAssociation_en_US-Rev0814.pdf.

Association, L. et al. (2019*c*), 'Moving to a formal governance structure'. https://libra.org/wp-content/uploads/2019/10/Libra-Association-Charter-Press-Release-.pdf.

Bano, S., Catalini, C., Danezis, G., Doudchenko, N., Maurer, B., Sonnino, A. and Wernerfelt, N. (2019), 'Moving toward permissionless consensus'. https://libra.org/en-US/wpcontent/uploads/sites/23/2019/08/MovingTowardPermissionlessConsensus_en_US_Rev0814.pdf.

Bano, S. e. a. (2019), 'State machine replication in the libra blockchain'. https://developers.libra.org/docs/state-machine-replication-paper.

Bansal, S., Bruno, P., Denecker, O. and Niederkorn, M. (2018), 'Global payments - a dynamic industry continues to break new

ground', *McKinsey and Company* . https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Global%20payments%20Expansive%20growth%20targeted%20opportunities/Global-payments-map-2018.ashx.

Bashir, I. (2018), *Mastering blockchain: Distributed ledger technology, decentralization, and smart contracts explained*, Packt Publishing Ltd.

Beltran, D. O., Kretchmer, M., Marquez, J. and Thomas, C. P. (2013), 'Foreign holdings of us treasuries and us treasury yields', *Journal of International Money and Finance* **32**, 1120–1143.

Berentsen, A. and Schär, F. (2017), 'Bitcoin, blockchain und kryptoassets: Eine umfassende einführung', *Aufl.Norderstedt: BoD–Books on Demand* .

Bertoni, G., Daemen, J., Peeters, M. and Van Assche, G. (2013), Keccak, *in* 'Annual international conference on the theory and applications of cryptographic techniques', Springer, pp. 313–314.

BFS (2019), 'Swiss consumer price index', *BFS* . https://www.bfs.admin.ch/bfs/en/home/statistics/prices/consumer-price-index.html.

Blackshear, S., Cheng, E., Dill, D. L., Gao, V., Maurer, B., Nowacki, T., Pott, A., Qadeer, S., Rain, D. R., Sezer, S. et al. (2019), 'Move: A language with programmable resources'. https://developers.libra.org/docs/assets/papers/libra-move-a-language-with-programmable-resources.pdf.

Buterin, V. (2014), 'Slasher: A punitive proof-of-stake algorithm', *Ethereum Blog* . https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/.

Buterin, V. (2015), 'Vitalik buterin: On public and private blockchains'.

Buterin, V. et al. (2013), 'Ethereum white paper', *GitHub repository* pp. 22–23. https://github.com/ethereum/wiki/wiki/White-Paper#ethereum.

Buterin, V. et al. (2014), 'Ethereum white paper: a next generation smart contract & decentralized application platform', *First version* . https://github.com/ethereum/wiki/wiki/White-Paper.

Catalini, C., Gratry, O., Hou, J. M., Parasuraman, S. and Wernerfelt, N. (2019), 'The libra reserve', *Libra White Paper* . https://libra.org/en-US/wp-content/uploads/sites/23/2019/08/TheLibraReserve_en_US_Rev0814.pdf.

Celement, J. (2019*a*), 'Facebook statistics and facts', *Statista* . https://www.statista.com/statistics/346167/facebook-global-dau/.

Celement, J. (2019*b*), 'Instagram statistics and facts', *Statista* . https://www.statista.com/statistics/183585/instagram-number-of-global-users/.

Celement, J. (2019*c*), 'Whatsapp statistics and facts', *Statista* . https://www.statista.com/topics/2018/whatsapp/.

Choi, G. and Park, H. (2009), 'A reform of the international monetary system'.

Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V. et al. (2016), 'Blockchain technology: Beyond bitcoin', *Applied Innovation* **2**(6-10), 71.

Dei, W. (1998), 'B-money protocol', *Cypherpunks Archives* . http://www.weidai.com/bmoney.txt.

Delgado-Segura, S., Pérez-Sola, C., Navarro-Arribas, G. and Herrera-Joancomartí, J. (2018), Analysis of the bitcoin utxo set, *in* 'International Conference on Financial Cryptography and Data Security', Springer, pp. 78–91. https://eprint.iacr.org/2017/1095.pdf.

Demirguc-Kunt, A., Klapper, L., Singer, D., Ansar, S. and Hess, J. (2018), *The Global Findex Database 2017: Measuring financial inclusion and the fintech revolution*, The World Bank. https://globalfindex.worldbank.org/.

FINMA (2018), 'Guidance - payments on the blockchain', *FINMA* . https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20190826-finma-aufsichtsmitteilung-02-2019.pdf?la=en.

Hollander, L. (2019), 'The ethereum virtual machine: How does it work?', *Medium* . https://medium.com/mycrypto/the-ethereum-virtual-machine-how-does-it-work-9abac2b7c9e.

Horst, A. (2019), 'Vodafone group statistics and facts', *Statista* . https://www.statista.com/statistics/241610/revenue-of-vodafone-since-2008/.

Insight, G. M. (2019), Personal identity management market size, industry outlook, regional analysis, application development, competitive landscape & forecast 2019-2025, Global Market Insight. https://www.gminsights.com/industry-analysis/personal-identity-management-marketf.

Josh, Z. (2018), 'Imf warns of possible emerging-markets crisis', *The Wall Street Journal* . https://www.wsj.com/articles/imf-warns-of-possible-emerging-markets-crisis-1539129600?tesla=y.

Khan, V. and Goodell, G. (2019), 'Libra: Is it really about the money?', *Available at SSRN 3441707* . https://arxiv.org/ftp/arxiv/papers/1908/1908.07474.pdf.

King, M. (2004), 'The institutions of monetary policy', *American Economic Review* **94**(2), 1–13. https://www.jstor.org/stable/pdf/3592848.pdf.

Lamport, L., Shostak, R. and Pease, M. (1982), 'The byzantine generals problem', *ACM Transactions on Programming Languages and Systems (TOPLAS)* **4**(3), 382–401. https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf.

Li, W., Andreina, S., Bohli, J.-M. and Karame, G. (2017), Securing proof-of-stake blockchain protocols, *in* 'Data Privacy Management, Cryptocurrencies and Blockchain Technology', Springer, pp. 297–315. http:/www.ghassankarame.com/CBT_Blockchain17.pdf.

Mazareanu, E. (2019), 'Uber statistics and facts', *Statista* . https://www.statista.com/statistics/833743/us-users-ride-sharing-services/.

Merkle, R. C. (1987), A digital signature based on a conventional encryption function, *in* 'Conference on the theory and application of cryptographic techniques', Springer, pp. 369–378. https://link.springer.com/content/pdf/10.1007/3-540-48184-2_32.pdf.

Nakamoto, S. (2008), 'Bitcoin: A peer-to-peer electronic cash system'. https://bitcoin.org/bitcoin.pdf.

Nakamoto, S. et al. (2019), 'Unspent transaction output'. https://bitcoin.org/en/blockchain-guide#introduction.

Poddebniak, D., Somorovsky, J., Schinzel, S., Lochter, M. and Rösler, P. (2018), Attacking deterministic signature schemes using fault attacks, *in* '2018 IEEE European Symposium on Security and Privacy (EuroS&P)', IEEE, pp. 338–352.

Ray, J. et al. (2013), 'Ethereum accounts and not utxo's', *GitHub repository* pp. 22–23. https://github.com/ethereum/wiki/wiki#accounts-and-not-utxos.

Reidenberg, J. R. (2015), 'The transparent citizen', *Loy. U. Chi. LJ* **47**, 437. https://heinonline.org/HOL/Page?handle=hein.journals/luclj47&div=14&g_sent=1&casa_token=&collection=journals.

Reyzin, L. and Yakoubov, S. (2016), Efficient asynchronous accumulators for distributed pki, *in* 'International Conference on Security and Cryptography for Networks', Springer, pp. 292–309. https://eprint.iacr.org/2015/718.pdf.

Sims, C. A. (2016), Fiscal policy, monetary policy and central bank independence, *in* 'Kansas Citi Fed Jackson Hole Conference'. https://cache-igetweb-v2.mt108.info/uploads/1575/filemanager/be86c36ea82e26503b67af5dd140038a.pdf.

Szabo, N. (2005), 'Bit gold.(1998)'.

Szmigiera, M. (2019), 'Coinbase statistics and facts', *Statista* . https://www.statista.com/statistics/803531/number-of-coinbase-users/.

Times, F. (2019), 'Whatsapp's push into mobile payments', *Financial Times* . https://www.ft.com/content/e045cdd2-0503-11e9-99df-6183d3002ee1.

Valenta, M. and Sandner, P. (2017), 'Comparison of ethereum, hyperledger fabric and corda', *[ebook] Frankfurt School, Blockchain Center* . https://pdfs.semanticscholar.org/00c7/5699db7c5f2196ab0ae92be0430be4b291b4.pdf.

Vizjak, A. (1994), 'Exploiting your synergy potential: promoting collaboration between business units', *Long Range Planning* **27**(1), 25–35. https://www.sciencedirect.com/science/article/abs/pii/0024630194900043.

Watson, A. (2019), 'Spotify statistics and facts', *Statista* . https://www.statista.com/topics/2075/spotify/.

Wood, G. et al. (2014), 'Ethereum: A secure decentralised generalised transaction ledger', *Ethereum project yellow paper* **151**(2014), 1–32.

Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K. (2016), 'Where is current research on blockchain technology?—a systematic review', *PloS one* **11**(10), e0163477.