|| Volume 6 || Issue 6 || June 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

DIGITAL INDIA DIGITAL ECONOMY USING BCT

Prajwal Deshmukh[1], Gargi Kulkarni[2], Meezan Shaikh[3],Vaishnavi Taral[4], Dr. K. S. Thakare [5]

Dept of IT Engineering, SAE, Savitribai Phue Pune University, Pune, Maharshtra, India [1,2,3,4,5]

Abstract: Moneyless communities have existed since the time human communities came into existence. Human beings used the "barter system" wherein they exchanged items as per their requirements. Eventually, we moved on to the money system using cash, coins etc. However, as the value of money increased and cyber security became a concern in online transactions. So, we once again find ourselves moving from cash to cashless transactions. Non-cash transactions are now very convenient since it is possible in modern times to use digital currencies for online transactions. But while online transactions are convenient, it is important to focus on securing online transactions. This article focuses on online transaction systems that make use of the blockchain technology to tackle cyber security issues. In other words, official tender (money) exists, is recorded, and is only exchanged in digital (electronic) form. Such an idea has always been discussed extensively, especially since the world began to address the rapid and increasing use of digital methods for recording, managing, and exchanging money in commerce, investment and daily life in many parts of land, and trade. Money made is usually paid electronically. Some countries now impose restrictions on transactions and transaction rates that can be legally used for non-electricity payments. Here in this paper, we will discuss how we can use the blockchain digital India digital economy technology.

Keywords: *Digital Economy, Cash, SHA256, AES, Digital India, Java, JSP , Servlet.*

I INTRODUCTION

Today money is not safe in the form of cash and banks. Consider this scenario: Rs 10 lakh invested in a fixed bank for 2 years. Interest for every quarter of the seven areas was received or accepted, but a few months before the deposit gets matured, bank due to an increase in financial problems (which eventually led to the bank's regulator placing more controls) doesn't pay hard work on maturity. In many such cases, investors have lose their hard-earned money to banks due to financial mismanagement of banks - and as a result, the Reserve Bank of India (RBI) has taken Prompt Corrective Action (PCA) against them. Currently, Central Bank of India ,UCO Bank, Maharashtra Co-operative (PMC) Bank , United Bank of India, , Indian Overseas Bank, Punjab and, to name a few are under RBI's PCA . The record-breaking history of cooperative banks is daunting. According to RBI data, there were 1,926 Bank Cooperatives (UCBs) in 2004; and 16 years ago, the RBI was forced to merge 129 weak alliances with strong banks. About 246 UCBs have fallen in the last 16 years. Day by day, the risk of automatic failure is swiftly increasing; potential risks are well- organized and things can get out of hand quickly if timely measures are not taken. The latter, namely the 21st edition of the Financial Stability Report (FSR) released by the RBI, identifies a number of negative risks, although India's financial system remains stable. All major indicators of risk, global risk, financial market risk, and expected macroeconomic risk, remain in the 'high' to 'high' range. The RBI has warned all stakeholders of the potential increase in the sector's Gross Non- performing Assets (GNPAs) in the future. As natural calamities, pandemics and man-made disasters continue to affect health and livelihoods, the impact on debt growth, the quality of banking assets, and banking adequacy is severe.

The redistribution of corporate balance sheets, that made steady progress in the pre-pandemic era, had a significant impact on the economy of countries. Macro's credit risk assessment shows that the GNPA rating for all SCBs could rise from 8.5 percent in March 2020 to 12.5% in March 2021 under the first round. If the macroeconomic situation worsens, the rate could rise to 14.7 percent under greater pressure, according to RBI's Financial Stability Report. According to the FSR, approximately 67% of the public bank customers (PSBs) and 49% of the private sector customers received the suspension from April 30, 2020. About 1/3 of the private sector bank loan and 2/3 of the PSBs were under suspension. This is an ominous situation. In many cases, the government has made sure that the bank depositors are safe; but such guarantees cannot be entirely trusted. Given that the NPAs of many banks are increasing, customers' hard- earned money is not 100 percent secure in banks. Financial pressures on the Indian banking system (and the credit market) are very constructive, and this rise in the level of the system could explode the investors' money without error.

The government introduced the Financial Dispute Resolution and Financial Insurance (FRDI) Bill in Parliament in August 2017 but withdrew it in August 2018. Bail- in is contrary to bail release. When a government rescues a bank, it primarily uses taxpayers' money to save the business. Conversely, the bail-permit clause allows the use of the investors' money to reduce bank debt. But with so much media opposition, the government has had to back down from the proposal. Just before the COVID-19 pandemic hit the country in March, the government was considering introducing a modified version of the FRDI, and re-introducing it as the Bill Sector Development and Regulation (FSDR) Bill. And now that the banking and financial sector is under a lot of pressure in the midst of the coronavirus, negotiations to establish a solution under the legal framework of the new FSDR system have begun to form. Non-Banking Companies (NBFCs), payment banks, insurance companies, major market players, cooperatives, local banks all will be under the proposed settlement authority. A systematic approach to formal funding to deal with depressed assets is required, according to RBI Governor Shaktikanta Das.

II LITERATURE SURVEY

The practice of money laundering and the realization of everyday life began in the 1990s, when electronic banking was on the rise. With the 2010 digital payment methods becoming more widespread. Examples include mediators such as PayPal, digital wallet systems such as Apple Pay, telecommunications and NFC payments via electronic or smartphone card, and electronic bills and banking, all broad uses. [3] At this point money was no longer desirable in other types of transactions that would historically be the norm to pay by tangible tender, and large sums of money in some cases were treated with suspicion, due to its flexibility and ease of use in money laundering and terrorist financing. In addition, payments in large amounts have been strictly prohibited by some suppliers and retailers, [5] to the point of coining the term "money war". [6] The 2016 U.S. Consumer User Survey states that 75% of respondents have chosen a credit or bank card as their payment method while only 11% of respondents prefer cash. [7] Since the establishment of the two companies in 2009, digital payments can now be made through mechanisms such as Venmo and Square. Venmo allows people to pay directly to other people without earning money. Square is a new feature that allows especially small businesses to receive payments from their customers.

In 2016, only about 2% of the value generated in Sweden was cash, and only about 20% of commercial transactions were in cash. Less than half of the country's banking branches conduct cash transactions. [2] Cash withdrawals are considered to be banking that persuades employers to make direct payments in the 1960s, banks that charge checks that started in the 1990s, banks introduced a simplified Swiss smartphone-to-phone system in 2012, and Zettle's introduction of small retailers accepting creditcards-2011. [2]

Existing online payment systems are vulnerable to cyberattacks and undemocratic. Cyberattacks like ransomware attacks are especially prominent in the existing online payment systems. The dependency on a single central authority for payments is a major cause of these attacks.[9]

S. Kumari and S. Farheen's "Blockchain based Data Security for Financial Transaction System," [12] focuses on providing security to the blockchain system using various mechanisms. The proposed model consists of the financial transaction based system which works on the RFID technology. The data obtained from the system can be only accessed by the clients who are authorized hence providing the first level of security by providing authentication to the valid client using M2M authentication. Once the user is authenticated, The proposed system is a financial transaction-oriented system that uses RFID technology. The data from the RFID passive tag is captured and collected from the RFID reader and is placed in the server (local system).The data that is stored in the server is stored using the blockchain mechanism. The hash is divided, and one part is stored in the cloud which is Amazon s3. This mechanism incorporates the first level of security. The second level of security is achieved by authenticating the client with M2M authentication. The user who wants to access the data present in the blockchain needs to get authenticated first; the process of authentication is provided by the RSA algorithm. The keys are generated using the RSA(Rivest-Shamir- Adleman) mechanism.

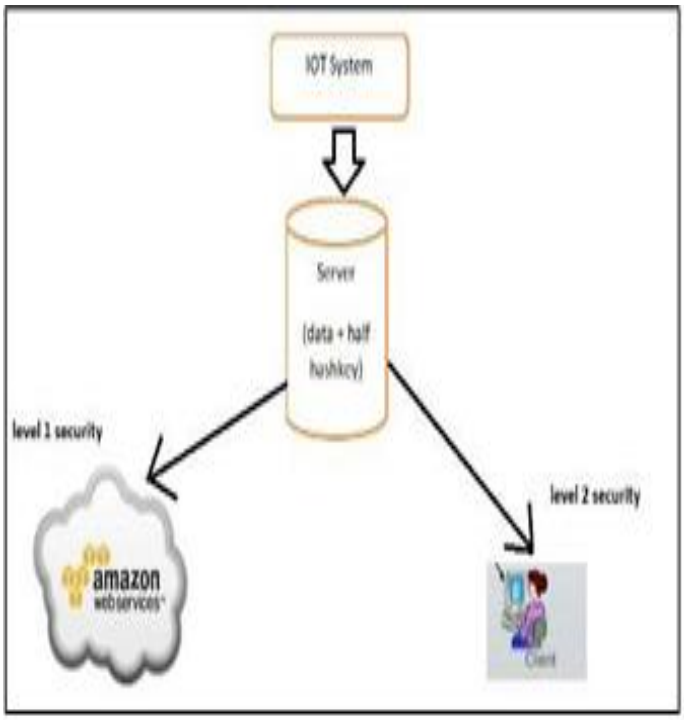

FIG.1 RFID BASED DIGITAL PAYMENT SYSTEM

The purpose of the key is to enable mutual authentication between a user and the IoT system. The key size ranges from 1024 to 4096 bit typical. The keys are private and public which are employed for RSA. Here the public key is kept at the server and a private key is given to the client. The process of encryption and decryption takes place. That is an OTP is generated using the random class method where OTP is encrypted using the public key of the server and sent to the user. If the client is a valid user, then the client will be able to decrypt using his private key and tell the OTP to the server. For this process to take place the keys are exchanged in the form of the certificate. The OTP, certificate, private and public keys are kept in the database and filled by the server and the client when it's time to fill their fields.

Technologies and Algorithms used:

IoT Environment

RFID (Radio-frequency identification) for data communication Amazon S3 for data storage

RSA Algorithm for process of authentication

SHA-1 Algorithm to generate hash for the blocks.

As a result, They have successfully implemented the e-commerce payment system for both merchant and customer. So First, when the customer selects a product on the merchant's online shopping mall, the payment screen generates. The customer scans the QR code to execute the payment procedure. The blockchain subsystem transmits the payment result to the merchant and the customer. tests were run sequentially on the merchant, customer, and blockchain subsystems. The verification process confirmed whether the digital signature for the merchant's message, as well as that for the customer's message, was accurately created .

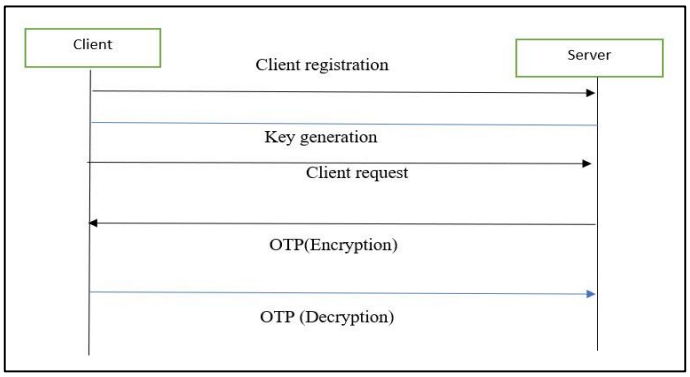

FIG.2 CLIENT SERVER INTERACTION

Following the advent of digital payment systems , several efforts been made about leveraging the advantages of the blockchain technology to better digital payments. One such study , E-commerce payment model using blockchain Shee-Ihn Kim1 · Seung-Hee Kim1 Received: 6 March 2019 / Accepted: 4 September 2020 © Springer- Verlag GmbH Germany attempts to do away with the payment gateways associated with the digital payment system.

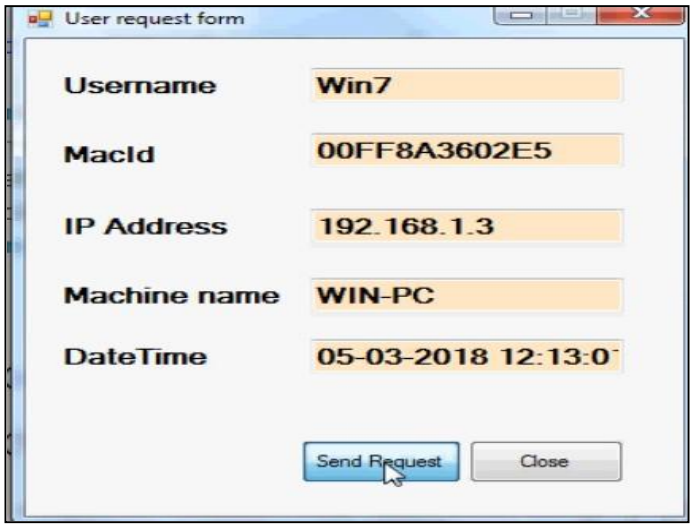

FIG. 3 A) USER INTERFACE

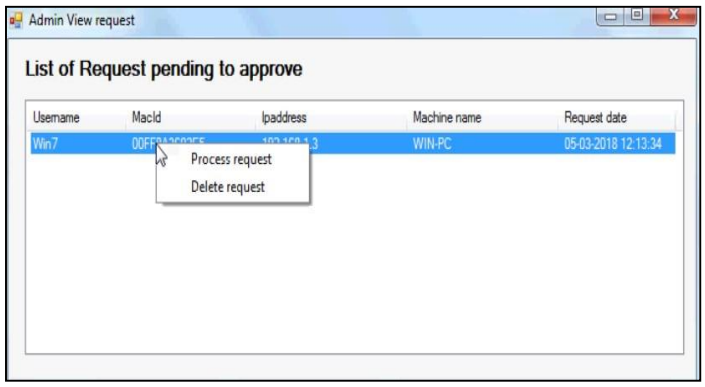

FIG. 3B) VIEW PENDING REQUESTS TO BE APPROVED

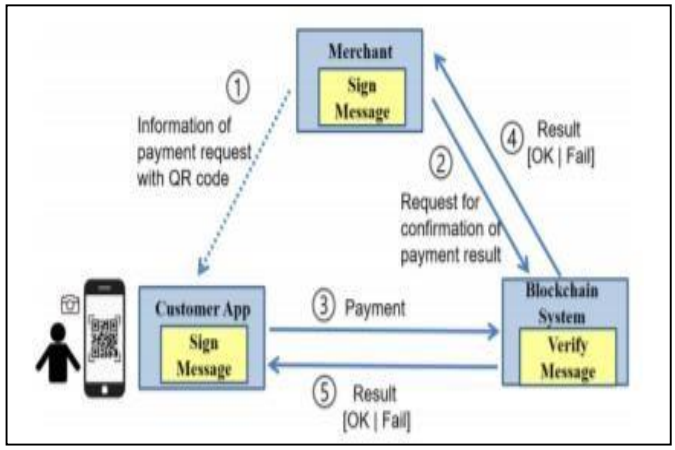

FIG.4 PAYMENT MODEL USING QR CODE

This paper proposed blockchain e-commerce payment system comprises the merchant, customer's smartphone application, and blockchain system. The payment processing procedure is as follows:

1) After selling its products and services, the merchant requests the customer to make payment using a blockchain cryptocurrency, merchant makes the payment request through a QR code displayed on the customer's web browser where QR code contains the information of M_Address, Amount, Time Stamp, M_TX_ID, and Merchant's Digital Signature as a QR code.
2) To confirm whether the customer has made the payment, the merchant requests confirmation to the blockchain system.

After purchasing products and services from the merchant, the customer scans the QR code to pay the price to the merchant. The payment is not transmitted directly to the merchant. Request is made to the blockchain system, which contains the transaction ledger.

3) The blockchain system deducts the payment amount from the customer's account and raises the same amount in the merchant's account. After executing this transfer between the accounts, the blockchain system transmits the results to the merchant. The merchant confirms the payment ,and begins to provide the purchased service to the customer.
4) The blockchain system also transmits the payment result information to the customer's smartphone application.

As a result, They have successfully implemented the e-commerce payment system for both merchant and customer. So First, when the customer selects a product on the merchant's online shopping mall, the payment screen generates. The customer scans the QR code to execute the payment procedure. The blockchain subsystem transmits the payment result to the merchant and the customer. tests were run sequentially on the merchant, customer, and blockchain subsystems. The verification process confirmed whether the digital signature for the merchant's message, as well as that for the customer's message, was accurately created .

FIG.5.A) RESULTING APP USING QR CODE

FIG.5.B) USER INTERFACE

Another such system was proposed in R. Gupta, C. Kapoor and J. Yadav, "Acceptance Towards Digital Payments and Improvements in Cashless Payment Ecosystem," 202 0 International Conference for Emerging Technology (INCET), 2020.[11]

This proposal leverages the use of the relatively new smart contract payment system , using Ethereum. a reliable, secure, and contemporary working model for a Digital Payment Wallet where shared e-wallet is used primarily to support transactions made by minors under the supervision of their parents. Therefore, a rather secure and contemporary transaction technology . Where the following steps have been followed:-

1) Create an account to deploy Smart Contract on Ropsten Test Network.
2) From Ropsten Test Faucet, Transfer 1 ether to the user account created by mentioning the account address.
3) Transfer funds from one wallet to another by providing the primary account address and the amount of transaction to "*transferTo*" function.
4) Primary 1 receives the notification for confirming the transfer of funds.
5) When the transaction is confirmed, funds are successfully transferred, and wallet balance is updated suitably.
6) For Adding new participant (primary or minor digital user), Primary 1 can add another primary account, Primary 2 by calling the function *"add_owner"* in the backend, using the address of the Primary 2. This will send a request to add 'Primary 2' to the other primary users of the shared wallet. If accepted, Primary 2 is successfully the added owner of the shared wallet.
7) We can also check the current wallet balance by calling *"wallet_balance"* function in the backend of Remix IDE.
8) If minor account makes a transaction of amount greater than spending limit, primary account receives an alert to grant or decline permission.

FIG.6 A) PAYMENT APP USING ETHEREUM SMART CONTRACT

FIG.6 B) PAYMENT APP USING ETHEREUM SMART CONTRACT

: SETTINGS

While this proposed system does a commendable job of using the Ethereum ecosystem, there is still the need to ease Indian economy trusting and accepting cryptocurrencies as a norm. While research is on going on such topics , it is important to keep in mind that not every layman possesses the knowledge or the resources to carry out payments by making use of cryptocurrencies.
One way to overcome these problems associated with existing online payment systems is the use of blockchain technology to create a decentralized system that uses distributed databases.

Such systems have been previously conceptualized , that suggest an architecture to seamlessly integrate e-wallets of different banks and participating institutions using blockchains that shall act as a foundation of Digital ledger technology (DLT) for financial sector in India. A swarm based peer-to-peer network is designed for the proposed ewallet system .The proposed solution shall minimize the load on the Core Banking Solution of the banks thus reducing the loadon the servers at the data centres.[9]
While such systems provide a better level of protection against cyber-crimes ,there is still some scope for levelling up the security of transactions , especially at the user's end. There is scope for improvement.

III PROPOSED SYSTEM

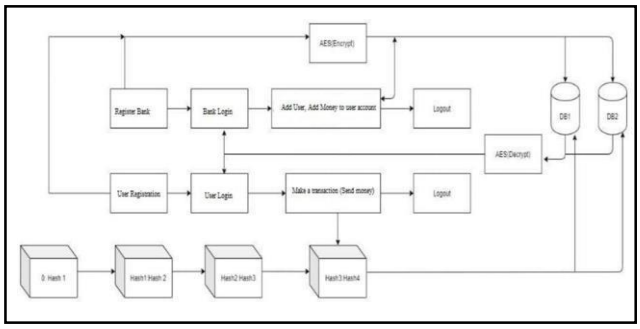

FIG. 5 PROPOSED SYSTEM ARCHITECTURE

The system Fig. 1 is a combination of two separate entities i.e. an Android application on the user's end to initiate the transactions. The users added to a bank's database are managed by the trusted authority using a web interface , created using JSP servlets .Each time a new user(customer) creates an account in a bank , her data is stored in an encrypted database. The data is encrypted using the Advanced Encryption Standard(AES).When the user successfully initiates a transaction , the details of the transaction are stored securely in the form of an encrypted block. Each block is "connected" with the previous block by creating a chain of sorts by using hash values. These hash values are generated each time using the details of current transaction and the hash value of the previous block.

The Secure Hash Algorithm(SHA-256) is used to generate unique hash values for each block .As shown in the diagram, the important components of the diagram are AES encryption block, AES decryption block, Transaction Block, Block chain, and databases. So, whenever user registers to system the information will be first encrypted and then stored to the DB1and DB2 simultaneously, whenever user wants to login the information from the database will be first decrypted i.e. regained into original format and feed for the login. When bank logins, bank can add user, can add money to user account which will be also stored simultaneously to both the databases. Whenever user logins to the system user can add beneficiary and transfers the amount or make a transaction after which a block will e generated which will add to the block chain.

Whenever a transaction is to take place in the system, a record of that transaction is kept in the form of a hash value in the block. Each subsequent block will be attached to the previous block and in this way a series of visible blocks will occur. The current block hash value is determined using current block data and the previous block hash. This way if any block is invalid, then all hash blocks should be changed.

Many such copies are stored on separate servers, which will ensure data security and confidentiality.

Whenever a transaction is to take place in the system, a record of that transaction is kept in the form of a hash value in the block. Each subsequent block will be attached to the previous block and in this way a series of visible blocks will occur. The current block hash value is determined using current block data and the previous block hash. This way if any block is low then all hash blocks should be changed. Many such copies are stored on separate servers, which will ensure data security and confidentiality. Since this system uses distributed trust, it will maintain the visibility of the transaction.

IV CONCLUSION

Indeed, the road towards complete digitisation is very long. The Indian government is undertaking stern measures to promote digital payment services, for instance, the Data Protection Bill 2019. A recent initiative as of 2019 is FASTag- A digital service that mandates tolls to be paid digitally. However, while pacing up with everyday advancements, one often neglects parallel factors that slow India's digital growth by a significant rate. The fundamental objective of this study was to determine possible, yet inexplicable factors slackening complete digitisation and to discover feasible solutions that can generate improvements in a potential cashless ecosystem. Apart from noncryptic facts, like, poor network and connectivity, ineffective security and support, we find that a significant population of minors (users below 18 years of age) transact digitally, although they may not be legally allowed to do so. We see that KYC authentication is not yet mandatory at all digital platforms, and at platforms where it is, the procedure for KYC completion is not entirely digital. Also, additional fees for making wallet-to-bank transactions, partial acceptance of digital payments by merchants, unreliable processes, and the complex nature of navigation and transaction protocols, etc. cause a reduction in digital customer base. As an outcome of these findings, an improvement scope has been discussed wherein two main advantageous suggestions have been

made, including, an encrypted , distributed ledger as opposed to a central database , and most importantly the consumer doesn't have to bother with the intricacies and details associated with using cryptocurrency.

I. FUTURE SCOPE

Although the technology of blockchain is relatively simple, more effective, and highly secure, its implementation without the use of cryptocurrency is trickier. Blockchain technology will boost India's initiative to make the Indian financial system corruption free and robust to cyber threats that are
prevalent in today's day and age. Here, we recommend a capable model for advancements in the existing digital payment system. Nonetheless, a vast scope lies beyond this study., exploitation of confidential transaction information, applicability of short term loans, improvements in use of biometrics for reliable authentication, necessary user-oriented policy changes essential for India's growing economy

II. REFERENCES

[1]THE COST OF CASH IN THE UNITED STATES" (PDF). The Fletcher School Tufts University. p. 9. Archived from the original (PDF) on 1 December 2016. Retrieved 17 December2016. Henley, Jon (June 4, 2016). "Sweden leads the race to become cashless society" – via www.theguardian.com.

[2]"The UK is getting closer to becoming a completely cashless society". The Independent. May 21,2015.

[3]"Cashless-Society.org". Cashless-Society.org.Archived from the original on 2017-12-14. Retrieved 2017-01-27.

[4]Tompor, Susan (4 September 2016). "A cashless society? Some retailers turn noses up at currency". USA Today. Retrieved 3 July 2020.

[5]Negative" Interest Rates and the War on Cash". February 8,2016.

[6]https://en.wikipedia.org/wiki/Cashless_society

[7]https://www.personalfn.com/dwl/are-you-assumingmoney-in-bank-deposits-as-safe-watch-out

[8]Avoid Shortcomings of Cashless Transaction System using Blockchain,Abdulaziz Albesher; Kareem Kamal A.Ghany. 978-1- 7281-1232-9/19/$31.00 c 2019 IEEE

[9]An Interoperable and Secure E-Wallet Architecture based on Digital Ledger Technology using Blockchain ,Karan Singh , Nikita Singh, Dharmender Singh Kushwaha.2018 International Conference on Computing, Power and Communication Technologies (GUCON), 2018, pp. 165-169, doi: 10.1109/GUCON.2018.8674919.

[10]E-commerce payment model using blockchain Shee-Ihn Kim1 • Seung-Hee Kim1 Received: 6 March 2019/ Accepted: 4 September 2020 © Springer-Verlag GmbH Germany, part of Springer Nature 2020.

[11]R. Gupta, C. Kapoor and J. Yadav, "Acceptance Towards Digital Payments and Improvements in Cashless Payment Ecosystem," 2020 International Conference for Emerging Technology (INCET), 2020, pp. 1-9, doi: 10.1109/INCET49848.2020.9154024..

[12]S. Kumari and S. Farheen, "Blockchain based Data Security for Financial Transaction System," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 2020, pp. 829-833, doi: 10.1109/ICICCS48265.2020.9121108.