Facebook's Libra: Big Bang or Big Crunch? A Technical Perspective and Challenges for Cryptocurrencies

Article *in* SSRN Electronic Journal · August 2019

DOI: 10.2139/ssrn.3445150

CITATIONS
0

READS
233

1 author:

John Taskinsoy
Istanbul Aydin University
29 PUBLICATIONS **215** CITATIONS

SEE PROFILE

Facebook's Libra: Big Bang or Big Crunch? A Technical Perspective and Challenges for Cryptocurrencies [*]

Dr. John Taskinsoy [a]

ABSTRACT

Libra cryptocurrency is a new invention; as with any disruptive invention, Libra blockchain presents some risks. Facebook's formal announcement of Libra had the "big bang" effect in the cryptocurrency markets; equally, the industry will witness "big crunch" if Libra sputters out resulting from a failure to receive all appropriate approvals from central banks, regulators, and law makers who are eager to run headlong into backlash to Libra in order to punish Facebook with a troubled past of privacy abuse and exploitation of users' data. Libra's unique features are distinctly different from Bitcoin and over 2,400 altcoins. Although Facebook claims Libra as a permissioned decentralized blockchain, but this is far cry from truth because Libra is a non-mineable cryptocurrency without the need of providing mathematical solutions to double spending problem. Under Bitcoin's permissionless decentralized blockchain without a trusted third party, every new bitcoin is minted through a mining process which starts with a block, and then a ledger comprising timestamped transactions in a chronological order is distributed to all nodes (miners) in the Bitcoin network who check and validate transactions based on consensus before they are added to the end of each coin in its block. As a start, Libra blockchain will be governed by the Libra Association as a de facto central authority, which will initially comprise 28 private founding-members, each of which will act as a validator to ensure Libra's stability. Libra is cost efficient in electricity usage and more consistent than other cryptocurrencies; Libra's superior functionality, higher security, and vast scale due to its user base of nearly 3 billion will eventually make Libra become a viable alternative reserve crypto-currency to the dollar. Libra's proof-of-stake algorithm supported by a new programming language "Move" plus the use of LibraBFT consensus make Libra 1/3 more secure than Bitcoin, Libra can function correctly even if 1/3 of its network fails or hacked. Libra's PoS leads to higher transaction throughput, lower latency, and lower energy cost.

Keywords: Libra; Facebook; Libra Association; Cryptocurrency; Bitcoin; Blockchain

JEL classification: O31, G12, E42, C40

[*] This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

[a] Corresponding author email address: johntaskinsoy@gmail.com
Faculty of Economics & Business – Universiti Malaysia Sarawak (Unimas), 94300 Kota Samarahan, Sarawak, Malaysia.

1.0 Introduction

Throughout history, the evolution of money points to an alternated shift between commodity money and credit money (King, 1999; Goodhart, 2000). At the backdrop of ever more financial turmoil since the global financial crisis (GFC)[1] of 2008 along with the US' severe abuse of sanction power as a central focus of its foreign policy, the old interest in search for a viable alternative to the U.S. dollar such as Libra has reemerged (since the late 1990s, the U.S. has imposed 60 sanctions[2] on 35 nations). Central banks, regulators and law makers running headlong into backlash to Libra may backfire and cause inadvertent damages to consumers as well as adverse effects in future innovative technologies (see Reitman, 2019). Christine Lagarde, Managing Director of the International Monetary Fund (IMF), urged central banks not to ignore "winds of change" and consider looking into the case of central bank digital currency (Lagarde, 2018; Bech & Garatt. 2017; Mancini-Griffoli, 2018; McLeay et al., 2014).

The first wave of cryptocurrency research was in the early 1980s that began with Chaum's proposal for "untraceable payments" in 1983 (e.g. Chaum, 1982). The second wave consisting of variations and extensions of antecedent research was in the 1990s that proved to be a decade for groundbreaking events that took a leap of faith that internet would make the dream of electronic cash a reality (e.g. Woodford, 2000; Camenisch et al., 2005; Okamoto & Ohta, 1992). Applications such as combating email spam (Dwork & Naor, 1992; reasons of failure, see Laurie & Clayton, 2004), internet-based payment system (Sirbu & Tygar, 1995) and minting digital coins (Rivest & Shamir, 1997) never saw a widespread deployment. Furthermore, skepticism among risk-averse investors caused the notable attempts by DigiCash (Chaum et al., 1998; Schoenmakers, 1998) and Peppercoin (Rivest. 2004) to fail, in turn DigiCash (1990) filed for bankruptcy in 1998. In the late 1990s, two attempts at creating a decentralized digital currency emerged; "b-money"[3] by Wei Dai (Dai, 1998) and Bitgold by blockchain pioneer Nick Szabo[4] (Goldschlag & Stubblebine. 1998; Vishnumurthy et al., 2003; Okamoto & Ohta, 1992; Kocherlakota, 1998; Sander & Ta-Shma, 1999). One of the first successful attempts had a head

---

[1] Developments in technology and financial sectors have played an important role in the evolution of money. In the 1990s, the homegrown Asian crisis of 1997-98 prompted the introduction of the Financial Sector Assessment Program (FSAP) jointly developed by the IMF and World Bank in 1999 and stress testing became a mainstay in banking regulation and supervision. The savings glut, financial innovation (i.e. mortgage-backed instruments), and the Federal Reserve's (Fed's) expansive (i.e. cheap dollar) policy created a lax credit environment which ushered predatory lending practices, resulting in the 2006 mortgage debacle and the inevitable GFC of 2008 which marked the birth of Basel III, macro stress testing, and cryptocurrencies. China, Russia, Turkey, and Iran have been searching alternative mediums of exchange since The US' abuse of sanction power and its use of dollar as a weapon of mass economic destruction have been at the center of US foreign policy that caused political tensions (Taskinsoy, 2012; 2013a, b; 2018a, b, c, d; 2019a, b, c, d, e, f, g, h, i, j, k, l, m, n).

[2] Sanctions on Russia, Iran, Sudan, Venezuela, North Korea, Cuba, China, Qatar, Turkey, and EU have not deterred any of these countries' behaviors. Economists and historians believe that sanctions are counterproductive and damaging for the economies of all nations involved. For the past two decades, repeated sanctions imposed on Iran and North Korea have proved to be non-deterrent in the behavioral change of offenders (see Martin, 1990; Rogers, 1996; Pape, 1997).

[3] http://www.weidai.com/bmoney.txt

[4] Szabo (2005), "Bit Gold" available at: http://unenumerated.blogspot.rs/2005/12/bit-gold.html

on collision with the government; e-gold was established in 1996 and after reaching several million users over a decade of operation, it was shut down by the U.S. government in 2008.

Cryptocurrencies appeared on the map when a mysterious user under the alias Satoshi Nakamoto[5] created Bitcoin as a purely peer-to-peer network of electronic cash without the need of trusted-third parties; he made Bitcoin public by registering a domain name *"bitcoin.org"* (August 2008) and posting a White Paper to Cypherpunks mailing list in October 2008 entitled *"Bitcoin: A peer-to-peer Electronic Cash System"* (Nakamoto, 2008). During the design of Bitcoin, his prior knowledge of efforts regarding electronic cash in the 1990s helped him; he used proof-of-work similar to Adam Back's Hashcash (see Back, 2002), and learned from Merkle trees (Merkle, 1980; 1987), cryptographic proof (Chaum et al., 1998), and timestamping digital documents (see Haber & Stornetta, 1991, 1997; Bayer et al., 1993). Under the Bitcoin blockchain, a timestamp server timestamps a hash of a block of items and publishes the hash via distributed ledger which proves that the data and the relevant transaction existed (Law et al., 1996; Huang et al., 2014; Vishnumurthy et al., 2003). After Bitcoin's genesis block was mined in the first few days of January 2009; on January 12, as a symbolic transaction Satoshi sent 10 BTC to a computer programmer by the name of Hal Finley (Nakamoto, 2008). However sale of a good involving bitcoins occurred at the end of 2009, a bitcoin user swapped 10,000 BTC for an order of two pizzas from Papa Jones in the U.S.[6] (Kristoufek, 2015; Phillips & Gorse, 2017; Taskinsoy, 2018a, 2019c, d, e).

Unfortunately, Bitcoin soon after its debut in January 2009 has been associated with illicit activities; therefore, various branches of government authorities in countries have called for greater scrutiny of Bitcoin on terrorism-financing, money-laundering, illegal drugs (i.e. Silk Road[7]) and human trafficking (Bonneau et al., 2015; Gudgeon et al., 2019; Christin, 2013). Despite difficulty to get a grasp on the Bitcoin phenomenon (Franco, 2014; Sovbetov, 2018), still Bitcoin has gained immense popularity and become a household name (Wallace, 2011). When the price of bitcoin hit the $1,000 mark, investors' craving increased; the frenzy turned into mania when bitcoin price passed $10,000; and when bitcoin price hit the unprecedented $20,000 mark (i.e. intraday high of $20,089 in December 2017), even ordinary folks became avid Bitcoin enthusiasts/investors. During Bitcoin's decade-long existence, many Bitcoin owners have been subject to losses resulting from black market websites (i.e. Silk Road), collapsed exchanges (i.e. Mt. Gox; for risks, see Moore & Christin, 2013), Ponzi schemes (Huang et al., 2014) and Botnets which have been often used for spamming and criminal purposes.[8]

---

[5] Satoshi Nakamoto a pseudonym; his identity is unknown whether Satoshi even exists, and it is a he or she.
[6] Available online: http://www.bitcoin2040.com/bitcoin-price-history (accessed 10 August 2019).
[7] On October1, 2013 the FBI shut down the black market website Silk Road and seized its assets including 26,000 bitcoins.
[8] A Botnets uses Trojan viruses to control users' computers and Ponzi schemes are fraudulent investing scam s which are similar to a pyramid scheme where funds from new investors are used to pay the earlier investors.

Since Bitcoin's debut in January 2009, 2,446 cryptocurrencies have sprouted like wild mushrooms; nevertheless, Facebook's Libra cryptocurrency[9] is a recent invention with a brand new encryption language "Move" which is specifically developed for this purpose. Although the formal announcement of Libra has been metaphorically denoted as "big bang" due to its vast scale (a user base of nearly 3 billion), it could turn into a big blub if Facebook fails to receive all appropriate approvals from the U.S. Federal Reserve (the Fed) and regulators before the planned launch date of 2020 (perfect eye vision or blindfolded?). The transition of fiat money into cryptocurrency form is inevitable whether various government authorities like or dislike. Economists along with experts and advocates assert that most central bank gold reserves in the future will be supplemented by digital coins even if central banks, regulators, and law makers run headlong into backlash to Libra in order to punish Facebook that already has a troubled past of privacy abuse and exploitation of users' data (for Cambridge Analytica debacle, see Albright, 2018; Cohen, 2013; Coombs, 2005; for the rise of cryptocurrencies, see Adrian & Mancini-Griffoli, 2019; Andolfatto, 2018; Catalini et al., 2019; Chiu & Wong, 2014; Duffie, 2019).

In May 2019, Facebook registered Libra Networks LLC in Geneva, Switzerland. The term "Libra" was first used as a unit of weight in Ancient Rome, it is also one letter different from French word "libre" which is the root of "liberty or freedom". Libra's symbol of waves suggests that money flows without borders with hassle free and little or no transaction cost (LA, 2019). Unlike Bitcoin's permissionless decentralized blockchain without a trusted party (Nakamoto, 2008); however, Libra's permissioned decentralized blockchain with a trusted party will be governed by the Libra Association as a de facto central authority comprising 28 heavyweight founding-members mostly from the U.S. such as Visa, MasterCard, PayPal, Facebook Calibra, and eBay (Bonneau et al., 2015; Gudgeon et al., 2019; Lagarde, 2018; McLeay et al., 2014; Phillips & Gorse, 2017; Taskinsoy, 2018a, 2019c, d, e). At the backdrop increasing opposition among the ire central banks and the resultant pushback from the G7 (Reitman, 2019), a growing number of sovereign states are furious that Libra cryptocurrency will compete with currencies of developing nations, plus the Libra Association as a central governing body of Libra will make monetary policies as deemed necessary to keep the value of Libra stable.

Technically, many differences exist between Bitcoin and Libra; as a start, the most distinct difference is that Bitcoin is mineable with a preset maximum supply of 21 million coins, but Libra is not mineable with unlimited supply. Both Bitcoin and Libra are based on cryptography proof and run on blockchain as their infrastructure technology; for Bitcoin, the proof-of-work starts with the first block for every mined bitcoin and is based on cryptography where nodes (miners) solve double-spending problem, then a timestamp server timestamps a hash of a block of items and publishes the hash to all nodes in

[9] Also referred to as electronic money, digital money, cryptocurrency, digital cash, virtual money, and digital currency.

the network via the distributed ledger which proves that the data and the relevant transaction existed (Bayer et al., 1993; Haber & Stornetta, 1991, 1997; Massias et al., 1999). Libra, on the other hand, uses a new programming language specifically developed for Libra called "Move" (Blackshear et al., 2019) to execute transactions that are made visible to validators and clients by the Logical Data Model based on Merkle trees (Merkle, 1980; 1987). For safety and liveness, Libra uses HotStuff as the basis for Libra's Byzantine Fault Tolerant – LibraBFT (LA, 2019; Bernstein et al., 1987; Castro & Liskov, 1999; Pfitzmann & Köhntopp, 2001; Reed, 1978; Wood, 2016; Yin et al., 2018).

2.0 Literature Review

Many electronic cash schemes and online payment systems existed prior to Bitcoin but none of these earlier efforts saw a widespread deployment (Table 1). Some of the foundational work since the late 1970s paved the road to the inevitable birth of Bitcoin in 2009 as the first successful cryptocurrency; as such, Chaum's proposal of "untraceable payments" via anonymous cryptocurrency (Chaum, 1982); proof-of-work (PoW) such as combating email spam (Dwork & Naor, 1992; Laurie & Clayton, 2004); DigiCash (Chaum et al., 1998; security aspects, see Schoenmakers, 1998); Peppercoin (Rivest. 2004) and Lamport's consensus (Lamport, 1998). Two efforts at creating a decentralized cryptocurrency emerged; b-money (Dai, 1998), minting digital coins based on proof-of-work (Rivest & Shamir, 1997), and Bitgold by blockchain pioneer Nick Szabo (Goldschlag & Stubblebine. 1998; Vishnumurthy et al., 2003; Okamoto & Ohta, 1992; Kocherlakota, 1998; Sander & Ta-Shma, 1999). The advent of internet accelerated the speed of developments in the field of cryptocurrency (Woodford, 2000; Camenisch et al., 2005; Okamoto & Ohta, 1992). The last of the Mohicans, e-gold (established in 1996) after reaching several million users was shut down by the United States government in 2008 citing legal issues.

Table 1: Earlier Electronic Payments Systems & Proposals

ACC	CommerceSTAGE	Hashcash	Mini-Pay	PayMe	Secure Courier
Agora	Cybank	HINDE	Minitix	PayNet	Semopo
AIMP	CyberCash	iBill	MobileMoney	**PayPal**	SET
Allopass	CyberCoin	IMB-MP	Mojo	PaySafeCard	SET2GO
n-money	CyberGold	InterCoin	Mollie	PayTrust	SubScrip
BankNet	DigiGold	Ipin	Mondex	PayWord	Trivnet
Bitbit	Silk Road	Javien	MPTP	Peppercoin	TUB
Bitgold	E-Gold	Karma	Net900	PhoneTicks	Twitpay
Bitpass	ECash	LotteryTickets	NetCard	Playspan	VeriFone
C-SET	eCharge	Lucre	NetCash	Polling	VisaCash
CheckFree	eCoin	MagicMoney	NetCheque	Proton	Wallie
ClickShare	First Virtual	MicroMint	NetFare	Redi-Charge	Way2Pay
CommerceNet	FSTC	Micromoney	No3rd	S/PAY	WorldPay
CommercePOINT	Globe Left	MilliCent	One Click Charge	Sandia Lab E-Cash	X-PAY

Source: Narayanan et al (2016)

In the pre-Bitcoin world, traditional online transactions had relied on trusted third parties to perform three essential tasks; (i) to validate every transaction; (ii) to ensure secured execution of transactions; and (iii) maintain a chronology of transaction history. Blockchain became a household name after a mysterious creator the alias Satoshi Nakamoto launched Bitcoin in 2009[10] as a decentralized purely peer-to-peer electronic cash system without the need of a trusted central authority (see Nakamoto, 2008). Even a decade later many of us still do not understand blockchain technology (Katz & Lindell, 2014; Levy, 2001; Ferguson et al., 2012); in fact, some people see it as a magical invention to solve all our problems, but there may be unforeseeable hazards to this prophecy (Clarke, 1962). Facebook's Libra in essence is different from Bitcoin, it's so called decentralized blockchain with a trusted third party will be governed by the Libra Association as the de facto central authority (LA, 2019).

Unlike Libra (non-mineable), Bitcoin is a mineable cryptocurrency minted through a mining process[11] where miners (nodes) earn bitcoins as they solve double-spending problem based on proof-of-work (PoW) algorithm (i.e. proof-of-stake – PoS does not give rewards). Bitcoins enter the circulation via mining which is capped at a maximum supply of 21 million (Libra has unlimited supply), so far 17.3 million have been mined and the mining is forecast to end in 2140 when all of the 21 million bitcoins are in circulation (Hayes, 2017). As an incentive, miners (nodes) receive a reward for every block successfully added to the blockchain (Houy, 2014; Kroll et al., 2013). The reward size of 50 BTC per block began in 2009 and the first halving took place in 2012 where the reward was reduced from 50 BTC to 25 BTC (halving occurs after about 210,000 new blocks are added). After a second halving in 2016, the reward is currently at 12.5 BTC, which will be halved again for the third time to 6.25 BTC in 2020 (Hayes, 2015; Taskinsoy, 2018a). Between 2016 and 2019, about 150 bitcoins are mined per hour (3,600/day and 1,314,000/year); however, almost half of the mined bitcoins are sold to cover operational expenses. The cost of mining a single bitcoin varies significantly among countries due to electricity cost; the U.S. ranks 41st ($4,758), Russia ($4,675) and Iceland ($4,746) rank slightly better than the U.S.; South Korea is the costliest ($26,170) while Venezuela is the cheapest ($531).[12]

Both Bitcoin and Libra use cryptography as an encryption technique for security (Narayanan et al., 2016), nonetheless blockchain is not completely risk-free of cyberattacks or hacking (e.g. Yeoh, 2017;

---

[10] Satoshi Nakamoto supposedly worked about two years writing the codes for Bitcoin. Once writing of codes was completed, he registered the domain name bitcoin.org on 18 August 2008 and published his White Paper on 31 October 2008. Next, he kicked off Bitcoin project on 9 November 20008. On 3 January 2009, he created the genesis block (i.e. first block); a week later on 9 January 2009, Bitcoin v0.1 was released. As a symbolic first Bitcoin peer-to-peer transaction took place on 12 January 2009 when Satoshi sent 10 BTC to a computer programmer by the name of Hal Finley.

[11] A majority of 2,467 traded cryptocurrencies are non-mineable. Bitcoin as a mineable cryptocurrency is the most dominant with 68% of the market share; Out of the top-100 list by market capitalization, about two-thirds or 64 of them are non-mineable such as Ripple-XRP, Binance Coin, Tether, EOS, Stellar, UNUS SED LEO, Chainlink, Tezos, NEO, and IOTA.

[12] https://www.marketwatch.com/story/heres-how-much-it-costs-to-mine-a-single-bitcoin-in-your-country-2018-03-06

Risberg, 2018).[13] If internet is viewed as the first generation of the digital revolution, blockchain is considered to be the second generation, but both are disruptive. Regardless, Bitcoin offers some key advantages (Grech & Camilleri, 2017); anonymity[14] (identity/personal data is kept anonymous), self-sovereignty (users manage own data), transparency (distributed ledger), immutability (records are permanent, not falsified or edited), disintermediation (all transactions are executed without the need of a central authority), and collaboration (users transact with each other directly, i.e. purely peer-to-peer without a trusted third party). While Staples et al. (2017) investigated inherent risks as well as opportunities using blockchain, Vigna and Casey (2016) examined how the advent of blockchain has changed electronic cash and payment systems. Due to Facebook's already troubled past concerning privacy and exploitation of users' data (i.e. Cambridge Analytica), Facebook's Libra is surrounded by a great deal of uncertainty; furthermore, overly irritated central banks (the Fed and ECB in particular) as well as regulators and law makers have serious doubts that Libra can ensure privacy and security, plus called for greater scrutiny of Libra on terrorism-financing, money-laundering, global stability, illegal drugs and human trafficking (Bonneau et al., 2015; Gudgeon et al., 2019; Christin, 2013).

Blockchain, think of it as a physical chain where each link of the chain represents a block in blockchain, is a distributed ledger comprising a chronology of transactions timestamped by a timestamp server; in other words, a new block has a link to and uses input from the preceding block (Haber & Stornetta, 1991). New Bitcoin are minted via a mining process governed by core Bitcoin developers and nodes (Kroll et al., 2013; Garay et al., 2014); whereas, Libra will be minted by the Libra Association as the de facto central authority (LA, 2019). Bitcoin is an unstable cryptocurrency with no intrinsic value, its value mainly comes from belief, trust and speculation (Back et al., 2014; Barber et al., 2012); on the other hand, Libra is designed as a more stable cryptocurrency backed by its "Libra Reserve" that includes a basket of four low-volatile fiat currencies (i.e. dollar, euro, pound, and yen) plus low-risk central bank reserves (see Taskinsoy, 2019c, d, e; Reitman, 2019; Wong, 2019). Both Bitcoin and Libra run on a decentralized blockchain protocol with some technical variations; Bitcoin's permissionless blockchain is based on a Proof-of-Work[15] (PoW) algorithm (Becker et al., 2012; Bentov et al., 2014) as shown in Figure 1, where nodes run transactions in a purely peer-to-peer network that relies on consensus (Ben-Sasson et al., 2014); Libra's permissioned blockchain however is supported by a

[13] Although blockchain as an infrastructure technology is very secure, but the security or integrity of the system may be bridged or compromised by a group of hackers, designers or people who are in charge of running the network. A Japanese based Mt. Gox was hacked first, followed by DAO (Ethereum), Bitfinex, NiceHash, and Coincheck.

[14] Bitcoin takes anonymity very seriously, even Bitcoin's creator Satoshi Nakamoto is a pseudonym. No one knows for sure the true identity of Satoshi, whether it is a he, she, or a machine (i.e. artificial intelligence).

[15] Cryptocurrencies that are based on a mining process and proof-of-work are more difficult to be hacked than non-mineable coins based on proof-of-stake. Besides PoW and PoS, following variations have been proposed; proof-of-coin-age by Peppercoin (King & Nadal, 2012), proof-of-deposit by TenderMint (Kwon, 2014), proof-of-burn (Stewart, 2012), proof-of-activity (Bentov et al., 2014). Whether Facebook's Libra can achieve stability remains to be an open problem.

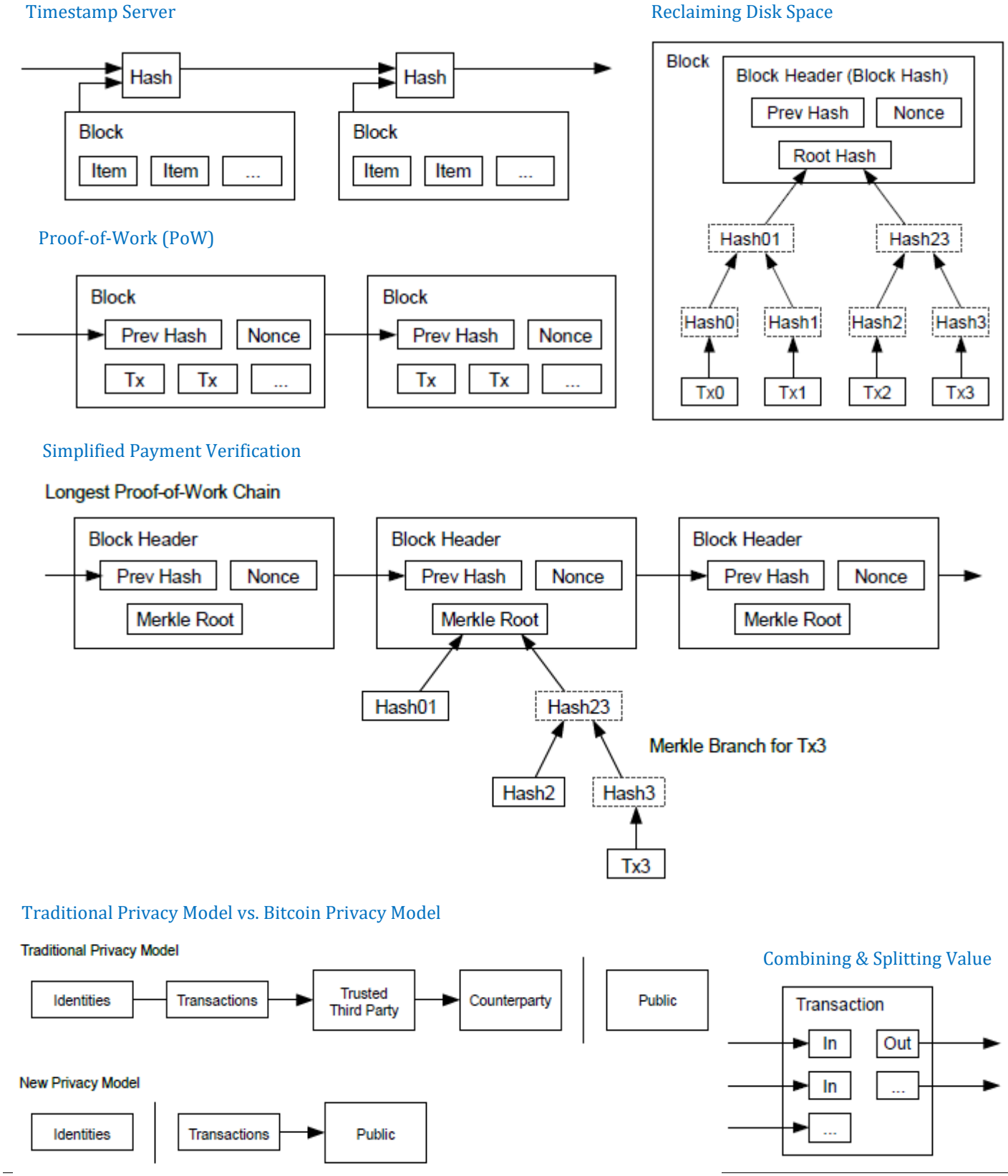
Proof-of-Stake (PoS) algorithm (e.g. Catalini et al., 2019; Josefsson & Liusvaara, 2017), where nodes rely on an improved consensus such as LibraBFT (Buchman et al., 2018; Yin et al., 2018). Distinctly different from Bitcoin, Libra uses a new programming language "Move" which is specifically written for Libra to implement smart contracts (Blackshear et al., 2019; Lamport et al., 1982; Lamport, 1998).

There are obvious differences between Libra and other cryptocurrencies in terms of cost, consistency, functionality, scalability, and security. In theory, adopting blockchain is easy and free, but in practice, nodes incur operational costs under mineable cryptocurrencies (Bouoiyour & Selmi, 2016); the cost of mining a single bitcoin is not confined to electricity expense, but also to rent, equipment, and CPU time (see Houy, 2014; Kroll et al., 2013; Kristoufek, 2015). Libra, similar to Ripple, will have a very small cost to users who transfer money or purchase goods online (Chiu & Wong, 2014; Chiu & Koeppl, 2017; Dwyer, 2014; Hayes, 2017). Consistency varies significantly among cryptocurrencies, which tends to be low for mineable coins and strong for non-mineable coins such as Libra which is forecast to take only few seconds to confirm and execute as many as 1000 transaction (Kim, 2017; Sovbetov, 2018). Bitcoin is the first successful decentralized cryptocurrency (Nakamoto, 2008), during the past decade, more than 2,440 altcoins have sprouted through which, many decentralized applications (i.e. dApps) along with new programming languages enabling smart contracts have emerged (Move in Libra, Solidity in Ethereum, and Plutus in Cardano); for more, see Blackshear et al (2019), Buterin (2013), Vukoli´c (2015), Biryukov & Pustogarov (2015), Eyal (2015), Garay et al (2014),

While scalability is Libra's biggest strength, it is Bitcoin's biggest weakness. Libra's blockchain based on PoS can process many transactions thanks to its user base of close to three billion account holders worldwide. Libra's high scalability along with its fast processing time (i.e. performance), according to Vukoli´c (2015), are inseparable (Figure 2). Under Bitcoin's blockchain using PoW and consensus[16] (Dwork & Naor, 1992; Nakamoto, 2008), a far smaller number of transactions per second (about 8) is processed (Cascarilla, 2015), which makes Bitcoin a cryptocurrency of low scalability and speed when compared with peers such as Ethereum (15), Ripple (1,500), and Libra (estimated 1,000).[17] Even Visa on a regular day, processes 25,000 (for challenges on cryptocurrencies, see Bonneau et al (2015)). In the PoW hashing scheme, Bitcoin's version is derived from Adam Back's Hashcash (Back, 2002) based on SHA-256 hash function where transactions are hashed in a Merkle tree (see Merkle, 1980, 1987; Eastlake & Hansen, 2011). Cryptocurrencies based on PoW is more secure; mineable Bitcoin tolerates 50% (1/2) of malicious nodes, but Libra's PoS tolerates 33% (1/3), more secure than Bitcoin.

[16] Bitcoin's PoW is not vulnerable to Sybil (i.e. copies of nodes) attacks. Bitcoin's consensus algorithm includes the following steps: A new block is created by a node in about 10 minute intervals; transactions are broadcast to all nodes via distributed ledger; after transactions' validity is confirmed, nodes broadcast their blocks; as a final step, the acceptance of a new block is granted by a full consensus and by including its hash in the next block that is created.

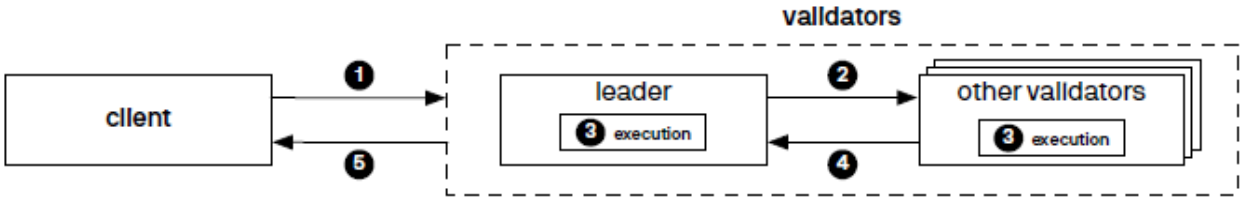
[17] https://blocksplain.com/2018/02/28/transaction-speeds/



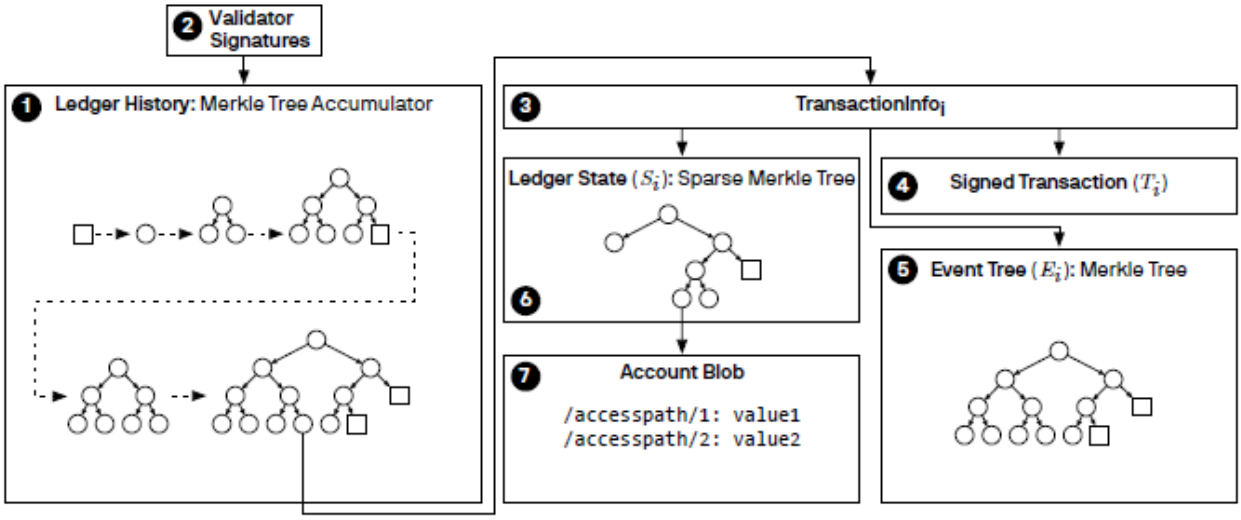
Source: Nakamoto (2008)

Figure 1: Overview of Bitcoin Blockchain Protocol

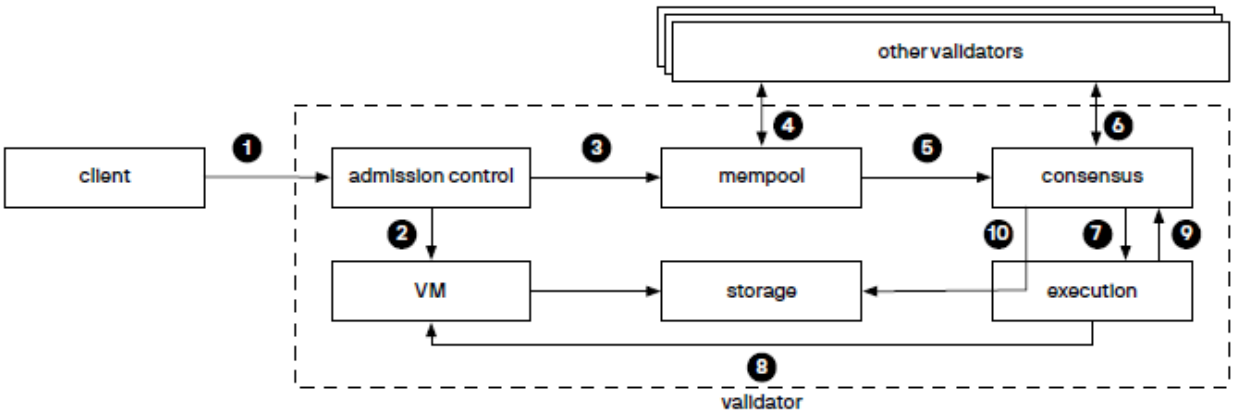
Libra Protocol



Authenticated Data Structures



Libra Networking



Source: The Libra Association

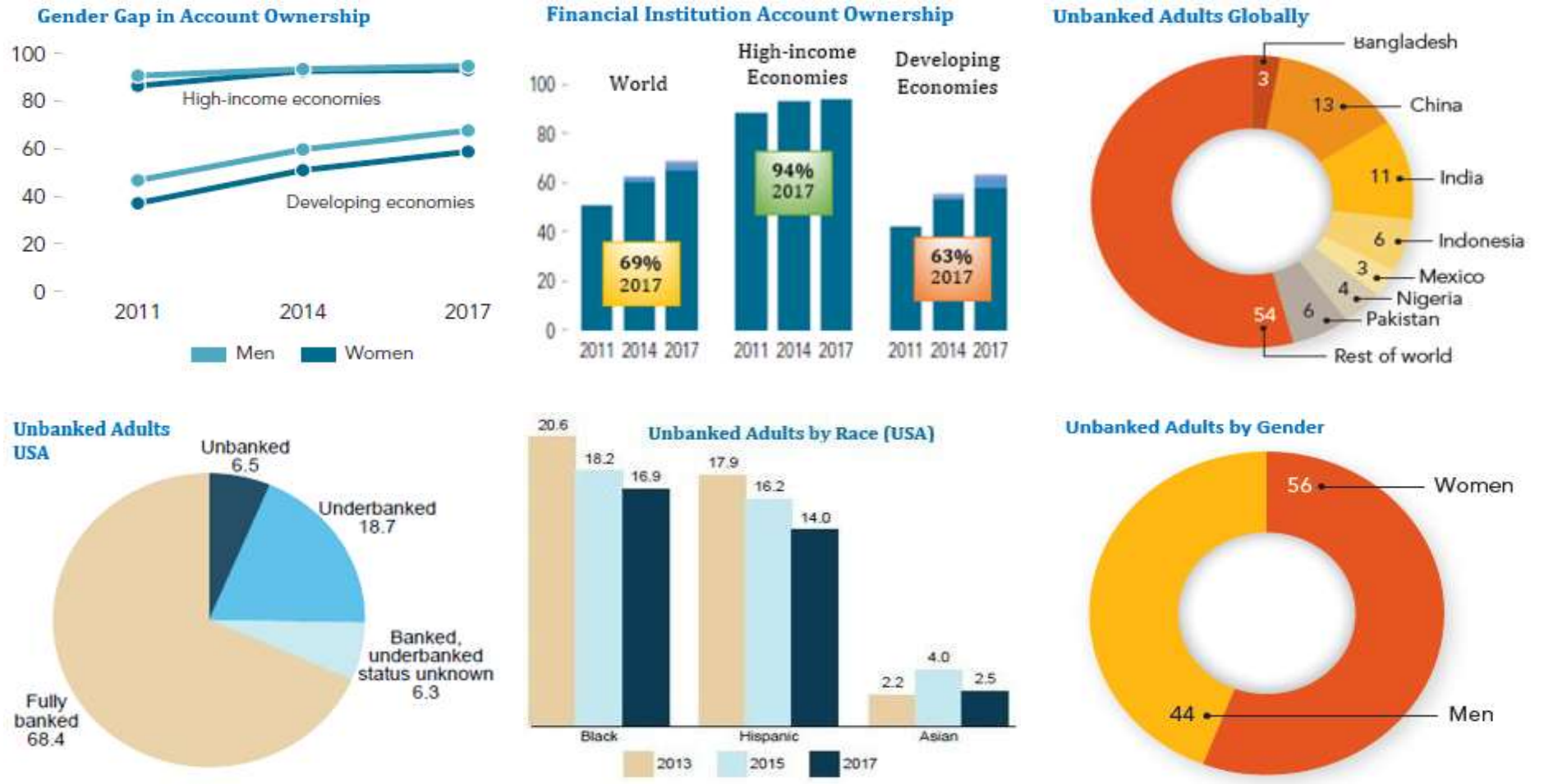
Figure 2: Overview of Libra Blockchain Protocol

Notes: Under Libra blockchain protocol, executing a transaction follows six specific steps; (1) the signature on the transaction is verified to match the sender's public key; (2) the sender gets authenticated (verified) and his/her LibraAccount is checked for sufficient Libra coins (funds); (3) running prologue ensures that the account has enough Libra coins, the Move bytecode verifies the transaction script and modules that no duplication, double spending, or violation of safety (i.e. type, reference, and resource); (4) modules are published under the sender's account (no module with the same name, meaning duplication is not permitted); (5) successfully completed transaction scripts are committed to the global state, but not the failed ones; and (6) Move virtual machine (VM) runs the epilogue to finalize the transaction.

Both Bitcoin and Libra blockchain are open source, meaning they are designed to allow developers to build on them without needing to get a permission (Nakamoto, 2008; LA, 2019). Like dollar, which is the unit of the dollar system, Bitcoin is divisible by eight decimals (by 100,000,000) and its smallest denomination is called a Satoshi equating 0.000000001 BTC. With the widespread use of internet, expanding coverage of wireless networks (data) and fast proliferation of smartphones, increasingly more people throughout the world are online for ecommerce and financial intermediation. Libra as a currency for everyday use, and in stark contrast to Bitcoin, one Libra will equal ∓ one dollar. Bitcoin has no intrinsic value, therefore its value mainly comes from belief, trust and speculation (Back et al., 2014; Barber et al., 2012); on the contrary, Libra is designed as a stable cryptocurrency backed by its "Libra Reserve" comprising a basket of four low-volatile fiat currencies (dollar, euro, pound, and yen) plus low-risk central bank reserves (Taskinsoy, 2019c, d, e; Reitman, 2019; Wong, 2019).

The new programming language "Move" and the use of LibraBFT consensus algorithm makes Libra more secure than Bitcoin and other altcoins (LA, 2019). Move takes care of the *double-spend* problem by making the properties of real assets and digital assets the same; moreover, Move's automatic proof (i.e. it checks changes in account balances of payers and receivers) feature facilitates 100 times more transactions to be executed than Bitcoin and Ethereum. Not only the easier transaction codes of Move make the implementation of Libra's governance policies more secure, they help Libra evolve further to facilitate smart contracts. Move and LibraBFT ensure safety of funds and financial data plus the integrity and anonymity of personal account information (i.e. Libra user identity is not linked to the real world identity). LibraBFT consensus protocol makes Libra 1/3 more secure than Bitcoin, 1/2 and 2/3 respectively, meaning that Libra can function correctly even if 1/3 of its network fails or hacked. Bitcoin's PoW leads to a lower transaction throughput, higher latency, and greater energy cost (Wood, 2016; Catalini et al., 2019; Buchman et al., 2018; Josefsson & Liusvaara, 2017; Yin et al., 2018).

One of Facebook's many goals with Libra is to revolutionize electronic payment systems and money transfers; Libra as a stable cryptocurrency is going to enhance financial inclusion and global stability as a public good (LA, 2019). Many agree that financial inclusion aids development and helps people escape destitution as access to and use of financial services enable people to invest in their careers, tertiary education, businesses, and health (Demirgüç-Kunt et al., 2017). Despite continued growth in account ownership since 2011 (Figure 3), 31% of adults (1.7 billion) globally did not have an account in 2017 (Demirgüç-Kunt et al., 2018). The National Survey of Unbanked Households (FDIC, 2018) shows that 6.5% of the U.S. households were unbanked as of 2017 (14.1 million adults and 6.4 million children), up from 7.6% in 2009. The FDIC report indicates that 52.7% of unbanked households in the U.S. cited "do not have enough money" as a reason for not openıng a bank account (FDIC, 2018).



Source: Demirgüç-Kunt et al (2018); FDIC (2018)

Figure 3: Financial Inclusion Worldwide and the U.S. (2017)

Notes: Account ownership worldwide grows but inequality between men and women or rich and poor continues to persist; as of 2017, the gender gap in account ownership worldwide was 7 percentage points, 72% men compared to 65% women (gender gap in developing countries was 9 percentage points). Financial inclusion throughout the world has improved since 2011, nevertheless 31% of adults did not have an account in 2017, up from 39% in 2014 and 49% in 2011. In other words, account ownership rose from 51% (2011) to 61% (2014) and then to 69% (2017), Out of the world's 1.7 billion unbanked adults, 46% of them (782 million) live in 7 countries; furthermore, 56% of the unbanked adults (950 million) are women and the remaining about 750 million (44%) are men. However in China, India and Turkey, women make up circa 60% of the unbanked adults. In 2017, 6.5% or 8.4 million households in the U.S. were unbanked, which amounts to 14.1 million adults and 6.4 million children (i.e. there were 129.3 million U.S. households in 2017). Also in 2017, the number of underbanked U.S. households was 18.7%, or 24.2 million households comprising 48.9 million adults and 15.4 million children. In the U.S., 68.4% of the households in 2017 were fully banked; and interestingly, 58.7% of the unbanked households in 2017 stated that they were not likely to open a bank account, not having enough money was given as the main reason.

3.0 Methodology

This article of Libra cryptocurrency is based on both the academic and online literature. We provide a high-level technical overview of Libra and blockchain technology. Our broad analysis of Libra cryptocurrency looks at various models and categories of implementation approaches. We discuss the components of blockchain technology and provide illustrative visuals when possible. We also compare consensus models used in Libra and Bitcoin blockchain networks. We touch on the use of blockchain technology in other applications such as smart contracts. The article discusses limitations and misconceptions surrounding Libra and its permissioned decentralized blockchain. Finally, this article presents some recommendations and directions for future research.

4.0 Concluding Remarks

Libra cryptocurrency is a new invention on grounds of both theory and practice; its unique aspects are distinctly different from Bitcoin and over two thousand altcoins (i.e. Ethereum and Ripple). Libra runs on blockchain protocol but without a chain of blocks; this is far different than Bitcoin blockchain where every new bitcoin is minted and enters circulation via a mining process which starts with a block, and then a ledger comprising timestamped transactions in a chronological order is distributed to all nodes (miners) in the Bitcoin network who check and validate transactions based on consensus before they are added to the end of each coin in its block. Libra is surrounded by massive uncertainty and confusion, although Facebook promotes Libra blockchain as a decentralized peer-to-peer system of electronic cash, this is a far cry from truth. Unlike Bitcoin's permissionless decentralized blockchain without a trusted party (i.e. purely peer-to-peer); Libra's permissioned decentralized blockchain will be governed by the Libra Association as a de facto central authority, which will initially comprise 28 private founding-members each of which will act as a validator to ensure Libra's stability.

As with any disruptive invention, Libra cryptocurrency along with its blockchain as an infrastructure technology present some risks; therefore, its further success or failure will depend on various factors and key developments on the regulatory front (the Fed and ECB in particular). Regardless of mounting pressure and lack of clarity, Libra – as a stable global cryptocurrency – promises to revolutionize the existing electronic payment systems and money transfers worldwide by enhancing financial inclusion and stability as a public good. Since pseudonym Satoshi Nakamoto created the genesis block (i.e. first block) on 3 January 2009 and introduced Bitcoin on 9 January 2009, a total of 2,446 cryptocurrencies have sprouted like wild mushrooms; as of 11 August 2019, the combined market capitalization was $298 billion, 68.3% of which is dominated by Bitcoin (i.e. market value of $204 billion). However, the current market cap is still well below the peak of $830 billion reached on December 17, 2017.

Facebook's formal announcement of its Libra coin had the "big bang" effect in the cryptocurrency market; equally, the industry will witness "big crunch" if Libra sputters out resulting from a failure of receiving all appropriate approvals from central banks, regulators, and law makers running headlong into backlash to Libra in order to punish Facebook which already has a troubled past of privacy abuse and exploitation of users' data. Libra is cost efficient and more consistent than other cryptocurrencies; Libra's superior functionally, higher security, and vast scale due to a user base of nearly 3 billion make Libra potentially qualify as an alternative reserve cryptocurrency to dollar. Libra will have little or no cost for transferring money digitally or purchasing goods online. While Bitcoin and other mineable altcoins have low consistency, Libra has high consistency and is forecast to execute 1,000 transactions per second as opposed to about 10 by Bitcoin. Libra's permissioned blockchain is based on Proof-of-Stake (PoS) algorithm, where nodes (validators) rely on LibraBFT consensus; moreover, Libra uses a new programming language "Move" specifically written for Libra to implement smart contracts.

The new programming language "Move" and the use of LibraBFT consensus algorithm makes Libra more secure than Bitcoin and other altcoins. Move takes care of the *double-spending* issue by making the properties of real assets and digital assets the same. Move's automatic proof facilitates 100 times more transactions than Bitcoin and Ethereum. Furthermore, easier transaction codes of Move make the implementation of Libra's governance policies more secure and help Libra evolve to enable smart contracts. Move along with LibraBFT ensure safety of funds and financial data plus the integrity and anonymity of personal account information; more importantly, LibraBFT consensus protocol makes Libra 1/3 more secure than Bitcoin, Libra can function correctly even if 1/3 of its network fails or hacked. Libra's PoS leads to higher transaction throughput, lower latency, and lower energy cost.

To launch Libra, Facebook's effort to satisfy concerns or demands from all sides is both irrational and implausible task to accomplish. Instead of halting its Libra project until all regulators are satisfied, Facebook should move ahead with its planned launch date of 2020, but for the time being, Facebook should ensure the relevant parties that Libra blockchain will protect consumers and satisfactorily address issues on terrorism financing, money laundering, and national security. A decade has passed since Bitcoin's debut in January 2009, still a growing number of states strongly oppose the notion of cryptocurrencies. As a result, countries have strengthened their regulatory framework against the perceived threat of cryptocurrencies. As of 2018, 24 nations issued a ban on digital coins (15 implicit and 9 absolute), 34 nations passed anti-money laundering and anti-terrorism financing laws (i.e. but some countries still have no regulation dealing with cryptocurrencies); additionally, 8 member-states of the Eastern Caribbean Currency Union are taking part in the Eastern Caribbean Central Bank pilot which will study and test the use of cryptocurrencies alongside national currencies.

References

Adrian, T. & Mancini-Griffoli, T. (2019). The Rise of Digital Money. Fintech Notes, Washington, D.C.: International Monetary Fund.

Albright, J. (2018). The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle Accessed on line at: https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-andcambridge-analytica-debacle-b69fe692d747.

Andolfatto, D. (2018). Assessing the Impact of Central Bank Digital Currency on Private Banks. Federal Reserve Bank of St. Louis Working Paper 2018–026C.

Back, A. (2002). Hashcash-A Denial of Service Counter-Measure. http://www.hashcash.org/papers/hashcash.pdf.

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Tim´on, J. & Wuille, P. (2014). Enabling Blockchain Innovations with Pegged Sidechains.

Barber, S., Boyen, X., Shi, E. & Uzun, E. (2012). Bitter to Better—How to Make Bitcoin a Better Currency. In Financial Cryptography.

Bayer, D., Haber, S. & Stornetta, W. S. (1993). Improving the Efficiency and Reliability of Digital Time-Stamping. In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

Bech, M. L. & Garatt. R. (2017). Central Bank Cryptocurrencies. BIS Quarterly Review.

Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H. & B¨ohme, R. (2012). Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency. In WEIS.

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E. & Virza. M. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. In IEEE Symposium on Security and Privacy.

Bernstein, P. A., Hadzilacos, V. & Goodman, N. (1987). Concurrency Control and Recovery In Database Systems." Addison-Wesley.

Bentov, I., Lee, C., Mizrahi, A. & Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. Cryptology ePrint Archive, Report 2014/452.

Biryukov, A. & Pustogarov, I. (2015). Bitcoin over Tor isn't a Good Idea. IEEE Symposium on Security and Privacy.

Blackshear, S., Cheng, E., Dill, D. L., Gao, V., Maurer, B., Nowacki, T., Pott, Qadeer, S., Rain, Russi, D., Sezer, S., Zakian, T. & Zhou, R. (2019). Move: A Language with Programmable Resources. https://developers.libra.org/docs/move-paper.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A. & Felten, E. W. (2015). Sok: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In Symposium on Security and Privacy. IEEE, 2015, pp. 104–121.

Bouoiyour, J. & Selmi, R. (2016). Bitcoin: A Beginning of a New Phase? Economics Bulletin, 36, 1430–40.

Buchman, E., Kwon, J. & Milosevic, Z. (2018). The Latest Gossip on BFT Consensus. CoRR, vol. abs/1807.04938.

Buterin, V. (2013). A Next-Generation Smart Contract and Decentralized Application Platform. White paper, http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Camenisch, J., Hohenberger, S. & Lysyanskaya, A. (2005). Compact ecash. In EUROCRYPT.

Cascarilla, C. G. (2015). Bitcoin, Blockchain, and the Future of Financial Transactions. In CFA Institute Conference Proceedings Quarterly (Vol. 32, No. 3, pp. 18-24). CFA Institute.

Castro, M. & Liskov, B. (1999). Practical Byzantine Fault Tolerance. In USENIX Symposium on Operating Systems Design and Implementation (OSDI), 1999, pp. 173–186.

Catalini, C., Kominers, S. D. & Jagadeesan, R. (2019). Market Design for a Blockchain-Based Financial System. Working paper no. 3396834. Social Science Research Network.

Chaum, D. (1982). Blind Signatures for Untraceable Payments. CRYPTO.

Chaum, D., Fiat, A. & Naor, M. (1998). Untraceable Electronic Cash. CRYPTO.

Chiu, J. & Wong, T-N. (2014). E-money: Efficiency, Stability and Optimal Policy. Bank of Canada, Working Paper, 2014–16, April.

Chiu, J. & Koeppl, T. (2017). The Economics of Cryptocurrencies—Bitcoin and Beyond. Queen's Economics Department Working Paper 1389.

Christin, N. (2013). Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. In WWW, 2013.

Clarke, A. C. (1962). Hazards of Prophecy: The Failure of Imagination. From Profiles of the Future: An Inquiry into the Limits of the Possible.

Cohen, J. E. (2013). What is Privacy for? Harvard Law Review 126.

Coombs, K. A. (2005). Protecting USER PRIVACY in the Age of DIGITAL LIBRARIES. Computers in Libraries 25(6), 16-20.

Dai, W. (1998). B-money. http://www.weidai.com/bmoney.txt.

Demirgüç-Kunt, A., Klapper, L. & Singer, D. (2017). Financial Inclusion and Inclusive Growth: A Review of Recent Empirical Evidence. Policy Research Working Paper 8040, World Bank Group, Washington, DC.

Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S. & Hess, J. (2018). The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. World Bank Group.

Duffie, D. (2019). Digital Currencies and Fast Payment Systems. Mimeo, Stanford University.

Dwork, C. & Naor, M. (1992). Pricing via Processing or Combatting Junk Mail. CRYPTO.

Dwyer, G. P. (2014). The Economics of Bitcoin and Similar Private Digital Currencies. Journal of Financial Stability, 333, pp. 1-11.

Eastlake, D. & Hansen, T. (2011). US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF). RFC 6234 (Informational), May, available at: http://www.ietf.org/rfc/rfc6234.txt.

Eyal, I. (2015). The Miner's Dilemma. IEEE Symposium on Security and Privacy.

FDIC (Federal Deposit Insurance Corporation) (2018). FDIC National Survey of Unbanked and Underbanked Households. Division of Depositor and Consumer Protection, October.

Ferguson, N., Schneier, B. & Kohno, T. (2012). Cryptography Engineering: Design Principles and Practical Applications. John Wiley & Sons.

Garay, J., Kiayias, A. & Leonardos, N. (2014). The Bitcoin Backbone Protocol: Analysis and Applications. Cryptology ePrint Archive, Report 2014/765.

Goldschlag, D. M. & Stubblebine. S. G. (1998). Publicly Verifiable Lotteries: Applications of Delaying Functions. Financial Cryptography.

Goodhart, C. (2000). Can Central Banking Survive the IT Revolution? International Finance 3 (2): 189–209.

Grech, A., & Camilleri, A.F. (2017). Blockchain in Education. JRC Science for Policy Report, European Commission, https://ec.europa.eu/jrc/en/open-education.

Gudgeon, L., Moreno-Sanchez, P., Ross, S., McCorry, P. & Gervais, A. (2019). Sok: Off the Chain Transactions. IACR Cryptology ePrint Archive, vol. 2019, p. 360.

Haber, S. & Stornetta, W. S. (1991). How to Time-Stamp a Digital Document. In Journal of Cryptology, Vol 3(2), pp. 99-111, 1991.

Haber, S. & Stornetta, W. S. (1997). Secure Names for Bit-Strings. In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April.

Hayes, A. S. (2017). Cryptocurrency Value Formation: An Empirical Study Leading to a Cost of Production Model for Valuing Bitcoin. Telematics and Informatics 34, pp. 1308-132.

Houy, N. (2014). The Economics of Bitcoin Transaction Fees. Working Paper GATE 2014-07, halshs-00951358.

Huang, D. Y., Dharmdasani, H., Meiklejohn, S., Dave, V., Grier, C., McCoy, D., Savage, S., Weaver, N., Snoeren, A. C. & Levchenko, K. (2014). Botcoin: Monetizing Stolen Cycles. NDSS.

Josefsson, S. & Liusvaara, I. (2017). Edwards-Curve Digital Signature Algorithm (EdDSA). RFC, vol. 8032, pp. 1–60.

Katz, J. & Lindell, Y. (2014). Introduction to Modern Cryptography, Second Edition. CRC Press.

Kim, T. (2017). On the Transaction Cost of Bitcoin. Finance Research Letters, Volume 23, November 2017, Pages 300-305.

King, M. (1999). Challenges for Monetary Policy: New and Old. Speech delivered at a symposium sponsored by the Federal Reserve Bank of Kansas City, Jackson Hole, WY, August 27.

King, S. & Nadal, S. (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, August.

Kocherlakota, N. R. (1998). Money Is Memory. Journal of Economic Theory 81(2): 232–51, August.

Kristoufek, L. (2015). What Are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis. PLOS ONE, 10(4).

Kroll, J. A., Davey, I. C. & Felten, E. W. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. Proceedings of WEIS, Volume.

Kwon, J. (2014). TenderMint: Consensus without Mining, August.

LA (The Libra Association) (2019). An Introduction to Libra. https://libra.org/en-us/whitepaper.

Lagarde, C. (2018). Winds of Change: The Case for New Digital Currency. Prepared for delivery by IMF Managing Director, Singapore Fintech Festival, November 14.

Lamport, L. (1998). The Part-Time Parliament. ACM Transactions on Computer Systems, vol. 16, no. 2, January, pp. 133–169., https://dl.acm.org/citation.cfm?doid=279227.279229.

Lamport, L., Shostak, R. & Pease, M. (1982). The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401.

Laurie, B. & Clayton, R. (2004). Proof-of-work proves not to work. WEIS.

Law, L., Sabett, S. & Solinas, J. (1996). How to Make a Mint: The Cryptography of Anonymous Electronic Cash. American University Law Review, vol. 46, no. 4, pp. 1131-1162.

Levy, S. (2001). Crypto: How the Code Rebels Beat the Government--Saving Privacy in the Digital Age. Penguin.

Mancini-Griffoli, T., Peria, M. S. M., Agur, I., Ari, A., Kiff, J., Popescu, A. & Rochon. C. (2018). Casting Light on Central Bank Digital Currency", IMF Staff Discussion Note SDN/18/08, November.

Martin, L. L. (1990). Coercive Cooperation: Explaining Multilateral Economic Sanctions. Princeton, NJ: Princeton University Press.

Massias, H., Avila, X. S. & Quisquater, J-J. (1999). Design of a Secure Timestamping Service with Minimal Trust Requirements. In 20th Symposium on Information Theory in the Benelux, May 1999.

McLeay, M., Radia, A. & Thomas. R. (2014). Money Creation in the Modern Economy. Bank of England Quarterly Bulletin 2014, Q1, pp. 14–27.

Merkle, R. C. (1980). Protocols for Public Key Cryptosystems. In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April.

Merkle, R. C. (1987). A Digital Signature Based on a Conventional Encryption Function. In Advances in Cryptology - CRYPTO '87, A Conference on the Theory and Applications of Cryptographic Techniques, Santa Barbara, California, USA, August 16-20, 1987, Proceedings, pp. 369–378.

Moore, T. & Christin, N. (2013). Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. In Financial Cryptography.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Unpublished paper, available at https://bitcoin.org/bitcoin.pdf.

Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies. Princeton University Press: Princeton, NJ, USA.

Okamoto, T. & Ohta, K. (1992). Universal Electronic Cash. CRYPTO.

Pape, R. A. (1997). Why Economic Sanctions Do Not Work. International Security 22, pp. 90–136.

Pfitzmann, A. & Köhntopp, M. (2001). Anonymity, Unobservability, and Pseudonymity—A Proposal for Terminology. In Designing privacy enhancing technologies, pp. 1–9.

Phillips, R.C, & Gorse, D. (2017). Predicting Cryptocurrency Price Bubbles Using Social Media Data and Epidemic Modelling. IEEE Symposium Series on Computational Intelligence.

Reed, D. P. (1978). Naming and Synchronization in a Decentralized Computer System. Ph.D. Dissertation, Massachusetts Institute of Technology, Cambridge, MA, USA.

Reitman, R. (2019). Could Regulatory Backlash Entrench Facebook's New Cryptocurrency Libra? Electronic Frontier Foundation (EFF) (July 10), https://www.eff.org/deeplinks/2019/07/could-regulatory-backlash-entrench-facebooks-new-cryptocurrency-libra.

Risberg, J. (2018). Yes, the Blockchain Can Be Hacked. (Accessed on 20 August 2019). https://coincentral.com/blockchainhacks/

Rivest. R. L. (2004). Peppercoin Micropayments. Financial Cryptography.

Rivest, R. L. & Shamir, A. (1997). PayWord and MicroMint: Two Simple Micropayment Schemes. Security Protocols Workshop.

Rogers, E. S. (1996). Using Economic Sanctions to Control Regional Conflicts. Security Studies 4, pp. 43–72.

Sander, T. & Ta-Shma, A. (1999). Auditable, Anonymous Electronic Cash. CRYPTO.

Schoenmakers, B. (1998). Security Aspects of the EcashTM Payment System. State of the Art in Applied Cryptography.

Sirbu, M. & Tygar, J. D. (1995). NetBill: An Internet Commerce System Optimized for Network Delivered Services. IEEE Personal Communications, 2(4):34–39.

Sovbetov, Y. (2018). Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, LiteCoin, and Monero. Journal of Economics and Financial Analysis, Vol. 2 (2), pp. 1-27, Tripal Publishing House.

Staples, M., Chen, S. Falamanski, S., Ponomarev, A., Rimba, P., Tran, A.P., Weber, I., Xu, X. & Zhu, J. (2017). Risks and Opportunities for Systems using Blockchain and Smart Contracts. Canberra. Commonwealth Scientific and Industrial Research Organization.

Stewart, I. (2012). Proof of Burn. Bitcoin it, December.

Szabo, N. (2005). Bit Gold. Available at: http://unenumerated.blogspot.rs/2005/12/bit-gold.html

Taskinsoy, J. (2012). Relevancy of Corporate Financial Policies and the Profit Maximization View of Islamic Banks. Journal of Social and Development Sciences, Vol. 3(6), pp. 184-193, June, ISSN 2221-1152.

Taskinsoy, J. (2013a). Rigorous Capital Requirements under Basel III: Possible impact on Turkey's financial sector. Journal of WEI Business and Economics, Vol. 2(1), pp. 1-30, April.

Taskinsoy, J. (2013b). Basel III: Road to Resilient Banking, Impact on Turkey's Financial Sector. LAP LAMBERT Academic Publishing, 237 pages, ISBN 13: 978-3-659-30696-9.

Taskinsoy, J. (2018a). Bitcoin Mania: An End to the US Dollar's Hegemony or another Cryptocurrency Experiment Destined to Fail? (December 1, 2018). Available at SSRN: https://ssrn.com/abstract=3311989 or http://dx.doi.org/10.2139/ssrn.3311989.

Taskinsoy, J. (2018b). Effects of Basel III Higher Capital and Liquidity Requirements on Banking Sectors across the Main South East Asian Nations. International Journal of Scientific & Engineering Research (IJSER), Vol. 9(4), pp. 214-37, April, ISSN 2229-5518.

Taskinsoy, J. (2018c). The Cost Impact of Basel III across ASEAN-5: Macro Stress Testing of Malaysia's Banking Sector. LAP LAMBERT Academic Publishing, 369 pages, ISBN-13 978-613-9-90012-1.

Taskinsoy, J. (2018d). A Macro Stress Testing Framework for Assessing Financial Stability: Evidence from Malaysia. Journal of Accounting, Finance and Auditing Studies (JAFAS), Vol. 4(3), July, ISSN 2149-0996.

Taskinsoy, J. (2019a). The Transition from Barter Trade to Impediments of the Dollar System: One Nation, One Currency, One Monopoly (March 6, 2019). Available at SSRN: https://ssrn.com/abstract=3348119 or http://dx.doi.org/10.2139/ssrn.3348119

Taskinsoy, J. (2019b). Pure Gold for Economic Freedom: A Supranational Medium of Exchange to End American Monetary Hegemony as the World's Main Reserve Currency (April 25, 2019). Available at SSRN: https://ssrn.com/abstract=3377904 or http://dx.doi.org/10.2139/ssrn.3377904.

Taskinsoy, J. (2019c). Facebook's Project Libra: Will Libra Sputter Out or Spur Central Banks to Introduce Their Own Unique Cryptocurrency Projects? (July 20, 2019). Available at SSRN: https://ssrn.com/abstract=3423453 or http://dx.doi.org/10.2139/ssrn.3423453

Taskinsoy, J. (2019d). This Time Is Different: Facebook's Libra Can Improve Both Financial Inclusion and Global Financial Stability as a Viable Alternative Currency to the U.S. Dollar (August 8, 2019). Available at SSRN: https://ssrn.com/abstract=3434493.

Taskinsoy, J. (2019e). Is Facebook's Libra Project Already a Miscarriage? (August 15, 2019). Available at SSRN: https://ssrn.com/abstract=3437857.

Taskinsoy, J. (2019f). Stress Testing Made Easy: No More US Banks Stumbling and Facing Public Embarrassment Due to the Federal Reserve's Qualitative Objection (March 17, 2019). Available at SSRN: https://ssrn.com/abstract=3354018 or http://dx.doi.org/10.2139/ssrn.3354018.

Taskinsoy, J. (2019g). Typology of Stress Testing: Microprudential vs. Macroprudential Stress Testing of Risk Exposures (March 28, 2019). Available at SSRN: https://ssrn.com/abstract=3361528 or http://dx.doi.org/10.2139/ssrn.3361528.

Taskinsoy, J. (2019h). Higher Capital and Liquidity Regulations of Basel Standards Have Made Banks and Banking Systems Become More Prone to Financial and Economic Crises (June 9, 2019). Available at SSRN: https://ssrn.com/abstract=3401378 or http://dx.doi.org/10.2139/ssrn.3401378.

Taskinsoy, J. (2019i). Ever More Financial Instability notwithstanding the Basel Standards and the IMF's Financial Sector Assessment Program (February 4, 2019). Available at SSRN: https://ssrn.com/abstract=3328473 or http://dx.doi.org/10.2139/ssrn.3328473.

Taskinsoy, J. (2019j). Asian Miracle, Asian Tiger, or Asian Myth? Financial Sector and Risk Assessment through FSAP Experience: Enhancing Bank Supervision in Thailand (May 9, 2019). Available at SSRN: https://ssrn.com/abstract=3385337 or http://dx.doi.org/10.2139/ssrn.3385337.

Taskinsoy, J. (2019k). A Delicate Moment in Turkey's Economic Transition: Can Turkey Survive Mounting Economic Problems without the IMF's Bailout Package? (June 22, 2019). Available at SSRN: https://ssrn.com/abstract=3408520 or http://dx.doi.org/10.2139/ssrn.3408520.

Taskinsoy, J. (2019l). Turkish Lira – A Fiat Currency that Resembles the Volatility of Cryptocurrencies: The Effects of Exchange Rate Volatility on Turkish Economy (February 15, 2019). Available at SSRN: https://ssrn.com/abstract=3335545 or http://dx.doi.org/10.2139/ssrn.3335545.

Taskinsoy, J. (2019m). We Need No Dime from the IMF: Is This a Temporary Illusion or Can the Turkish Economy Recover from the Current Recession without the IMF Loans? (July 9, 2019). Available at SSRN: https://ssrn.com/abstract=3417431 or http://dx.doi.org/10.2139/ssrn.3417431.

Taskinsoy, J. (2019n). A Hiccup in Turkey's Prolonged Credit Fueled Economic Transition: A Comparative Analysis of Before and After the August Rout (August 2, 2019). Available at SSRN: https://ssrn.com/abstract=3431079 or http://dx.doi.org/10.2139/ssrn.3431079.

Vigna, J. & Casey, M. J. (2016). The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order. Picador.

Vukoli´c, M. (2015). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. International Workshop on Open Problems in Network Security. Springer, 112–125.

Vishnumurthy, V., Chandrakumar, S. & Sirer. E. G. (2003). Karma: A Secure Economic Framework for Peer-to-Peer Resource Sharing. Workshop on Economics of Peer-to-Peer Systems.

Wong, Q. (2019). US Lawmaker Wants Facebook to Halt its Libra Cryptocurrency Project. CNET (2019-06-18); https://www.cnet.com/news/us-lawmaker-wants-facebook-to-halt-its-libra-cryptocurrency-project/ (accessed on 19 August 2019).

Wood, G. (2016). Ethereum: A Secure Decentralized Generalized Transaction Ledger. http://gavwood.com/paper.pdf.

Woodford, M. (2000). Monetary Policy in a World without Money. International Finance 3 (2): 229–60.

Yeoh, P. (2017). Regulatory Issues in Blockchain Technology. Journal of Financial Regulation and Compliance 25(2):196-208, May.

Yin, M., Malkhi, D., Reiter, M. K., Golan, G. G. & Abraham, I. (2018). Hotstuff: BFT Consensus in the Lens of Blockchain. arXiv preprint arXiv:1803.05069.

Yli-Huumo, J., Ko, D., Choi, S., Park, S. & Smolander, K. (2016). Where is Current Research on Blockchain Technology? A Systematic Review. PloS one 11, 10, e0163477.