Novel Payment Wallet Management with Blockchain Based Cryptocurrency

P.Selvaraj, S. Prabakaran, V. Krishnateja

Abstract*: Blockchain for business is a new concept which enables many industries and organizations to implement even the basic of systems on foundation of blockchain technology. Using this technology, our goal is to develop a payments system that enables transfer of funds for a monetary transaction between two parties. Hyperledger is an open source community oriented effort which was made to propel cross-industry blockchain advances that were available. The Linux Foundation has it. It has partners from everywhere throughout the world , at a worldwide dimension and incorporates ventures like funding, banking, Internet of Things, supply chains, assembling and Technology. Using Blockchain for Enterprise technology, we are going to develop a new payments system that makes use of regulated cryptocurrency. Using this system, we want to create a new cryptocurrency specific to the payment portal for people to buy, sell and pay or earn rewards using this cryptocurrency.

This system will majorly consist of participants and admins that will be divided based on the certificates assigned to every participant. Our implementation involves. using the fabric for creating a payment system run on the backend of blockchain technology. This will involve having a regulatory authority to maintain the cryptocurrency, ledger and authenticity of the users. Theoretically, the blockchain technology maintains anonymity for transactions. It uses a distributed ledger to record transactions for people to be able to make secure transactions without any repercussions. Blockchain for Enterprise implements Blockchain technology by using concepts like Trust, Privacy and Smart contracts in addition to the distributed ledger to create an industry friendly Blockchain business application. Blockchain is a rapidly growing field with multiple implementations which can be explored not just on anonymity but also on actual life implementations. Distributed ledger technology is applied to the payment systems. Cryptocurrency would now not only be used for anonymous transactions but also for regular day to day transactions.

***Index Terms*: Blockchain, Cryptocurrency, Etherium wallet, Hyperledger Fabric**

I. INTRODUCTION

Blockchain is an digital ledger record of financial exchanges that can be adjusted to record budgetary trades just as fundamentally everything that has value. The blockchain is a creating list of records which are called blocks. These blocks are associated using diverse cryptography frameworks. Each block contains a cryptographic hash of the past block, a timestamp, and exchange (transaction) data.

Revised Manuscript Received on July 05, 2019.

P.Selvaraj, Department of IT, SRM IST, Kattankulathur, Chennai, India.
S.Prabakaran, Department of CSE, SRM IST, Kattankulathur, Chennai
V.Krishnateja, Department of IT, SRM IST, Kattankulathur, Chennai

The blockchain is impenetrable to modification of the data by any design. It is "an open, conveyed record that can store exchanges between two gatherings productively and in an irrefutable and perpetual way". Blockchain is overseen by shared system which is governed by a fixed protocol. The data which is recorded in a block cannot be altered retroactively. Though the blockchain records can not be altered, yet blockchain is considered to be secure by design.

Hyperledger Fabric is a blockchain system implementation. It is one of the Hyperledger ventures that were encouraged by The Linux Foundation. It was proposed as a foundation for making applications and arrangements with secluded engineering. The Hyperledger fabric has features, for example, consensus, membership services which can be utilized as plug and-play. Container technology is utilized in Blockchain, it is utilized to have smart contracts called "chain codes". Chaincode fundamentally contains the application logic of the framework. Digital Asset and IBM at first contributed the Hyperledger Fabric, because of the first hackathon.

Using the Hyperledger Composer Fabric, blockchain can now be implemented on almost all business applications by creating a basic model for the applications using concepts like smart contracts, trust and distributed ledger. Using this technology, our usage includes using the fabric for creating a payment system run on the backend of blockchain technology. This will involve having a regulatory authority to maintain the cryptocurrency and database and authenticity of the users. Cryptocurrency is developed on three basic techniques: Confirmation of Work (POW), Proof of Stake and Proof of Elapsed time. Utilizing Ethereum we will make our very own digital currency utilizing verification of Work and afterward send that cryptographic money on to the decentralized system of the applications to be utilized for installments by the clients in a directed way.

II. LITERATURE REVIEW

Sarah Underwood [7] proposed an architecture for the blockchain technology and claimed that it has the potential to revolutionize the business transactions and online payment based applications. They also claimed that it has the potential to redefine the digital economy. It can be useful to individuals in creating nations with perceived character, resource proprietorship for individuals, and budgetary incorporation; and it could turn away financial crisis for countries, it can support effective healthcare programs which can be run efficiently, improve supply chains and their process and help to avoid exploitative conduct in high-value

businesses for example, diamond trading.

Blockchain can solve long standing problems that exist. Blockchain is now regarded as an existing solution and not an existing technology. Mahdi H. Miraz et al., proposed about the blockchain security by storing/maintaining a digital ledger of the transactions which are recorded. They claimed that these transactions cannot be recorded. Blockchain uses the concept of public key to record the identity of the users which acts as an extra layer of privacy. Blockchain has been effectively implemented in diverse non-money related frameworks, for example, in decentralized messaging, online voting, stockpiling frameworks, verification of-area and medicinal services. The study on blockchain must be done to guarantee improved security and to recognize its related challenges that are associated with this technology.

Buterin et al.,[9] proposed about the public blockchains that allowed the members to make these transactions in a secured way in trust-less environments. Important aspects, like data reversibility control, data privacy, transactions volume scalability, framework responsiveness and simplicity of protocol updates are essential for the a large portion of the corporate uses are not secured by open blockchain executions. Every one of these weaknesses have prompted the improvement alternate blockchain technologies to explain the above expressed details and are expected for confined gathering of people. Such new advances are grouped into two classifications private and consortium blockchains. The fundamental distinctive factor is their administration plot. In private chains, one member oversees or approves the entire framework though in the other, the people of consortium blockchains share the authority among themselves. New terms and ideas are creating to classify the methodologies among private and open blockchains, for example, semi-private or undertaking advances. Be that as it may, the significant contrasts are concerned for the most part with the application level rather than the building level.

Pilkington and Marc demonstrated a blockchain Technology [10]and the digital cash had been conceptualized with the assistance of a central server trusted to avoid twofold spending. In spite of major cryptographic advances, there were numerous disappointments like guaranteeing similarity between centralization, namelessness, and twofold spending anticipation. The Blockchain innovation ensures the transfer of the twofold spend issue, with the help of the possibility of public key cryptography. In this kind of encryption every operator is doled out with a private key and an public key conferred to each and every different specialists. Standards and Applications of this innovation is started when the future proprietor of the coins sends over his/her open key to the first proprietor. Hash helps in the exchange of the coins utilizing digital signature. Public keys are cryptographically created addresses which are put away in the blockchain. Each coin has a unique address, and a transaction in the crypto-economy is extremely basic, it is an exchange of coins from one location to another. Public keys are never tied to a real-world entity is a striking element of Blockchain. Transactions which happened although they are detectable, they are empowered without revealing one‘s identity, this is a major difference with transactions in fiat currencies except for money exchanges. Blockchain is a fundamental innovation, yet we uncover the potential dangers and downsides thatrepresent for the shift toward hybrid solutions.

K. Christidis and M. Devetsikiotis[11] demonstrated about the smart contracts which have become more popular in use for blockchains to digitization and automation of the execution of business workflow (i.e., contracts will be self-executing), and for those whose proper execution happens through the consensus mechanism.Zheng, Z et al., [12]explained about the Blockchain challenges and opportunities and they proposed a consensus strategy used in networks as a complicated computational process for authentication purposes.

III. EXISTING SYSTEM

There are lots of payment apps/gateways these days. A typical payment application which is developed consists of the following two modules.

A. Interfaces are used to bridge/connect to the outside world.

B. The flow for the processing of payment transaction is driven by the processing modules.

Several implemented interfaces are present in a single payment application.The interfaces can be of any kind relying upon the required no of upheld peripherals, POS models and approval systems. Two main functions are supported by the processor link:

A. Transaction parameters are converted to a specific format based on the payment processor message protocol.

B. The communication with the authorization host is done using a communication protocol supported by the payment processor.

A particular processor can communicate with a specific processor link as every interface is hard coded to speak with a particular processor however the area of the processor's server is typically delicate coded (designed). For instance, a host setup may contain the IP address and server port for TCP/IP-put together correspondence conventions with respect to private systems, or the URL for HTTP-based conventions over the Internet.

Another group of payment application blocks consists of modules dependent on flow processing that drive the payment process. It takes care from the moment of swiping the card to getting the dealer paid and the cardholder's account charged. The primary processing modules includes the following:

1. Router
2. S&F (Store and Forward)
3. TOR (Timeout Reversal)
4. Batch

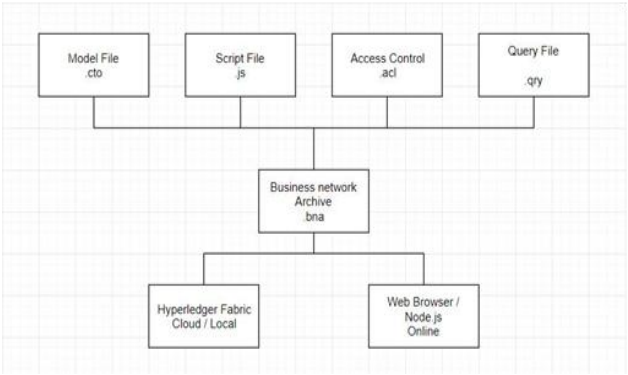

Figure 1. Architecture of the proposed system.

IV. PROPOSED SYSTEM

Blockchain is a very vast field already being implemented in the world with a rapid pace. Bitcoin is the most famous example of decentralized blockchain technology, which used Proof of Work as the basis in the genesis block. It maintains anonymity and people used it for anonymous transaction. Confirmation of work (PoW) is an consensus methodology utilized in systems. POW utilizes a convoluted computational procedure for verification purposes. In the POW, every one of the hub that is available in the system figures a hash value of the block header that changes always.

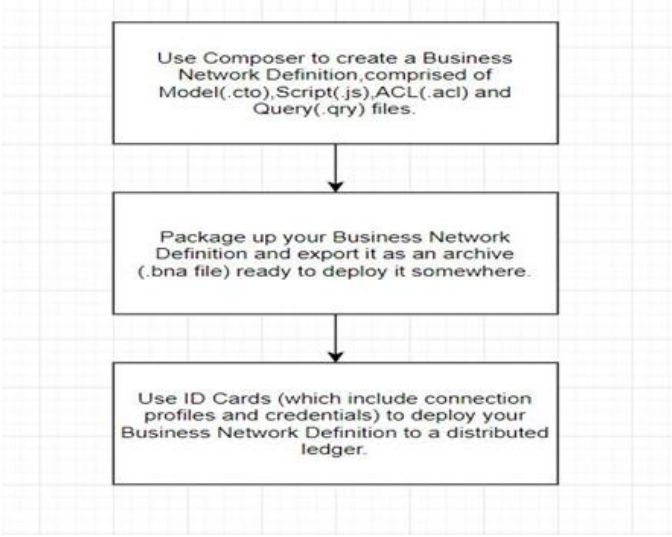

Figure 2: Block Diagram of the process.

As per the consensus methodology, the decided value ought to be equivalent or smaller than a particular given value. In the decentralized system, all individuals need to register the hash value incessantly by using different nuances until the goal is cultivated. When one hub achieves the specific value, each and every other hub ought to normally assert the right value.

At the point when that is done, the trades in the new block would be affirmed against frauds. Afterward, the accumulation of exchanges that was used for the computations gets affirmed to be the affirmed result, which is meant by another block in the blockchain. These hubs that figure the hashes are called miners and the Proof of Work framework is called mining. This essential standard of this innovation was exploited and was developed into an enterprise friendly blockchain system, which could be used by any organization. This has been implemented using the Hyperledger Fabric, which forms the basis for making business network applications using blockchain.

Our major aim is to develop a system that moves away from the conventional foundations of payments systems to a system that is made on the foundation of blockchain technologies. Developing a new payments system using cryptocurrency and blockchain concepts. Adding a regulatory authority to maintain the cryptocurrency and to facilitate users to make payments using the cryptocurrency whereby using the blockchain technology as base.

Thus Blockchain technology facilitates a lot of low cost payment processing services. Blockchain is fast ,secure and transparent. It uses encrypted ledgers which provide real-time verification of transactions using smart contracts, certificates etc.

V.METHODOLOGY

The methodology to be used in the project is feature driven development. In this project, the entire planning and project development is based on the features of the system. Every step is done to achieve a single feature and on completion, the focus is shifted to the next feature to be modelled. Using Hyperledger composer we will deploy a new business network in which firstly we describe about the name of the business, type etc.

After successful deployment and connection will add/create new participants with all the basic details like email, name etc., then will add assets to the registry. Building a business network application and developing the REST API which will form the basis of the application and the web service. Implementing the REST API in Android Studio for app development and Web services which are used as interface. Creating a viable decentralized network using the applications, in which cryptocurrency is created and deployed on the network.

The distributed ledger technology was applied to the payment systems. Implementing a new mode for payments using regulated cryptocurrency. Cryptocurrency would now not only be used for anonymous transactions but also for regular day to day transactions. Using this system, we will create a new cryptocurrency specific payment portal for people to buy, sell and pay or earn rewards using this cryptocurrency. As Blockchain facilitates fast, secure, transparent services through encrypted distributed ledgers that provide verification so finally we will add certificates and authentication for users and admin.

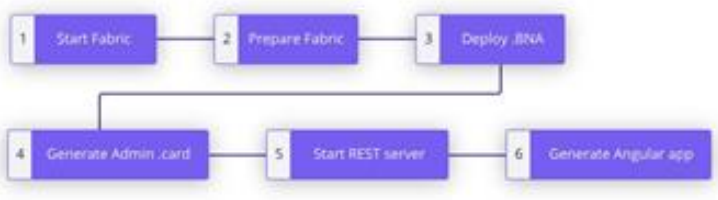

Figure 3. System Design.

Using concepts like smart contracts, trust, privacy etc., we are eliminating the anonymity that is essential to the traditional blockchain paradigm. We are changing the underlying technology to a distributed ledger technology and implementing blockchain concepts to facilitate a new payments system that will no only contain monetary transactions but will replace the essential day to day payments systems currently being used for making payments. We will create a new cryptocurrency which will replace the traditional currency usagebased on regions to a universally accepted currency worldwide.

To make a payments system using Blockchain for Enterprise technology as the basis and implementing a new mode for payments using regulated cryptocurrency. Using this system, we want to create a new cryptocurrency specific to the payment portal for people to buy, sell and pay or earn rewards using this cryptocurrency. Hence the Blockchain is a rapidly growing field with multiple implementations which can be explored not just on anonymity but also on actual life implementations. Distributed ledger technology is applied to the payment systems. Cryptocurrency would now not only be used for anonymous transactions but also for regular day to day transactions.

VI. IMPLEMENTATION

Our major aim is to develop a system that moves away from the conventional foundations of payments systems to a system that is made on the foundation of blockchain technologies.

There is a need for a regulatory authority to maintain the cryptocurrency and to facilitate users to make payments using the cryptocurrency.

I. Model File:

It consists of class definition for assets, users and transactions (processes) that are present in the business network.

II. Script File:

A script document or logic.js file contains functions which are used for transactions processing, and a package.json file which contains important business network related metadata.

III. Access control:

The access control permissions.acl document basically consists of access control rules which are used for controlling the network. The steps for creating a business network are given below.

Step 1: Creating the business structure.

The Hyperledger composer works on one basic key concept of Business Network Definition(BND).It defines the data model in which definitions of all required variables are explained in detail, the logic document for processing and access document has rules for the blockchain solution are defined.

We have to make an appropriate project structure on disk to create a BND.

1. Use a Yeoman skeleton business network create a Business Network Definition.
2. The command which is used is yohyperledger-composer:businessnetwork.
3. The above command requires a very much characterized details like name for the business-network, detailed info, creator name, email address and so forth.
4. To view the details use tutorial-network command it shows the details of the network like name, detailed info about the network such as creator name, email address.
5. Then follow the flow of selecting desired license, namespace etc.

Step 2: Creation of the Business Network.

A business network is comprised of users, transactions, assets, control rules, and optional procedures and various queries.

There are three file types:

1. First is a model file (.cto): It contains the class details for all valuables(assets), users, and process of exchange of currency(transactions) present in the business network.
2. Then permission document basically consists of rules for controlling the network or for accessing the network, a logic document contains the logic about how the exchange of assets taking place in the network, and a package.json file contains important business network related information.
3. Designing assets, users, and exchange of assets(etc)/transactions.
4. The first one that has to be changed is the model file which has definitions of the structure. The language used to script the file is Hyperledger Composer Modelling Language.
5. The contents have to be defined with the required class of asset, transaction, participant, and event.
6. Changes should be saved to org main(filename).network.cto.
7. Using JavaScript language logic file is defined.
8. In the model file, a exchange processing transaction should be defined which specifies the relationship between the asset and the user for exchange of currency. Exchange processing function file consists of the logic code to execute the transactions which are defined in the model file.

i. The logic.js script file has to be opened.

ii. The contents with the required logic for your network have to be replaced.

iii. The changes to logic file should be saved.

iv. In permission.acldocument new access control rules has to be defined according to the requirement of the network.

v.Your changes to permission document has to be saved.

Step 3: A business network archive has to be generated. Once when the network has been declared, it must be bundled into a deployable into a bna file.

1. Command line should be used to navigate to the tutorial-network directory.
2. From the directory, one has to run the following command: Composer archive create –t dir –n.

After the command has been successfully executed, a business network archive file called your-directory@0.0.1.bna will be created in the directory.

Step 4: Business network has to be deployed.

The .bna file is created, the business network can then be deployed to the instance of Hyperledger Fabric. The network can be started after the business network has been installed..

A Peer Admin business network card with the correct credentials is already created as part of development environment installation.

Step 5: Activating the business network:

When Business network is deployed to the Hyperledger Fabric it requires the Hyperledger Composer.

The networkhas to be introduced on the peer,after that only thenetwork willbegun.

The user, associated, and identification card to be made for network admin. In the end ,the network admin card is used. Then only the network can be pinged to check for response.

The following command should be used to install the business network from the directory:

1. This command is for installing the peer admin card in the network :Composer network install –card peername for the network –archivefileyour-directory@someversion.bna
2. The business network has to be started by running the following code command:

Composer network start –networkNamedirectoryname –(networkVersion) – networkadminadminname –networkAdminEnrollSecretadminpw –card cardname of the admin –file name.card

3. Run the following

Command to use the network admin identity as a business network card, Composer network ping –card admin@directoryname.

4. To verify whether if the network is successfully working, run the following command to call the network:

Composer network ping –card admin@filename

Step 6: Creating a REST API server

Hyperledger Composer can generate a REST API based on a business network .REST API provides a useful layer of language-neutral abstraction.

1. Navigate to the directory and run the following command to create a REST API:

Composer-rest-server

2. Then the process of selecting namespaces, security etc. for the API has to be followed.The generated API is connected to the deployed blockchainandabusiness network.

Step 7: Creating anAngular application using vscode

The Hyperledger Composer can also be generate an Angular 4 application running against the REST API.

1. Navigate to tutorial-network directory to create your Angular 4 application, and run the following command: yohyperledger-composer:angular
2. When asked to connect to running business network select YES.
3. Standard package json file questions (project name, description, author name, author email, license)should be entered.
4. admin@directory name for the business network card should be entered.
5. Connect to an existing REST API should be selected.
6. Enter http://localhost for the REST server address.
7. Enter 3000 for server port.
8. Select Namespaces are not used:

The Angular generator will then create the requirements regarding the project. Move to the project folder then run npm start to start the application. This will launch an Angular vs code application running against the REST API at http://localhost:4200.

VII. CONCLUSION

Hence a hyperleder based enterprise architecture is proposed. The blockchain based payment wallet management exhibited the anonymity of transactions while maintaining the authenticity of the user with the distributed ledger management system. The privacy and smart contract based distributed ledger management system is proposed. The proposed approach is deployed in a hyperledger based payment portal and the steps followed in the deployment are discussed. The business network was developed with the REST APIs and the angular JS based application. The results has shown the improved and effective payment management with the blockchain based crypotocurrency management.

REFERENCES

1. Hyperledger Composer - Create business networks https://hyperledger.github.io/composer
2. Creating Cryptocurrency - https://medium.com/coinmonks/create-your-own-cryptocurrency-in-ethereum-blockchain-40865db8a29f
3. Confidential Transactions by Gregory Maxwell - https://people.xiph.org/~greg/confidential_values.txt
4. Digital Currencies by Bank of International Settlements, Committee on Payments and Market Infrastructures - https://www.bis.org/cpmi/publ/d174.pdf
5. What is blockchain? How is it going to affect Business? By Luc Severeijns supervised by Prof.Dr. SandjaiBhulaihttps://beta.vu.nl/nl/Images/werkstuk-severeijns_tcm235-869851.pdf
6. Blockchain for Enterprise:Overview, Opportunities and Challenges- Elyes Ben Hamida, Kei Leo Brousmiche, Hugo Levard and Eric Thea, Institutefor Technological Research SystemX, France - https://hal.archives-ouvertes.fr/hal-01591859/document
7. Sarah Underwood, "Blockchain Beyond Bitcoin," Communications of the ACM, vol. 59, no. 11, pp. 15 , Available: https://doi.org/10.1145/2994581.
8. Mahdi H. Miraz and Maaruf Ali, "Blockchain Enabled Enhanced IoT Ecosystem Security,"proceeded in First International Conference on Emerging Technologies in Computing 2018 (iCETiC '18), London.
9. Pilkington, Marc, Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations, edited by F. Xavier Olleros and MajlindaZhegu. Edward Elgar, 2016. Available at SSRN: https://ssrn.com/abstract=2662660.
10. K.Christidis and M.Devetsikiotis, ―Blockchains and smart contracts for the internet of things, IEEE Access, vol. 4, 2016, pp. 2292–2303.
11. V. Buterin, ―On Public and Private Blockchains, 2015, Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.
12. Zheng, Z., Xie, S.,Dai, H-N., Chen, X. and Wang, H. (2018) _Blockchain challenges and opportunities: a survey‘,Int. J. Web and Grid Services, Vol. 14, No. 4, pp.352–375.

AUTHORS PROFILE

P.Selvaraj has been working as an Assistant Professor in SRMIST, Chennai for the past 13 years. He did M.Tech in IT from SRMIST, and currently pursuing research in software defined optical networks. He published 10 papers in reputed journals. His research interest includes artificial intelligence, machine learning, pattern recognition, intelligent networks etc.,

Dr. S. Prabakaran elvaraj has been working as Professor in SRMIST, Chennai for the past 12 years. He did M.E in CSE from Thapar university, Patiala and his Ph.D from IIIT, Gwalior. He published 75 papers in reputed journals. His research interest includes artificial intelligence, machine learning, pattern recognition, image processing etc.,

V Krishnateja completed B.Tech IT from SRMIST in 2019, Chennai. He has been constantly working in the Blockchain based projects.