International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 02, 2020
ISSN: 1475-7192

# Crypto Wallet: A Perfect Combination with Blockchain and Security Solution for Banking

[1]Nagendra Singh Yadav, [2]Vishal Kumar Goar, [3]Dr. Manoj Kuri

***Abstract:*** *A Bank is a financial institution which receives deposits and grant loans to its stakeholders. Finance is a stream of banking that involves settlement and controls the withdrawal and deposits. When a currency in the form of* ***cash*** *is deposited into a bank, it is taken care of by the finance process.E-wallets become a traditional method of banking these days since we have entered the age of digital banking, with which we can see a number of security loopholes specific to payment gateways, where the hackers steal the money from credit or debit cards by diverting the OTP to themselves. It all starts with a minimum amount, but the impact is bigger when the per-transaction amount is increased, by every attempt. The SIM clone is another problem area, which needs to get fixed these days. Using SIM clone, anyone can steal money from a user's account, if or not you are using online banking.This research paper touches on how effectively the banking system can handle frauds related to transactions by ensuring authenticity with the implementation of the system powered by blockchain.*

***Keywords****: Banking, Finance, UPI, Crypto, Blockchain, Crypto wallets, E-wallets.*

## I. INTRODUCTION

The block chain is one of the most talked-about topics in the corporate and academic world. A Distributed and network based technology "Blockchain" is a place into which information is stored in a Digital form into Shared Distributed Database [8-9]. Bitcoin has lead to the popularity of Blockchain Technology. In order to ensure the security and control over the data, Bitcoin equips Blockchain Technology [10-11]. The word Blockchain means storage of data into digital blocks and form a chain so that every time a new record is added to a block it becomes a part of existing chain. In order to keep a record, blockchain uses a ledger based system such that all the transactions are recorded onto it and it is accessible by everyone making it a public ledger. Blockchain was the only founding stone using which cryptocurrency was invented and designed. Cryptocurrency is one of the key reasons this technology has made really famous. [12,13] The cryptocurrencies also contain digital currencies and virtual currencies. Bitcoin is the first Blockchain technology to use crypto-money [14]. The virtual currency such as Bitcoin doesn't require any existence of central authority to facilitate the transaction and its processing. Bitcoin came into existence for the first time in the year 2008, right after the Global great financial depression that has sunk the markets all over the globe [15,16]. One of the main reasons for creating bitcoin was to overcome financial crises as they clearly demonstrated flaws in the traditional banking systems around the globe! The bitcoin was invented to facilitate the money transaction at the cheapest price per transaction internationally. But the journey of bitcoin never went exactly how it was planned. In short, the bitcoin was used widely in activities related to money

[1] *Govt. Engineering College Bikaner, Rajasthan, India, nksyadav100@gmail.com*

[2] *Govt. Engineering College Bikaner, Rajasthan, India, , dr.vishalgoar@gmail.com*

[3] *Govt. Engineering College Bikaner, Rajasthan, India, kuri.manoj@gmail.com*

**Received: 23 Dec 2019 | Revised: 05 Jan 2020 | Accepted: 27 Feb 2020** 

laundering and its purchases in the black market. This has left only one choice for the governments around the global, that is to ban the use of it [17-18].

There are a lots of misconceptions when we talk about bitcoin and blockchain . To make the difference clear, the bitcoin is a currency, a digital currency that uses blockchain to facilitate the transaction management and processing.[19]. The Blockchain technology can be used in other industries and in has several applications to offer. The highest potential of Blockchain exists in the finance and banking sectors.

## II. REVIEW LITERATURE

The author discusses how Bitcoin-beyond blockchain work bridges those flaws and some of the unresolved problems. Cryptocurrencies blockchains specifications and guarantees do not fit FinTech 's requirements on security and privacy from transaction throughput to primitives [1]. It analyses the safeguarding process of the distributed database and suggests a solution for the challenges of retaining the information confidentiality in them without token based on Blockchain. The authors say that without using mining and tokens, blockchain would significantly unravel procedure to maintain the confidentiality and validity of knowledge regarding bank transactions [2]. In this work Blockchain technology addresses the problem of cryptography consensus. And if there is a method to assure financial activity and transaction actions are stored in a particular databases without the central authority's intervention. It analyses the main design and technological features showcased by blockchain, and presents scenarios into which blockchain applications can be applied [3].

The research paper focuses on the use of blockchain as the Central Bank Digital Currency (shortly known as CBDC) basic prototype technology. The Central Bank Digital Currency prototype will benefit from the supervision, payment and use of the Blockchain technology. Problems such as safeguarding the confidentiality, transparency and speed of user transactions should be resolved to use the blockchain as CBDC 's fundamental technology [4].

This paper explores the challenges and opportunities posed by banking through the introduction of blockchain technology. The blockchain technology will turn the global financial system to achieve sustainable development, using systems that are more effective than they are at the moment [5]. Starting a prototype of E2E (end-to-end) interbank Payment Systems (IBPS) based on Hyperledger Fabric company's blockchain network. The model shows the business blockchain manifesto, which are defined by Hyperledger Fabric, capable to ease more productive and stable payment solutions [6]. The research proposes a model of systemic innovation to explore and track pathways to innovation. In order to Understand the growth cycle of innovation and the approach for winning market share of the banking sector, this model may be applied to any industry. The empirical results indicate the situation in which lots of banks are yet to develop or migrate their tradition banking system to Blockchain technology. The study, which is established on the structural innovative prototype, showcases the currently low structural characteristic of Blockchain banking [7].

## III. UPI (UNIFIED PAYMENT INTERFACE)

Unified Payment Interface typically known as UPI is a real-time mode of payment system that aims to settle all the transactions amongst “banks”, which was developed by the National Payments Corporation of India.[22]

All the money transactions are made using mobile platforms and transactions are instant in nature, keeping RBI track of Interface regulations. In other words, it's an integrated form of banks on a single mobile, powers up all the banking features by merging them all together and forms a cluster [20]. The user gets one single mobile application, using which they can maintain several other bank accounts. It does offer two Factor authentications like any other banking system.

Combining the functionality of UPI with E-wallets facilitates users to make payments just in nick of time by scanning QR code. The amount of money is debited and credited in real-time, so the user doesn't have to wait in a queue to make a deposit like any other banking system. The amount is deducted from the user's bank account itself, which makes the processing system more efficient.

## IV. CRYPTO WALLET

A Crypto wallet is made up of software which contains private and public key and uses blockchain to send and receive currency.[21] The currency in these wallets is added in the form of coins, such as bitcoin, Litecoin, etc. To trade or send or receive crypto coins or currency, one requires the crypto wallet gets created. The currency is not stored at one location instead they all exist in the form of transaction records on the blockchain.

As these wallets store private and public keys, a user is facilitated with various operations such as to send or receive coins, monitor coin balance, trade the coins on portfolio using the wallet. This also ensures the privacy of the user by using a hexadecimal address of the wallet. However, the address of currency to be exchanged differs from one service provider to another.

## V. TRADITIONAL E WALLETS

The traditional E–wallets comes with prepaid and Post-paid options which is to be opted by the user. It's a wallet that doesn't require the existence of a card, instead, a wallet is created into with money is added in the first place. Later on, that wallet can be used for transactions.

The transaction can differ from its usage as one can use E-wallet to make a payment directly from their bank account using UPI or they can either pay via wallet itself. After each transaction, the entry in the database is updated for the mode of payment that was adopted and the same will reflect in the customers wallet or bank account.

The implementation of prepaid and post-paid wallets can be seen into Paytm, in which they have recently started the post-paid mechanism that ensures that customer is able to spend the money from wallet up to a certain limit.

However, the E-wallets are designed to facilitate the transactions with the help of handheld devices such as smartphones which requires internet availability as a prerequisite. These wallets can be used on browsers to facilitates the transactions opted by the users.

## VI. IMPLEMENTATION OF CRYPTO WALLETS USING BLOCKCHAIN –

This implementation of a mobile-based crypto wallet using blockchain could be seen in the form of a Coinbase wallet, which is a mobile-based crypto wallet. [23]

This Crypto wallet is a mobile-based wallet, apart from transaction facilities they do offer multi-layer authentications, such as while accessing Coinbase Account from the browser, they ask for OTP as well as authentication for the device using email facility.

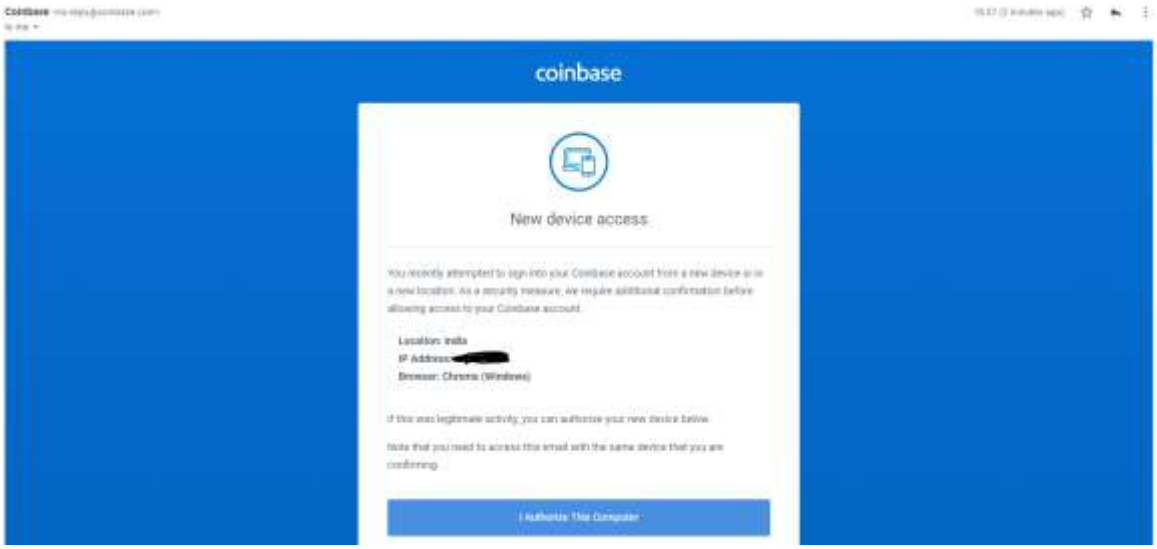


Figure – Coinbase E mail Authentication

***For security reasons we have to hide the IP address of the device used.**

Below is a transaction snip obtained using real-time bitcoin transfer from Coinbase Portfolio to Coinbase wallet. The transaction is a real-time transaction. A typical Bitcoin transaction Takes around 10 minutes of time, to reach the transaction confirmation stage.

Coinbase portfolio is a trading platform of cryptocurrency, which allows a user to trade and transfer crypto in various cryptocurrency as Litecoin, Bitcoin, etc. When a user trades in cryptocurrency and wants to transfer this cryptocurrency to its own or to a different wallet, the portfolio captures the last updated currency (i.e. USD$) value at the time of crypto transfer transaction.


**Figure 2–** Real-time Transaction of bitcoin from Coinbase portfolio to Coinbase wallet.

The above figure contains the transaction record of bitcoin which is initiated to Coinbase wallet from Coinbase Portfolio. The time and date stamps are associated with the transaction logs as displayed in above figure.

An average user has to wait for 10 minutes for a miner to record a transaction on the blockchain. Below is the snippet which contains Blockchain log for this transaction –

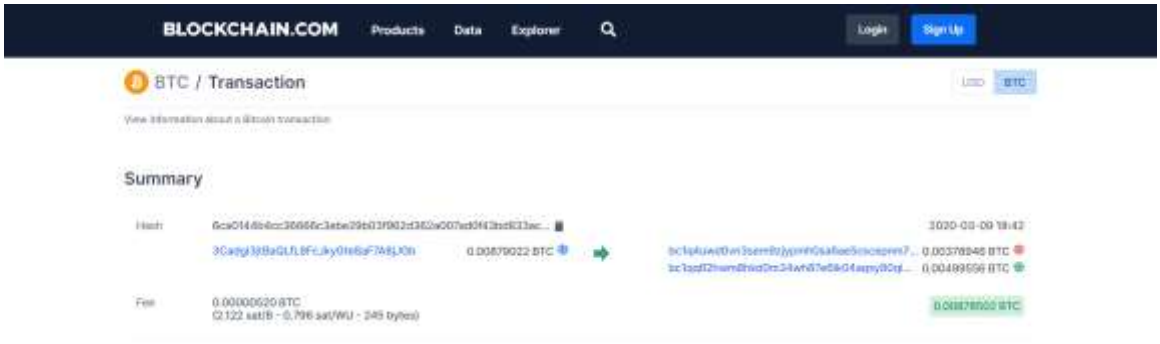


**Figure 3–** Blockchain Record of a Bitcoin transfer

The above figure contains the blockchain record on which the transaction records are being maintained to ensure all the transaction are recorded. For each transaction a miner fee is charged depending on the amount of bitcoin transfer equivalent to Santoshi.

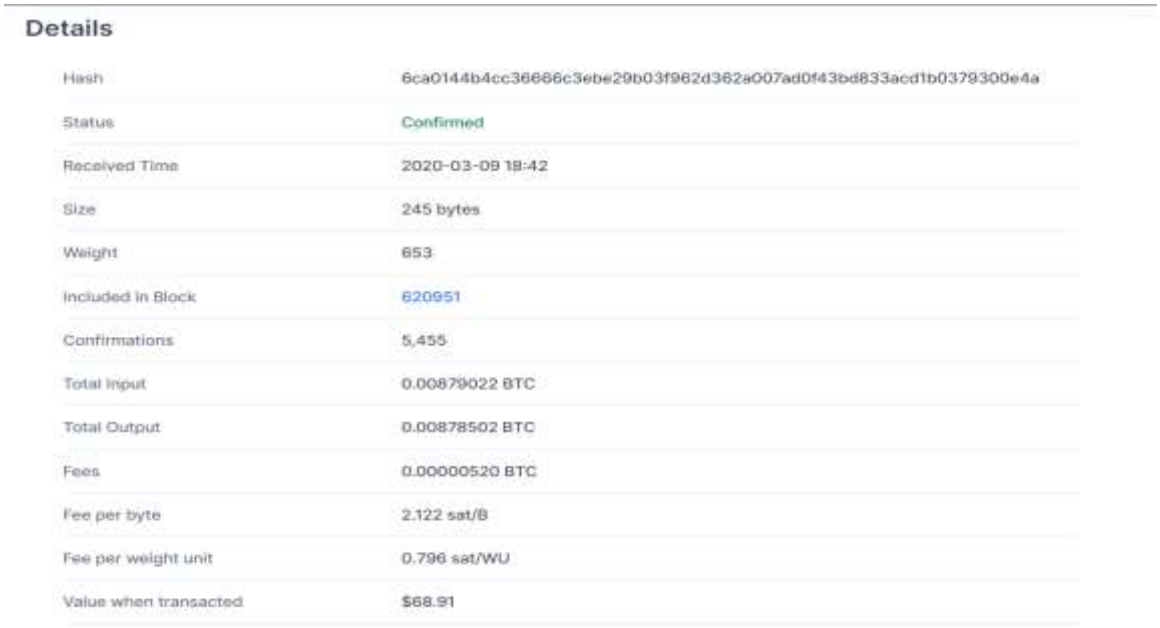


**Figure 3.1 –** Blockchain Record of a Bitcoin transfer

The above figure displays the Hash number or address, status of the transaction, date and time of transaction, the block number on to which transaction was recorded, along with all the bitcoin transfer equivalent to satoshi.

**Received: 23 Dec 2019 | Revised: 05 Jan 2020 | Accepted: 27 Feb 2020** 


**Figure 3.2 –** Blockchain Record of a Bitcoin transfer


**Figure 3.2 –** Blockchain Record of a Bitcoin transfer

Every Transaction in the blockchain is recorded by miners by charging miner fees in the form of some satoshi.

The Coinbase wallet offers wallet creation, unlike others where they ask for a password. Instead, Coinbase wallet creation only requires a user phrase that has to remember by user and the same can be stored of google drive as a backup code. There is no way to recover the account if the user has lost or forgot the phrase, meaning the user will no longer be able to access any of the wallet cryptocurrencies.

The wallet offers multiple transactions in the form of cryptocurrency upon providing the user with a unique address for each crypto transaction for a specific cryptocurrency.

The wallet is listed on the app store so that it can be used for mobile purposes.

For security reasons, the wallet username is cropped to protect the identity of the user. Below is the snip of Coinbase mobile wallet-


**Figure 4 –** Coinbase mobile wallet default screen

The above window is displayed to the user upon successful wallet creation. Please note that the username at this window has been cropped due to security reasons. At this screen the total amount of satoshi or crypto currency equivalent value in currency (based upon user selection) is displayed at this window.

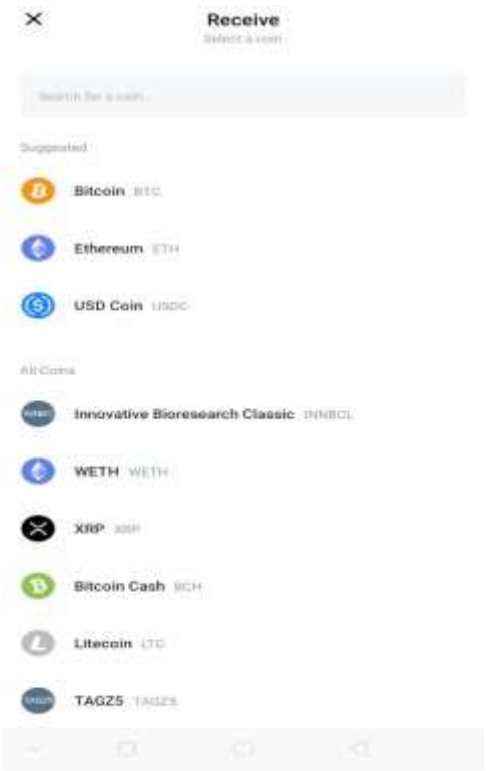


**Figure 4.1 –** Coinbase mobile wallet receive screen

The above Figure contains the all sort of cryptocurrency which a user wishes to receive or send.


**Figure 4.2** – Bitcoin wallet address of a Coinbase wallet

To receive a cryptocurrency in this example as bitcoin, a user has to share its wallet address to receive the cryptocurrency. With the help of the above figure, we can see that the user's privacy is maintained by hiding the information using specific addresses of wallets for each transaction without providing the actual details of the users such as bank account numbers. This ensures more trust in the system by relying on authenticity of each transaction which is impossible to delete once recorded.

## VII. PROBLEM STATEMENT

The Tradition online wallets don't guarantee to customers that they are secured with the type of wallets they choose. With time it has been proven that there is no such technology exists that can empower the banking system and protect customers' rights and customers against financial frauds. As goodwill comes with a cost that is a trust which takes years of time to build. The problem with the wallets is that they have a certain length of a password which can be obtained easily by the hackers. Similarly, OTP verification can be bypass through the system in fever cases such as credit cards to facilitates and steal the money.

## VIII. PROPOSED METHOD

As we have demonstrated in this research paper how a blockchain-based crypto wallet ensures transaction security and authenticity, using which we can prevent against such financial frauds.

**Received: 23 Dec 2019 | Revised: 05 Jan 2020 | Accepted: 27 Feb 2020** 

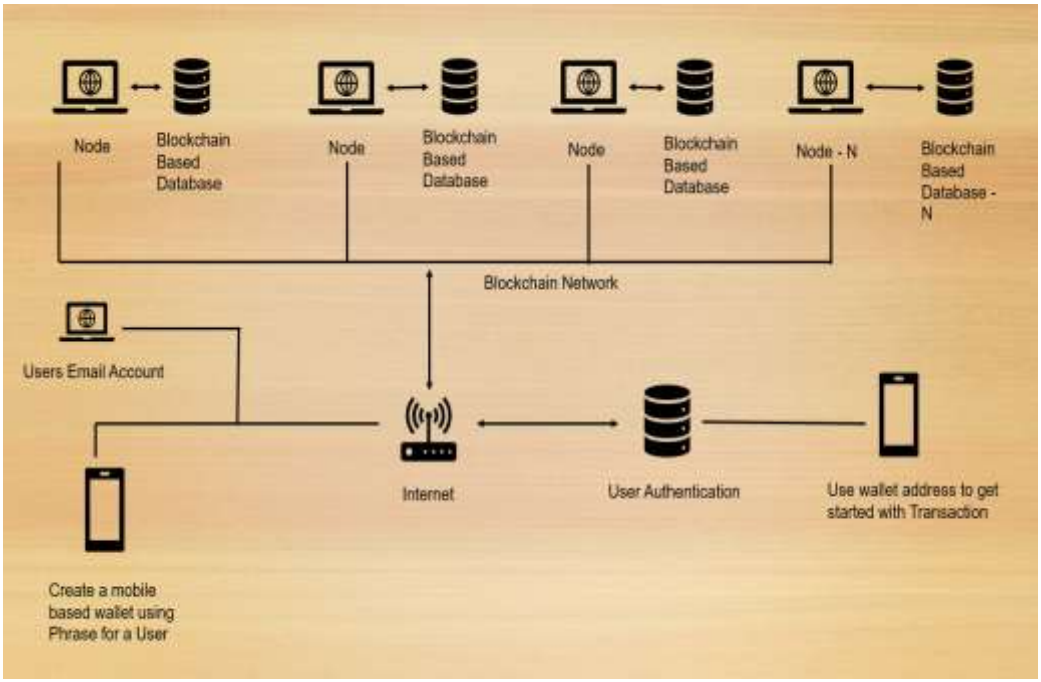


**Figure 5 –** Workflow for proposed method

Below are the parameters to be included or to be a part of the banking system to enhance transaction security using blockchain-based e-wallets – –

a. Instead of creating wallets with a password, mobile number or email address, the wallet should be created using a Phrase. This Phrase is provided to the specific user at the time of wallet creation. The customer can download the application on their mobile phone or smartphone and then instead of logging in, the customer has to enter the phrase which they have used at the time of the creation of a wallet. After entering the correct phrase only, a customer is authenticated in the system and upon verification, the customer can start with transactions using online wallet.

b. Email must be used to verify and monitor the transaction activity. Until or unless the verified user doesn't authenticate login with an email confirmation (by clicking on URL on the email sent by the wallet application), the login should not be initiated. Each transaction using the wallet should be recorded on the blockchain. After each transaction corresponding transaction email should be sent to the customers' email address.

c. A customer can initiate the transaction using a wallet address that can be also used to receive the transactions. This will also hide the customers' information from the outside world.

## IX. ANALYSIS

We do require blockchain implementation in the core banking system so that we can ensure that each transaction is authenticated and it is initiated by the user itself. Although the adoption of this technology is very feasible and reduces the security overhead that comes with a traditional banking system such as centralization. Blockchain-based wallet system and banking system dismantles the centralization of data and stores the data at several places since its key to success is the distribution of data across the network at the distributed databases. The data and customers both are very secured in the hands of the blockchain-based technology banking system.

**Received: 23 Dec 2019 | Revised: 05 Jan 2020 | Accepted: 27 Feb 2020** 

## X. CONCLUSION

The adoption of technology depends on the requirements of the business here in the case is for the banking system. The no of profits margin derives the adoption of technology. Most of the Banks around the globe have adopted blockchain as they value customer's privacy in the first place. There are always pros and cons related to each technology which goes the same in the case of blockchain too. They only problem with technology is the cost. The cost drives the business day to day operations, so this is where the banks have to think carefully before the adoption of this technology. The blockchain-based banking system becomes more temper proof when it is powered by blockchain.

## REFERENCE

1. Eyal, I. (2017). Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities Computer MDPI AG
2. Popova, N.A., Butakova, N.G. (2019). Research of a possibility of using blockchain technology without tokens to protect banking transactionsProceedings of the 2019 IEEE Institute of Electrical and Electronics Engineers Inc.
3. Wu, T., Liang, X. (2017). Exploration and practice of inter-bank application based on blockchain ICCSE 2017 - 12th International Conference on Computer Science and Education Institute of Electrical and Electronics Engineers Inc.,
4. Sun, H., Mao, H., Bai, X., (...), Hu, K., Yu, W. (2018). Multi-blockchain model for central bank digital currency Parallel and Distributed Computing, Applications and Technologies IEEE Computer Society
5. Cocco, L., Pinna, A., Marchesi, M. (2017). Banking on blockchain: Costs savings thanks to the blockchain technology Future Internet MDPI AG
6. Wang, X., Xu, X., Feagan, L., (...), Jiao, L., Zhao, W. (2018). Inter-Bank Payment System on Enterprise Blockchain Platform IEEE International Conference on Cloud Computing, CLOUD IEEE Computer Society
7. Harris, W.L., Wong limpiyarat, J. (2019). Blockchain platform and future bank competition Foresight Emerald Group Publishing Ltd.
8. Reiff Nathan (February 2020). Blockchain Explained. Retrieved From https://www.investopedia.com/terms/b/blockchain.asp.
9. Wu, B., Duan, T. (2019). The advantages of blockchain technology in commercial bank operation and management ACM International Conference Proceeding Series Association for Computing Machinery.
10. Wang, R., Lin, Z., Luo, H. (2019). Blockchain, bank credit and SME financing Quality and Quantity Springer Netherlands.
11. Liu, X., Yu, T. (2018). An automatic pattern recognition value system with listed banks based on blockchain Proceedings of 2018 IEEE 3rd Advanced Information Technology Institute of Electrical and Electronics Engineers Inc.
12. Li, L., Sy, M., McMurray, A. (2018). Blockchain Innovation and Its Impact on Business Banking Operations Advances in Parallel Computing IOS Press BV.

**Received: 23 Dec 2019 | Revised: 05 Jan 2020 | Accepted: 27 Feb 2020** 

13. Hassani, H., Huang, X., Silva, E. (2018). Banking with blockchain-ed big data Journal of Management Analytics Taylor and Francis Ltd.,
14. Higginson Matt, Hilal Atakan, Yugac Erman (June 2019). Blockchain and retail banking: Making the connection. Retrieved from https://www.mckinsey.com/industries/financial-services/ourinsights/blockchain-and-retail-banking-making-the-connection.
15. Hooper Matthew (February 2018). Top Five Blockchain Benefits Transforming Your Industry. Retrieved from https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefitstransforming-your-industry/
16. Farrell, S. (2019). Blockchain standards in international banking: Understanding standards deviation Journal of ICT Standardization River Publishers.
17. Guo, Y., Liang, C. (2016). Blockchain application and outlook in the banking industry Financial Innovation Springer Open.
18. Cui, L., Yuan, K., Zhao, X., Mou, L.Y.D. (2019). Construction of elderly mutual aid time bank based on blockchain Proceedings - IEEE International Conference Institute of Electrical and Electronics Engineers Inc.
19. Dozier, P.D., Montgomery, T.A. (2019). Banking on Blockchain: An Evaluation of Innovation Decision Making IEEE Transactions on Engineering Management Institute of Electrical and Electronics Engineers Inc.
20. Chatfield, A.T., Reddick, C.G. (2019). Blockchain investment decision making in central banks: A status quo bias theory perspective25th Americas Conference on Information Systems, AMCIS 2019 Association for Information Systems.
21. https://blockgeeks.com/guides/cryptocurrency-wallet-guide/
22. https://www.npci.org.in/product-overview/upi-product-overview
23. https://www.coinbase.com/

**Received: 23 Dec 2019 | Revised: 05 Jan 2020 | Accepted: 27 Feb 2020** 