Mobile Payment Using Blockchain Security

Murad Obaid[1*], Musbah Aqel[1], and Mahmoud Obaid[2]

[1] Department of Management Information Systems Cyprus International University, Lefkosa, Northern Cyprus, Mersin 10, Turkey
[2] Department of Computer System Engineering, Arab American University, Jenin - Palestine
[*] Corresponding author. E-mail: murad.s.obaid@gmail.com

Received: Feb. 16, 2021; Accepted: Mar. 22, 2021

Blockchain has become one of the most common methods for securing transfer data through decentralized peer-to-peer systems and has received extensive attention in recent years. Blockchain is an immutable ledger that allows the execution of a transaction in a secure and decentralized manner. This sophisticated but secure mechanism has an excellent reputation and has increased its customer base. Despite substantial attention, the blockchain system has many challenges that must be ad-dressed. This paper proposes a solution that provides a standard framework for mobile payments using blockchain technology. We further discuss security-related issues and attempt to determine the potential pitfalls with which such mechanisms can be exploited. We also investigate how popular currencies such as Bitcoin utilize security arrangements for safe transactions via mobile devices.

Keywords: Blockchain, Mobile Payment, Private Blockchain, Banking Blockchain, Blockchain Security

http://dx.doi.org/10.6180/jase.202108_24(4).0025

1. Introduction

Blockchain technology, as a cryptographic-based distributed ledger, provides trusted transactions through third parties in the network [1, 2]. Bitcoin blockchain was introduced in 2008 [3], and many blockchain systems, such as Ethereum [4, 5], have public and private accessibility. Blockchain popularity has increased globally and has had a substantial impact on the world [6]. It has been commercially dependent [7], impacted world currencies [8], and affected the proliferation of financially focused cyberattacks [9], such as ransom ware [10] and denial of services (DoS) [11].

The main feature of blockchain technology is its attractive flexibility for many business fields, such as banking [12], logistics [13], smart contracts [14, 15], the medicine industry [16] and cyber security [17, 18].Every member gets an updated copy of the encrypted ledger, which enables them to validate any new transaction. Primarily, blockchain technology is a distributed database of records or public ledgers of all transactions, digital events, and operations shared among stakeholders. This highly secured system contains a specific, correct record of all previous transactions [2]. The two terms "Blockchain" and "Distributed ledger technology" are actually interchangeable [19].

Blockchain is a revolutionizing technology. First implemented in digital cryptocurrency, blockchain is an important part of its functionality [3].

In previous years, we could exchange information to make monetary transfers using the internet. All of these transactions were performed by a trusted intermediary. These third parties were responsible for making transactions in a secure environment. Currently, the blockchain eliminates any central authority or 3rd party between a financial institution and a data exchange by using all features and characteristics of the blockchain: a decentralized, digital ledger, cryptographically secured, non-reputable, time-stamped, irrevocable, auditable, distributed, transparent and verifiable. Suppose we have N users in a network; they share data and make a transaction. They use a protocol known as a consensus algorithm instead of using an intermediary. This protocol creates interplay trust and allows peer-to-peer transactions. To facilitate this, the blocks build a blockchain system using network users and a protocol such as proof of work, hashed and with digital signatures[20]. Each block has a set of transactions signed by the owner digitally and verified by the reset users before being added to the block [20], as shown in Fig. 1.

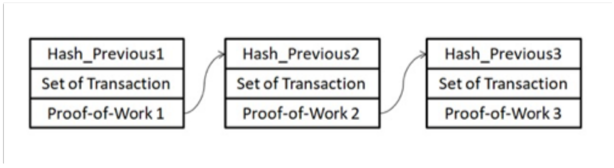

Fig. 1. Structures of Blockchain.

2. Trends and Related Research

The author in [17] explains the challenges with the use of security in centralized applications and gives us a comprehensive study of blockchain methods for a security services application in different areas of authentication, confidentiality, access control, and integrity assurance in the distributed network.

There are a large number of research areas that can apply a blockchain to avoid centralized entities, such as the cloud [21], Internet of Things (IoT), and Bigdata [22]. [23] Researchers believe that blockchains have characteristics that will be used within banking, but there is still a shortage of suitable uses of blockchains within modern society.

The blockchain could eliminate third parties, decrease costs, and increase profits for the banking industry [24].

Privet blockchain enables transactions that are faster and more secure. This technology will reshape the banking process and reduce costs.

The author in [25] explains that blockchain technology is trusted due to its trans-parency and its feature of making information publicly available while also confirming its integrity.

This paper [26] outlines some of the problems that are changing financial services due to rapid technological advances.

According to [24], the blockchain has assumed the most important role in the financial inclusion process.

In [27], the author explores how and why blockchain has become the puppet of the financial technology sector.

3. Proposed Solution Framework

This section explicitly details the proposed system in more details.

3.1. Overview

As payments are a great source of revenue for financial institutions, they expand the use of digital currencies (cryptocurrency) to satisfy the needs for all the new generation of internet users and online commerce. Financial institutions need to reap their benefits in the future and learn from these new technologies since cryptocurrencies have earned a remarkable reputation in the eyes of various control boards and governing bodies. Fig. 2, shown below, describes how the proposed solution works.

Customer A, who belongs to bank A (no geographic limits), wants to send money to customer B, who belongs to bank B. Customer A uses his or her mobile application to initiate the transaction, which includes defining the receiver mobile number and the amount of fiat currency and the currency type. Any node that receives the request first (called the issuer) checks for customer eligibility (blacklist, ML, fraud) creates the block and broadcasts the details to every node in the network. The issuer node sends three-digit codes to the sender's mobile phone for security verification. The sender enters his or her bank PIN code concatenated with the three digits that were received from the issuer. The acquirer bank checks for PIN validation by connecting to its own Hardware Security Model (HSM) system response and sends the validation message to all nodes.

The acquirer bank performs the exchange of fiat money (transaction amount plus commission) with the digital money (Ethereum or other digital currency) at the current rate, and the blockchain transfers the money to the receiver bank (beneficiary) after changing the digital money to fiat money in the beneficiary's currency. The blockchain divides the commission based on the commission policies and transfers the money to parties' accounts. All the nodes will validate the transaction, and the block will be closed and added to the blockchain transactions.

Messages sent to both sender and receiver mobile phones report transaction success; whenever any fail occurs in the middle of the process, everything is rolled back, and a message will be sent to the receiver about the failed transaction.

Our schema tries to eliminate most of the security vulnerabilities by using different security arrangements under the standard and implied security laws.

The sending customer must know his or her PIN code that is initiated by this customer's bank HSM on a high-level security model. This PIN code is requested only by the customer bank ecosystem, the customer must have a mobile phone and mobile SIM card. Multiple separated parts for authentication and process flow exist as follows.

The process is initiated by any node on the chain. The transaction is created in all parts (blockchain nodes). The PIN code is requested by the customer's owner bank using an additional PIN SMS backend, which means that the message will be sent to the sender who must have a mo-

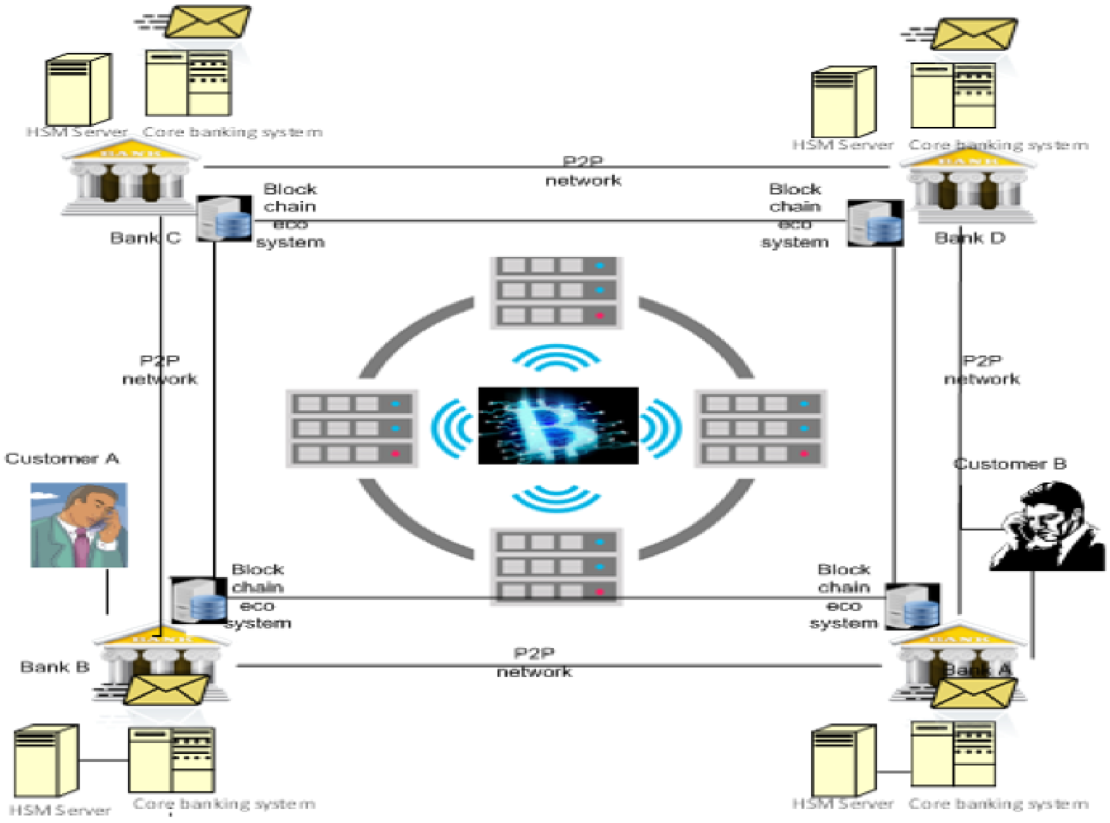

Fig. 2. New mobile payment using blockchain framework.

bile phone with a SIM card and additional PIN code. The PIN code authentication is done by the sender bank HSM, which is encrypted in a highly secure model. The customer eligibility is done by any node in the internal ecosystem, all transaction information flow will be encrypted, the customer banking system does final authentication, and none of the other parties will be involved in this part.

All parties are connected by a private network with secure VPN. To hack the system, the hacker would need to communicate with at least 3 parties, the sender bank, the receiver bank and the operator at the same time, and also have the system behavior, transaction workflow, encryption keys, sender mobile phone and the PIN code, which is certainly very difficult if not impossible: The encryption will be done using LMK that will include a mobile IME as well as the mobile account number.

3.2. Process Security

The blockchain will work on the Ethereum blockchain as a private network for our banking solution; this is one of the most robust, secured blockchains. The application on the mobile phone will encrypt the transaction text using the AES-256 algorithm using the LMK. Protection of passwords is essential because of their existence as a primary means for authentication. Our algorithm has the potential to detect and block such attempts; therefore, there is no chance of obtaining the original password in the case when hashing is deployed to accomplish such a task. Additionally, the hackers need the following components merely to initiate the transaction: the mobile phone device; the SIM card with the same number; the PIN code, which is in the customer's mind and on the hashing server; the authenticate application installed on the mobile phone; and the application password. Since all of this information is divided and physically stored in many locations, it is very difficult if not impossible to acquire them all.

Each node on the blockchain can get the transaction initiated by the customer, check for eligibility and create the block for this transaction. Each node (bank) has to validate each transaction to be an authorized transaction. The final authorization for security reasons and transaction legality must be taken from the customer account acquirer. The sender bank debits the customer account by the amount of the transaction plus commission by fiat currency (equal to the digital currency exchange), and the fiat currency is exchanged to digital currency (via blockchain

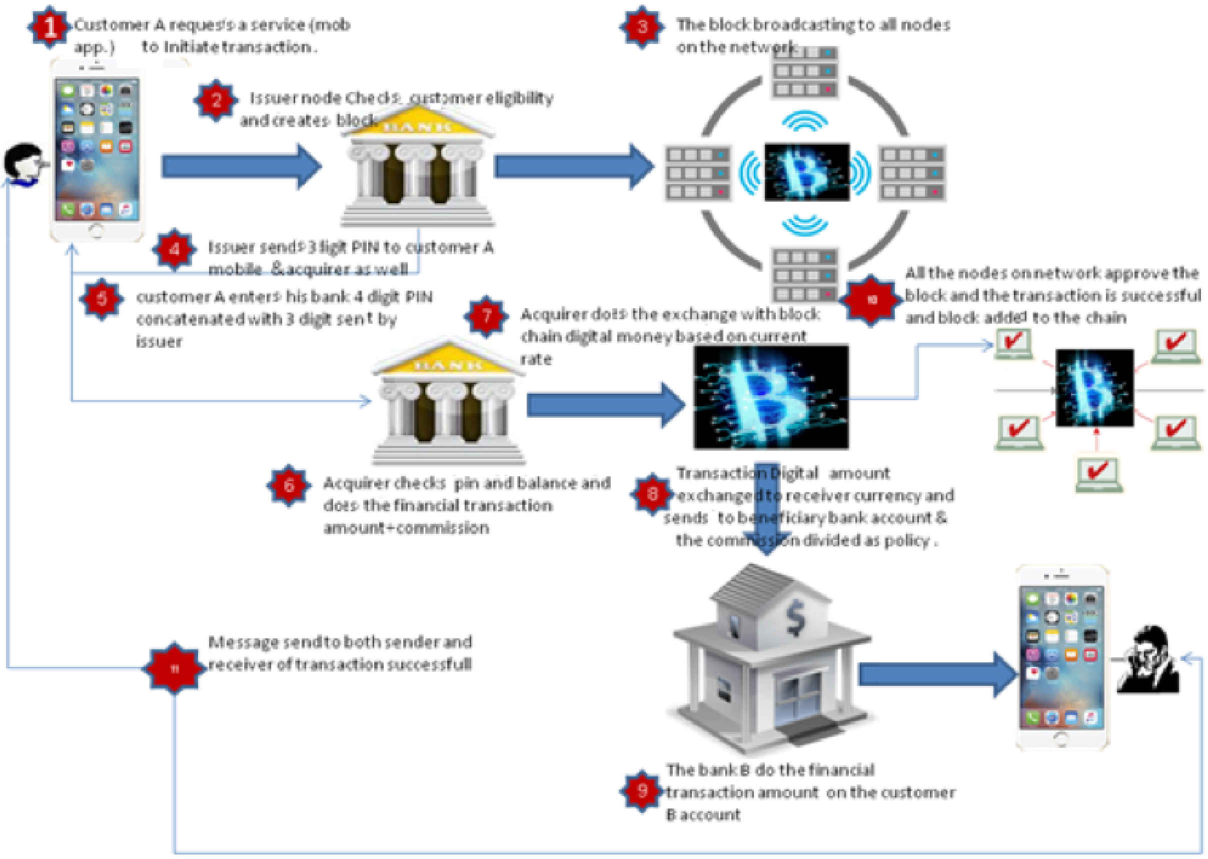
1 Customer A requests a service (mob app.) to Initiate transaction.
2 Issuer node Checks customer eligibility and creates block
BANK
3 The block broadcasting to all nodes on the network
4 Issuer sends 3 digit PIN to customer A mobile & acquirer as well
5 customer A enters his bank 4 digit PIN concatenated with 3 digit sent by issuer
BANK
7 Acquirer dots the exchange with block chain digital money based on current rate
10 All the nodes on network approve the block and the transaction is successful and block added to the chain
6 Acquirer checks pin and balance and does the financial transaction amount+commission
8 Transaction Digital amount exchanged to receiver currency and sends to beneficiary bank account & the commission divided as policy .
11 Message send to both sender and receiver of transaction successfull
9 The bank B do the financial transaction amount on the customer B account

Fig. 3. The Functionality of the Proposed Solution.

) and transferred to the receiver bank. The blockchain deducts the commission and exchanges the digital money for the receiver's fiat currency and transfers the money to the receiver bank account. All the nodes authorize the transaction, the block is closed, and the commission will be distributed based on the related policy, with every beneficiary receiving the prescribed rate.

4. Discussion

The secondary research method is deployed in this research to obtain the relevant information. Information is collected from various trusted resources, research papers, and studies to identify the significant points. Then, the collected information is analyzed to improve the overall effectiveness of the research.

Governing bodies of various countries emphasize improving the security of the present banking and financial systems and putting much effort into making all such activities transparent. The emergence of the cashless economy is enhancing the insecurity of online transactions. In this context, the performance of the blockchain is quite extraordinary. Furthermore, another concern regarding the blockchain security is that it considers pseudo-secrecy. As a result, Bitcoin clients do not need to provide their personal information for any kind of transaction. The blockchain domain has numerous security protocols that are utilized to authenticate transactions. However, when the role of authorities is considered in such transactions, they must rely on the legal process. However, these blockchain smartphones allow users to manage their passwords and other sensitive information. Along with that, the upgraded version of blockchain wallets also has the same potential in terms of providing security to the data because of the high-end encryption system. A considerable number of people do not use cryptocurrency often enough, which can make them concerned about such security issues; thus, they do not buy specific equipment to secure their digital transactions. To further improve security-related situations, decentralized applications are considered a potential solution. The dynamic mechanisms of such applications allow the user to keep all the related data information private. This does not mean that users cannot access the data, but it simply means that the mechanism saves all the information from unauthorized attempts.

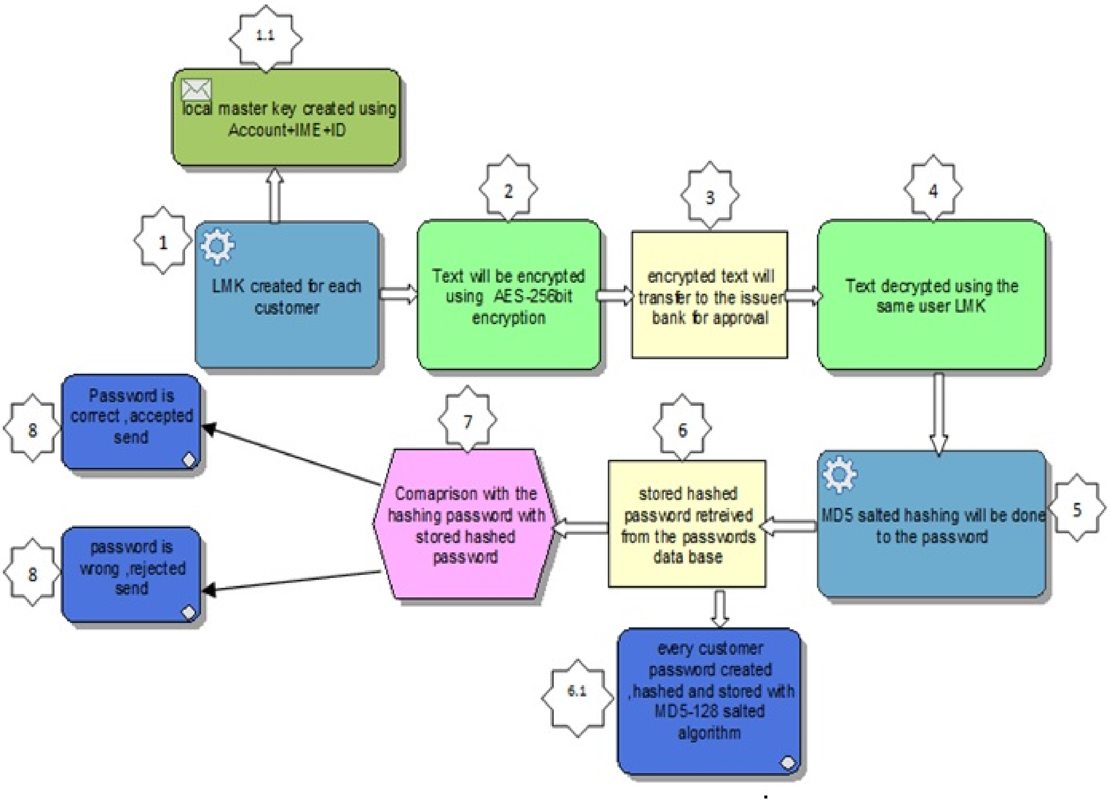
1.1
local master key created using Account+IME+ID
1
LMK created for each customer
2
Text will be encrypted using AES-256bit encryption
3
encrypted text will transfer to the issuer bank for approval
4
Text decrypted using the same user LMK
5
MD5 salted hashing will be done to the password
6
stored hashed password retreived from the passwords data base
6.1
every customer password created ,hashed and stored with MD5-128 salted algorithm
7
Comaprison with the hashing password with stored hashed password
8
Password is correct ,accepted send
8
password is wrong ,rejected send

Fig. 4. Security Aspects in the Proposed Solution.

The most notable thing about the blockchain, which can make the governments adopt this highly advanced payment system, is that all exchanges within a network are recog-nizable. The main reason for such agreements is to avoid the cases in which users attempt to avoid taxes illegally because of the privacy blockchain provides to them.

This literature gap is also considered a limitation of the current research paper. Moreover, the key findings of this research paper are as follows:

1. Inadequacy of safe and reliable software and hardware to secure the blockchain payments via mobile phones.
2. Limited scope for the technology to earn the trust of governments to categorize a blockchain as standard currency.

5. Conclusion

From the above information, it can be concluded that although blockchain has attained a remarkable level of popularity, government authorities and ordinary people still do not consider it a safe means of transactions. Apart from these issues, the lack of secure and reliable hardware and software also serves as an obstacle. For this study, we observed that there is a lack of literature in the domain of the blockchain, especially when the role of mobile phones is considered. Though this emerging next-generation technology has managed to receive massive attention, a significant literature gap can be seen. In this paper, the present market scenario of digital currencies is analyzed by keeping the main focus on the security of transactions using digital currencies. To explain it more carefully, we deployed a secondary research method and therefore analyzed existing information in the same domain.

References

[1] Tomaso Aste, Paolo Tasca, and Tiziana Di Matteo. Blockchain technologies: The foreseeable impact on society and industry. *computer*, 50(9):18–28, 2017.

[2] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. IEEE, 2017.

[3] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot, 2019.

[4] G Wood. Ethereum: a secure decentralised generalised transaction ledger [jelektronnyj resurs]. 32 c. *gavwood.*

com: official site URL: https://gavwood. com/paper. pdf data obrashhenija, 3, 2019.

[5] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 3(37), 2014.

[6] Morgen E Peck. Blockchains: How they work and why they'll change the world. *IEEE spectrum*, 54(10):26–35, 2017.

[7] Jørgen Svennevik Notland. Cryptocurrency as money.

[8] Shi Chen, Cathy Yi-Hsuan Chen, Wolfgang Karl Härdle, Teik Ming Lee, and Bobby Ong. Econometric analysis of a cryptocurrency index for portfolio investment. In *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1*, pages 175–206. Elsevier, 2018.

[9] Kim-Kwang Raymond Choo. Cryptocurrency and virtual currency: Corruption and money laundering/terrorism financing risks? In *Handbook of digital currency*, pages 283–307. Elsevier, 2015.

[10] Sajad Homayoun, Ali Dehghantanha, Marzieh Ahmadzadeh, Sattar Hashemi, and Raouf Khayami. Know abnormal, find evil: frequent pattern mining for ransomware threat hunting and intelligence. *IEEE transactions on emerging topics in computing*, 8(2):341–351, 2017.

[11] Opeyemi Osanaiye, Haibin Cai, Kim-Kwang Raymond Choo, Ali Dehghantanha, Zheng Xu, and Mqhele Dlodlo. Ensemble-based multi-filter feature selection method for ddos detection in cloud computing. *EURASIP Journal on Wireless Communications and Networking*, 2016(1):1–10, 2016.

[12] Martin Arnold. Five ways banks are using blockchain. *Financial Times*, 16, 2017.

[13] Bernard Marr. How blockchain will transform the supply chain and logistics industry. *Retrieved February*, 22:2018, 2018.

[14] Reza M Parizi, Ali Dehghantanha, et al. Smart contract programming languages on blockchains: An empirical evaluation of usability and security. In *International Conference on Blockchain*, pages 75–91. Springer, 2018.

[15] R Aitken. Smart contracts on the blockchain: Can businesses reap the benefits. *Forbes*, 2017.

[16] K Megget. Securing the supply chain. 2018.

[17] Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, and Mohammed Samaka. Security services using blockchains: A state of the art survey. *IEEE Communications Surveys & Tutorials*, 21(1):858–880, 2018.

[18] Paul J Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M Parizi, and Kim-Kwang Raymond Choo. A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, 6(2):147–156, 2020.

[19] Marcella Atzori. Blockchain technology and decentralized governance: Is the state still necessary? *Available at SSRN 2709713*, 2015.

[20] Deepak Puthal, Nisha Malik, Saraju P Mohanty, Elias Kougianos, and Chi Yang. The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine*, 7(2):18–21, 2018.

[21] Chi Yang, Deepak Puthal, Saraju P Mohanty, and Elias Kougianos. Big-sensing-data curation for the cloud is coming: A promise of scalable cloud-data-center mitigation for next-generation iot and wireless sensor networks. *IEEE Consumer Electronics Magazine*, 6(4):48–56, 2017.

[22] Deepak Puthal, Rajiv Ranjan, Surya Nepal, and Jinjun Chen. Iot and big data: An architecture with data flow and security issues. In *Cloud infrastructures, services, and IoT systems for smart cities*, pages 243–252. Springer, 2017.

[23] Stefan K Johansen. A comprehensive literature review on the blockchain as a technological enabler for innovation. *Dept. of Information Systems, Mannheim University, Germany*, pages 1–29, 2018.

[24] Tejal Shah and Shalilak Jani. Applications of blockchain technology in banking & finance. *Parul CUniversity, Vadodara, India*, 2018.

[25] Stefan Seebacher and Ronny Schüritz. Blockchain technology as an enabler of service systems: A structured literature review. In *International Conference on Exploring Services Science*, pages 12–23. Springer, 2017.

[26] Lawrence J Trautman. Is disruptive blockchain technology the future of financial services? 2016.

[27] Ittay Eyal. Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities. *Computer*, 50(9):38–49, 2017.