IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN BASED PAYMENT SYSTEM

[1]Deepak Kumar Baria, [2]Nitturi Vedavyas, [3]Thumalapalli Vineetha, [4]Parupalli Lasya Sara Dhruva

Bachelor of Engineering(computer-science),
Parul Institute of Engineering and Technology, Vadodara, Gujarat

Abstract: Blockchain payment systems are used to facilitate, process, and verify financial transactions made on a blockchain or distributed ledger system. These tools can be designed for businesses or financial institutions and may have different features depending on their intended use. Blockchain payment solutions enable customers to make transactions quickly and securely on a blockchain. A blockchain is a digital record of transactions that is stored and secured using cryptographic techniques. It is composed of a series of blocks, each of which contains a timestamp, transaction details, and the hash of the previous block. The use of hashes helps to link the blocks together and create a secure, immutable chain of records. By using a decentralized network of computers to validate and store the data, blockchain technology allows for the creation of a transparent and secure record of transactions that can be accessed and verified by all parties involved. The use of blockchain technology offers a secure alternative to traditional online payment systems.

Index Terms **– Blockchain, Ledger System, Transaction, Metamask wallet, Payment System.**

INTRODUCTION

A blockchain based payment system is a decentralized and secure way to facilitate financial transactions using peer-to-peer technology. One such system is MetaMask, a web3.0 browser extension that allows users to interact with the Ethereum blockchain using the Ganache blockchain. With MetaMask, users can make payments, create and manage smart contracts, and store their cryptocurrency assets all in one place. In order to develop and deploy applications on the Ethereum blockchain, developers can use tools like Truffle and React, which provide a comprehensive framework for building decentralized applications. By using these tools in conjunction with MetaMask and the Ethereum blockchain, developers can create a seamless and efficient payment system that offers unparalleled security and transparency.

As the blockchain technology is growing so faster now we are going in the new era Web 3.0. In future so many things, be work blockchain technology, this new era of internet motivated for this project blockchain based payment system for payments we do P2P transaction. We will be using blockchain Technology for implementing our project we will also use nodes, Smart contracts, proof of work algorithm, java script and its libraries such as react library etc. this all tools, technologies we will use for project. In this project we will create our own digital currency wallet and how the p2p transaction will done. Nowadays all the online payments are done by any third-party application or software.

All third-party companies collect our data and store it. If any bugs or hackers may hack and our data will steal, then it will not be safe for us. Here comes Blockchain technology which is more secure than centralized system because it decentralized system and it connects pair to pair networks and data will be store every node of the system. If any hacker wants to hack it, he must hack every node and its more difficult and more time taken so it more secures no third parties can view our data or change the data.

2.LITERATURE REVIEW:

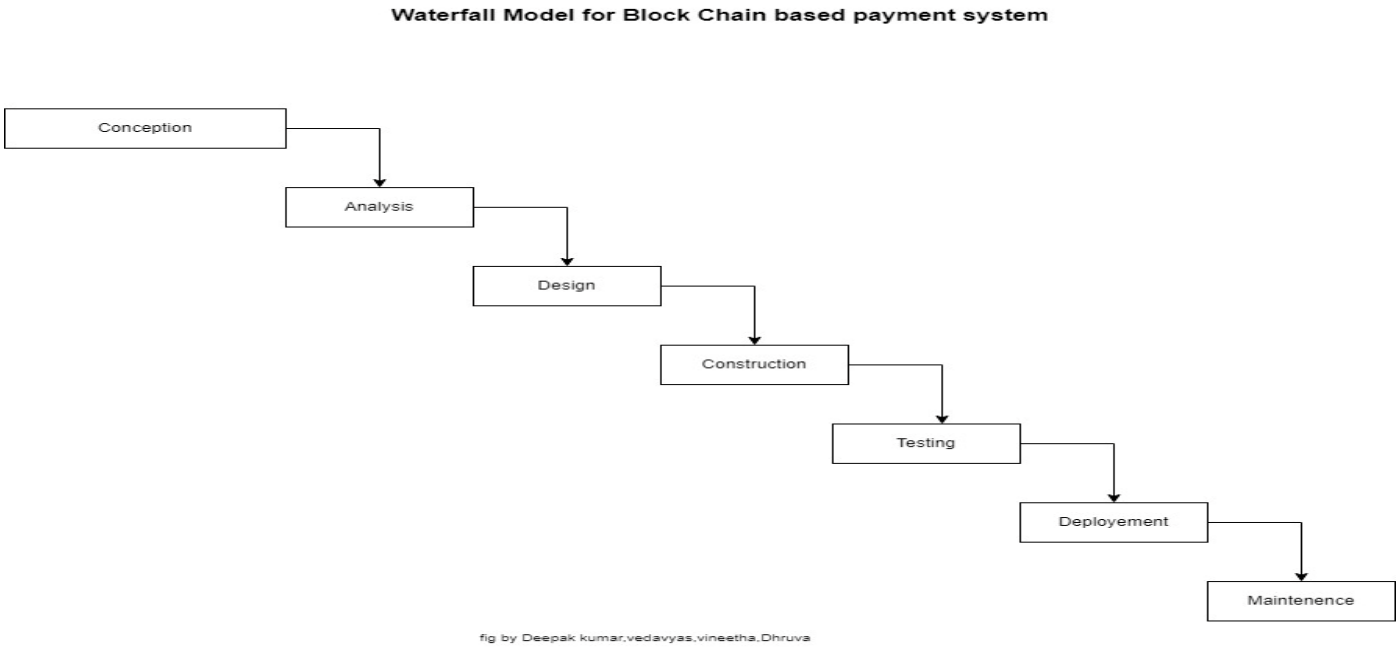
Blockchain technology is the perfect technology in payment systems block chain offers hastily, low- cost, secured payment services along with a distributed census that can give trust among the actors. Blockchain technology offers several advantages for the payment sector. First, it can provide a more secure platform for trade processes. The use of cryptographic hash functions in blockchain can prevent outside and inside attacks and ensure the integrity of data. Transparency is another benefit of blockchain, as it allows for the tracking of transactions and promotes accountability. Additionally, blockchain can streamline payment processing and reduce costs by eliminating the need for intermediaries. These factors make blockchain a promising technology for the payment industry.

- Digital identity verification
- High data security
- More anti plutocrat laundering (AML) protocols
- Automated know your client (KYC) processes
- Peer to peer (p2p) Transfer

Among those programs, decentralized charge structures (e.g., Bitcoin) had been one of the maximum mature blockchain programs with huge adoption. To support the privateness safety of decentralized charge structures, some of answers consisting of Monero and Zero cash had been proposed. However, absolutely Decentralized Anonymous Payment (DAP) structures may be criminally exploited, as an example in on-line extortion and cash laundering activities. Recognizing the significance of regulation, we gift a singular definition of Decentralized Conditional Anonymous Payment (DCAP) and describe the corresponding safety requirements. To assemble a concrete DCAP system, we first layout a Condition Anonymous Payment (CAP) scheme (primarily based totally on our proposed signature of knowledge), whose safety may be verified beneath neath the described formal semantic and safety models. To reveal utility, we evaluate the overall performance of our idea with that of Zero cash beneath neath the identical parameters and trying out environment.

3)RESEARCH METHODOLOGY

Waterfall methodology is used for this project



Conception: This is the first stage of the project, where the idea for the blockchain-based payment system is developed and the project objectives are defined.
Initiation: In this stage, a project team is assembled, a project charter is developed, and a project plan is created.
Analysis: The analysis stage involves gathering and documenting the requirements for the payment system, as well as identifying any risks that may impact the project. This may include researching and selecting the appropriate blockchain platform, determining the payment methods to be supported, and designing the user experience.
Design: In this stage, the design for the payment system is developed, including details such as the architecture, user interface, and any necessary algorithms. This may involve creating wireframes and mockups, as well as selecting any necessary third-party integrations.
Construction: During the construction stage, the payment system is actually built according to the design specifications. This may involve writing code, setting up infrastructure, and testing the system.
Testing: In this stage, the payment system is tested to ensure that it meets the defined requirements and to identify and fix any issues. This may include testing the security of the system, as well as conducting user acceptance testing.
Deployment: Once the payment system has been tested and any necessary changes have been made, it is ready to be deployed to its intended audience. This may involve setting up any necessary infrastructure, such as servers and databases, and performing any necessary data migration.
Maintenance: The maintenance stage involves ongoing support and updates to the payment system as needed. This may include adding new features, fixing any issues that arise, and ensuring the security of the system.

3.1 Block Chain Technology:

Blockchain technology creates a secure and transparent environment for transactions by using blocks to store data, hashes, and previous hashes. Each block in the blockchain contains a hash code of the previous block, which helps to keep the records safe and secure. A mathematical hash function is used to generate the hash code for each block. If a user wants to change the data in a block, a new block must be created, which helps to maintain the integrity of the blockchain. This system of linking blocks through hashes helps to ensure the security and transparency of transactions in a blockchain.
Data: In a blockchain, blocks can store transaction data. The specific type of transaction data stored in a block depends on the intended use of the blockchain. For example, financial institutions such as banks may store financial transaction data in blocks on their

blockchain. The purpose of storing this data in blocks is to create a secure and transparent record of transactions that can be accessed and verified by all parties involved. By storing transaction data in blocks, blockchain technology helps to ensure the integrity and security of financial and other types of transactions.

Timestamp: Blocks in a blockchain also contain a timestamp, which refers to the exact time and date of a specific transaction. The timestamp helps to track the order of transactions and provide a record of when they occurred. By including a timestamp in each block, blockchain technology helps to ensure the integrity and accuracy of the transaction data. This can be useful for verifying the authenticity of transactions and ensuring that they are properly recorded and tracked. Timestamps also help to provide a clear record of the history of transactions on the blockchain.

Hash: In a blockchain, a hash is a unique identifier that is generated using a cryptographic hash algorithm such as SHA-256. Each block in the blockchain contains the hash of the previous block, which helps to link the blocks together and create a secure chain. The use of hashes makes the blocks immutable, meaning that they cannot be altered once they are added to the blockchain. If a user tries to change the data in a block, it will create a new hash for that block and break the link to the previous blocks. This helps to maintain the integrity and security of the blockchain. There are three types of blockchain: private, public, and hybrid. The distributed ledger technology used in blockchain has been applied to payment systems, enabling the creation of a new mode for payments using regulated cryptocurrency. Blockchain-based payment systems offer fast, secure, and transparent services through encrypted distributed ledgers that provide user and admin verification. By using concepts such as smart contracts, trust, and privacy, it is possible to create a payment system using blockchain technology for enterprise purposes. This system can also involve the creation of a new cryptocurrency specifically for the payment portal, enabling users to buy and sell it.

Smart Contracts: Smart contracts square measure computer programs that may automatically execute the terms of a contract. once a pre-configured condition in a very smart contract among participating entities is met then the parties involved in a very written agreement is automatically create payments as per the contract in a transparent manner. nearly every business in today's digital economy is facing one sort of disruption the other because of the emergence of blockchain technology. Blockchain technology has the potential to become the new engine of growth within the digital economy wherever we have a tendency to square measure more and more increasingly the Internet to conduct digital commerce and share our personal data and life event Smart contracts enable the exchange of payments, property, shares, or any other valuable assets in a transparent and conflict-free manner, without the need for intermediaries. By using smart contracts, parties can conduct transactions in a secure and efficient way, avoiding the need for a middleman to facilitate the exchange. This can reduce costs and improve the speed of transactions, making them more efficient and convenient for all parties involved. Smart contracts can be used in a variety of industries and can help to increase the transparency and security of transactions.

Ganache: Ganache is a service which provides duplicate Ethereum account which works using Block Chain Technology, so that we can deploy our smart contracts for promising transactions. Basically, Ganache is a personal block chain system which supports both Ethereum and corda technology.

It comes in two varieties Ganache UI and Ganache CLI. Ganache UI is a desktop application for Ethereum development. It provides fake Ethereum to test the project and make the transactions. Ganache also stores the transactions and maintain a ledger for all transactions including time stamp.

Truffle: Truffle is a tool that allows developers to compile, link, and deploy smart contracts, as well as manage the binaries associated with them. It also offers the ability to deploy transactions and payments through MetaMask for added security. In addition, Truffle provides advanced debugging features such as breakpoints, variable analysis, and step functionality to help developers create and test their smart contracts. By using Truffle, developers can streamline the process of developing and deploying smart contracts, saving time and resources.

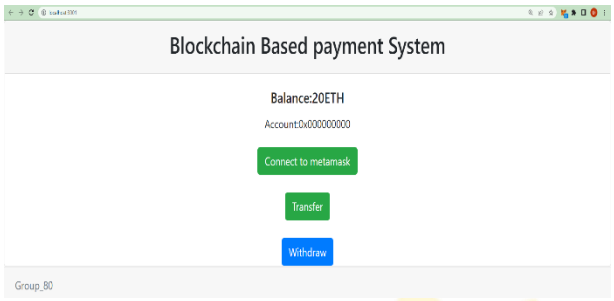
Meta Mask: MetaMask is a cryptographic wallet that enables users to interact with the Ethereum blockchain through a browser extension. It allows users to store and manage their account keys, broadcast transactions, send and receive Ethereum-based cryptocurrencies and tokens, and securely connect to decentralized apps (DApps). Websites or other DApps can use JavaScript code to connect to and interact with a user's MetaMask wallet by prompting the user for actions, signature requests, or transaction requests through the wallet as an intermediary. MetaMask is a convenient and secure way for users to manage their Ethereum wallet and interact with the blockchain.

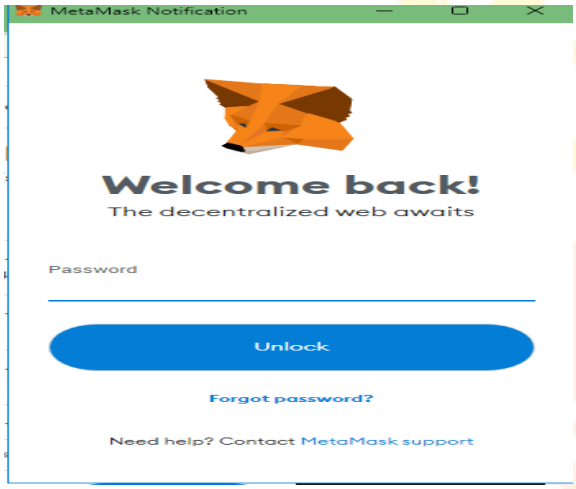
React JS: React JS is used in this project to develop Front-End of the project. The react JS framework is usually used to build interfaces and applications quickly and efficiently with less code comparatively. We used node JS in react JS for using some packages required for front end development. In this, one can develop applications by creating reusable components like Lego bricks. React encourages developers to separate complex UIs into individual reusable components that form as building bricks of the whole UI.

IV. RESULTS AND DISCUSSION

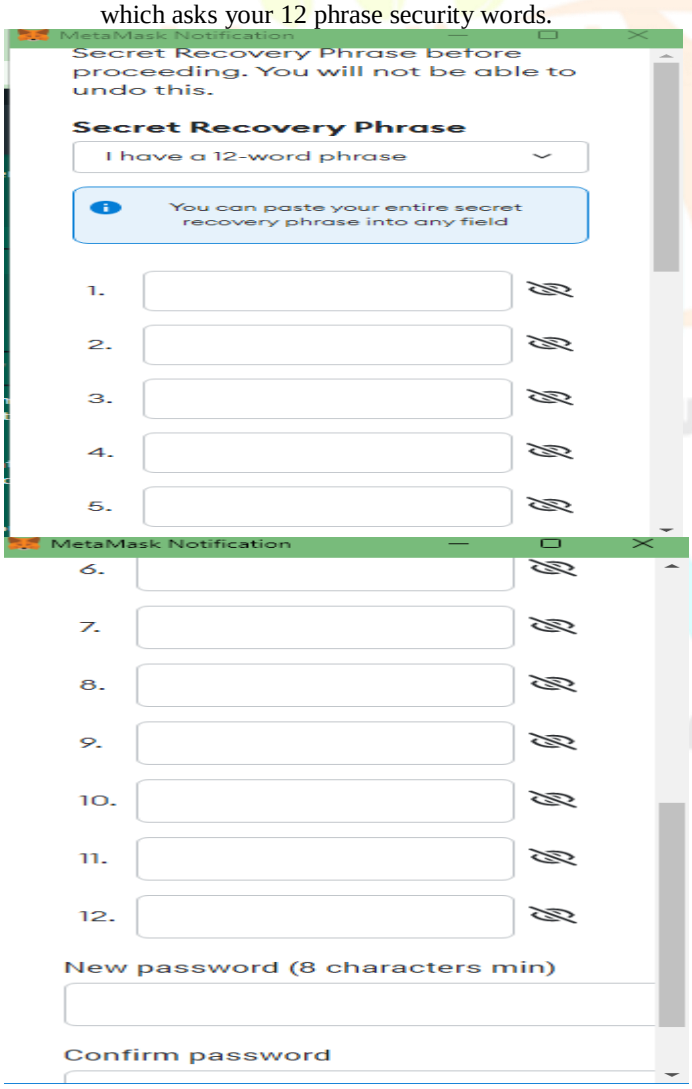
4.1 Discussions and Results:

- As part of discussions, we have gathered all the information regarding Block Chain from various sources of internet and some books which mentioned in references. We identified the process and made a UML diagram to follow. In this process we identified various services and used them accordingly. All the services used are mentioned in research methodology. In order to connect with Meta Mask using react we installed WEB3.0 dependencies. 'windows.ethereum.request' code line connects react application with Meta Mask application. Meta Mask is a wallet which is used to interact with the Ethereum Wallet. We identified Meta Mask as a service can provide us Ethereum Wallet through a browser extension which we can use for a block chain payment system.

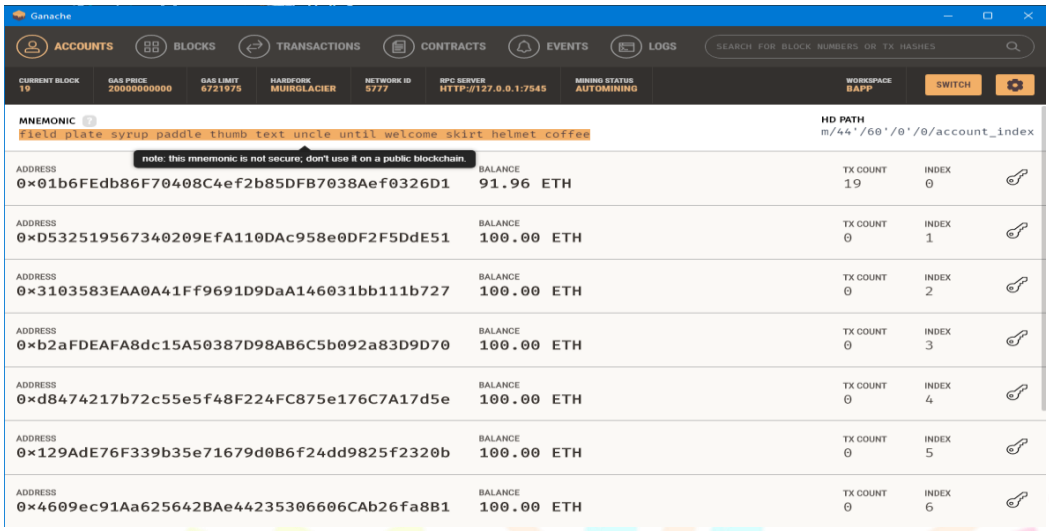




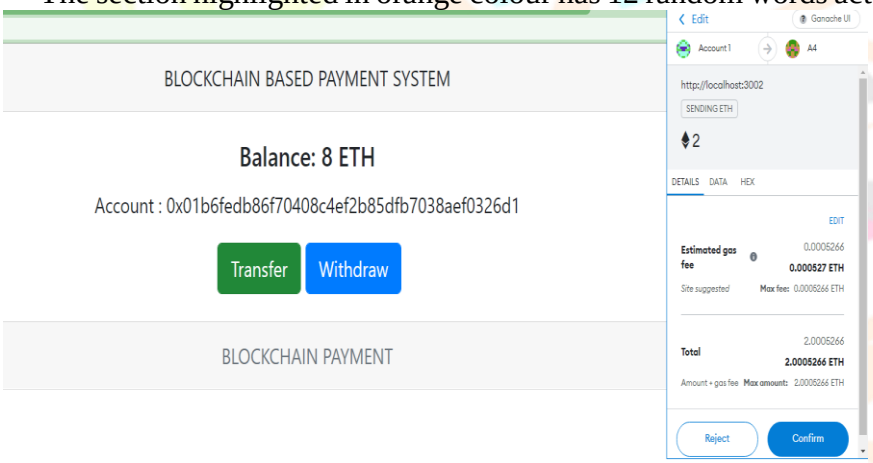
- To access our Ganache Block Chain accounts, we have to click on forgot password button and it redirects to the page which asks your 12 phrase security words.



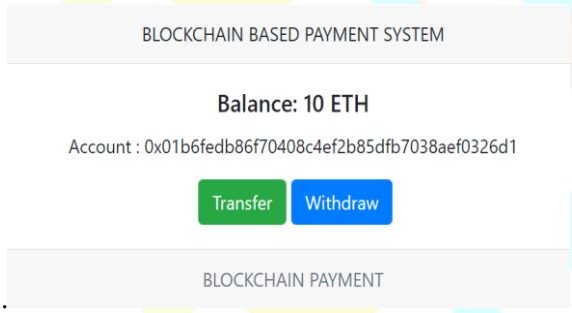
- From Ganache we can import the 12 phrase security words and fill them accordingly in the blanks observed in the image above. After verifying the 12-phrase security code one can create their password immediately.



- The section highlighted in orange colour has 12 random words acts as security phrase discussed above.



- After setting up the password the account is now open. Interface is shown in the Image above. The page shows the balance, account address and two buttons (transfer, withdraw).
- The button ‘transfer’ is used for transferring the Ethereum from Ganache to meta mask account so that no third party is involved and the transaction takes place securely.



.

5.Conclusion:

In this report, blockchain based payment system has been proposed, we have designed a secure transaction system with help of ganache blockchain, smart contracts, meta mask, and with truffle. Blockchain security protocols deals with gas-based payment in meta mask wallet. In addition, the implementation for transactions we used meta mask blockchain wallet and ganache for user accounts and transaction from one account to another account. Truffle is used to connect entire accounts of ganache with meta mask wallet and deals with the real time transactions for project. With help of Smart contracts we made minimum ether transactions in accounts at a time to deal with threshold transactions in blockchain. In this report, we also added literature review abstract from journals and their authors details and also, we discussed about the scope of the project how it helps in future and where the project will impact more and also discussed about what its aim and objectives of the project. In methodology we discussed how a project will start and which front end technologies will be used and how we choose blockchain platform for executing our transactions in the project. We also shown the partial implementation of the project or experimental setup for project.

6.References:

[1] Mattila, J.: 'The Blockchain Phenomenon', in Editor (Eds.): 'Book the Blockchain Phenomenon' (Berkeley Roundtable of the International Economy, 2016, edn.)

[2] Beck, R., Stenum Czepluch, J., Lollike, N., and Malone, S.: 'Blockchain – the Gateway to Trust-Free Cryptographic Transactions'. Proc. Twenty-Fourth European Conference on Information Systems (ECIS), Istanbul, Turkey2016 pp. Pages

[3] Teigland, R., Yetis, Z., and Larsson, T.O.: 'Breaking out of the bank in Europe-exploring collective emergent institutional entrepreneurship through bitcoin', Available at SSRN 2263707, 2013

[4] Ingram, C., and Morisse, M.: 'Almost an MNC: Bitcoin Entrepreneurs' Use of Collective Resources and Decoupling to Build Legitimacy', in Editor (Eds.): 'Book Almost an MNC: Bitcoin Entrepreneurs' Use of Collective Resources and Decoupling to Build Legitimacy' (IEEE, 2016, edn.), pp. 4083-4092

[5] Bollen, R.: 'The legal status of online currencies: are bitcoins the future?', Journal of Banking and Finance Law and Practice, 2013

[6] Van Alstyne, M.: 'Why Bitcoin has value', Communications of the ACM, 2014, 57, (5), pp. 30-32

[7] Giaglis, G.M., and Kypriotaki, K.N.: 'Towards an Agenda for Information Systems Research on Digital Currencies and Bitcoin', in Editor (Ed.) ^(Eds.): 'Book Towards an Agenda for Information Systems Research on Digital Currencies and Bitcoin' (Springer, 2014, edn.), pp. 3- 13

[8] Dahlberg, T., Mallat, N., Ondrus, J., and Zmijewska, A.: 'Past, present and future of mobile payments research: A literature review', Electronic Commerce Research and Applications, 2008, 7, (2), pp. 165-181

[9] Staykova, K.S., and Damsgaard, J.: 'The race to dominate the mobile payments platform: Entry and expansion strategies', Electronic Commerce Research and Applications, 2015, 14, (5), pp. 319-330

[10] Nakamoto, S.: 'Bitcoin: A peer-to-peer electronic cash system', in Editor (Ed.) ^(Eds.): 'Book Bitcoin: A peer-topeer electronic cash system' (2008, edn.).