ISSN No:-2456-2165

Stack DApp based Distributed Ledger for Decentralized Banking

Ankit Khandelwal[#1], Madhav Narayan Singh[#2]
[1]School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore, 632014, India
[2]School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore, 632014, India

Abstract:- Blockchain is one of the IT industry's fastest-growing technology niches. We chose to use blockchain technology to develop a web application for our project. We'll create a fully functional crypto-currency with full stack functionality and blockchain logic. We are proposing a new improvement in which we will not use any database server at the backend. Instead, we'll use Redis to create a publisher/subscriber network that will enable us to broadcast various messages and chain them across the network. Every node in the network will have a wallet, and they will make various transactions, which will then be added to the blockchain to block, and then broadcasted to the rest of the chain This eliminates the need for a database infrastructure to be created and maintained. We will create a mining algorithm (proof of work algorithm) for selecting blocks (collection of transactions) that will change its difficulty rate based on the computational power present in the node to node network, and for each block mined and successfully added to the chain will be rewarded with a reward in the form of our Cryptocurrency.

Keywords:- *Blockchain; Development; Cryptocurrency; Consensus; Proof Of Work (POW).*

I. INTRODUCTION

One of the big issues facing the IT industry is information security and fraud, and the introduction of Blockchain has given rise to “hack proof” systems. To hack a system that uses blockchain, the hacker must first hack more than half of all the systems that use the blockchain network, making hacking virtuallyimpossible. This will provide our website with a level of confidence and protection that no other genericwebsite can guarantee.

The lack of a centralised database is also a plus. Data storage is one of the most expensive components ofany IT architecture, but it can be greatly reduced by using a decentralised database. The REDIS has beenused by us.

Server that assists us in providing a publisher and subscriber that assists us in broadcasting the transaction as well as the newly modified chain through the nodal network. We have used a method to change the complexity based on the network's computing capacity. The transactions are checked by the miner network, and those miners have a local Transactional pool where they can get a group of transactions andcreate a block, which can then be added to the consensus chain and broadcasted as a newly modified chain, with the miner who found the block being rewarded.

II. RELATED WORKS

Cocco et al research .'s [3] This study examines the problems and opportunities of applying blockchain technology in the banking industry, providing food for thought on the disruptive technology's potential. Blockchain technology has the potential to improve the global financial infrastructure, allowing for more sustainable development and the use of more efficient methods than are currently available.

There is an actual performance of the Bitcoin system to understand the potential of blockchain technology to support the financial system, as well as highlighting its major limitations, such as the significant energy consumption due to the high computing power required, and the high cost of hardware.

In order to measure the efficiency of the Bitcoin system in its actual functioning, we established three quantities: "economic efficiency," "operational efficiency," and "efficient service," and we assessed the electrical power and hash rate of the Bitcoin network over time. The findings indicate that by solving the shortcomings of the Bitcoin system, and therefore of blockchain technology, we may be able to manage financial processes more efficiently than we can now.

Due to the influence of Bitcoin popularity and network power consumption, the EE, which is defined as theratio of the value of bitcoins mined to the power consumption of 1 kWh, is very volatile. Second, the OE iscurrently increasing, showing that fees are becoming increasingly important to the Bitcoin system's long- term viability. The OE is defined as the ratio of the value of voluntary fees to the energy cost of a transaction.Mining operations will be paid only until the total number of bitcoins in circulation hits 21 million.

Hassani et al research's [5] The most detailed evaluation of blockchain's impact on banking to date, summarising the opportunities and difficulties from the perspective of bankers. We also examine the potential influence of big data from blockchain on financial data analytics, as well as the growing relevance of filtering and signal extraction in the banking industry. While there is evidence of a few banks adopting blockchain technology in small groups or in isolation, there is a need for more research and development into several aspects of banking with blockchain to overcome the challenges that are currently preventing its adoption in banking around the world, as well as how the consensus is reached.

[6] discovers improvements to KYC measures, exchange velocities, and security, and cost decreases, brilliant agreements, straightforwardness and the possibility to expand the quantity of exchanges a bank can measure as the key chances. Conversely, we additionally discover arrangement and working expenses, normalization prerequisites, steadiness of the cash, security (which is strangely both a chance and challengein certain viewpoints), enactments and guidelines, and versatility to be the key difficulties looked by banksinvestigating embracing blockchain innovation in the cutting edge age. While the lion's share of these difficulties could be defeated through broad innovative work, the absence of scholastic exploration based interest in this branch of knowledge is of concern. It is normal that this audit can go about as a method for effectively distinguishing existing exploration holes for blockchain-ed large information in banking and accordingly rouse more scholastics, scientists and brokers to dive into this branch of knowledge and discover answers for the current difficulties while enhancing the current chances. As a feature of the conversation component, we additionally think about the significance of separating and sign extraction methods to the financial area in future. Utilizing genuine information for instance, we show how the financial area could profit by information and investigation into separating and sign extraction in huge amounts of information as it tries to embrace blockchain innovation and extend its tasks.

Coupling blockchain with the Internet of Things could give a vigorous, decentralized approach to deal with the quickly expanding number of organized gadgets. [7] states, empowering dynamic reconfiguration of blockchain boundaries could prompt a framework equipped for suffering evolving conditions. Survey blockchain plan as a cycle with adjustable viewpoints assists with examining what boundaries can be pickedto self-oversee in an independent framework. In this paper, we gave a less difficult point of view of blockchain plan components for a 173 IoT framework, specifically for the obtaining of sensor information.Despite the fact that we still can't seem to completely investigate a strategy for key dissemination for our framework, we have planned the structure we need to consolidate blockchain with IoT and the cloud. Zarrinet al's research [19] looks into Blockchain's ability to establish a stable and secure decentralised Internet model. A critical examination of recent Blockchain-based approaches capable of decentralising the Internetof the future. With regards to contemporary Internet and Blockchain issues, we identify and examine two research elements of Blockchain that have a high influence in implementing the decentralised Internet whilekeeping varied designs in mind. The first is the consensus algorithms, which are critical to the Blockchain's decentralisation. We highlight three important consensus algorithms, namely PoP, Paxos, and PoAH, as being better suitable for establishing consensus for such a large-scale Blockchain-enabled Internet architecture. The second area we looked into was Blockchain's compatibility with other new Internet technologies, as well as its impact on those technologies. Such new Internet technologies, when used in conjunction with Blockchain, could help to overcome Blockchain's known weaknesses, making it more streamlined, efficient, and appropriate for Internet decentralisation.

Blockchain applications have recently emerged that extend far beyond their original application domains invirtual currencies; for example, they are now crucial in industries such as domain registration, crowdfunding, prediction markets, and even gambling. Second-generation blockchain technologies enable not only the execution of basic transactions, but also the computation of data on a network, where payments,for example, are conditional on the state of some internal or external variables (much the same way as financial derivatives have a payout that is a function of an underlying financial instrument). This is the foundation for ‘smart contract' technologies, which will be crucial building blocks for these new applicationareas, as we will see. As a result of these second-generation technologies, third-party data ledgers (Devanbuet al. [4]), e-contracts/smart contracts and virtual contracts (Kosba et al. [9]), e-assets or remote asset title transfers , and other applications.

The launch of Bitcoin, a decentralised crypto-currency for the internet, is closely related to the creation of blockchain technology. Nakamoto [12] suggested how a group of users could conduct safe peer-to-peer financial transactions, bypassing financial middlemen and lowering the cost of international payments. However, in doing so, Nakamoto established a structure known as the blockchain, as well as a communication protocol, that essentially solved the Byzantine Generals' Problem and allowed the network to attain consensus without knowing the identities of users or trust relationships.

[1] discover to estimate the usability of blockchain technology by investigating behavioural elements that affect customers' intention towards blockchain-based cryptocurrency transactions. Given the complexity of the technology, this study proposes a new integration model: The Technology Acceptance Model (TAM) together with new external variables regarding blockchain adoption characteristics such as trust, regulatory support, social influence, design, and experience. Surveys were conducted among international users to identify the impacts of these variables on their intention. The findings indicate two powerful constructs (regulatory support and experience) that encourage customer's trust toward blockchain-based applications. The surveyed people agreed significantly feeling secure and they can trust the Blockchain-based applications when it is regulated and ensured by the local government. Also, at a certain level of experience, users feel trusted using blockchain-based applications, the increases in trust supported technology adoption. As such, governments and businesses can dedicate efforts to enhance customers’ trust and ultimately promote better acceptance of blockchain technologyand its applications.

The Bitcoin digital currency depends for its correctness and stability on a combination of cryptography, distributed algorithms, and incentive driven behavior. We examine Bitcoin as a consensus game and determine that it relies on separate consensus about the rules and about game state. An important aspect of Bitcoin’s designis the mining mechanism,

in which participants expend resources on solving computational puzzles in order to collect rewards. This mechanism purportedly protects Bitcoin against certain technical problems such as inconsistencies in the system's distributed log data structure. We consider the economics of Bitcoin mining, andwhether the Bitcoin protocol can survive attacks, assuming that participants behave according to their incentives.

[8]Discover the issues that have been raised in terms of privacy, security and risk. It is important that the right balance is achieved between the rapid development of Blockchain technology and its legal stability, assuring thatthe legal and regulatory dimensions do not hinder innovation in this space. This paper identifies the technological and regulatory dimensions related to Blockchain technology. It reviews the basic concepts related to Blockchain technology and "distributed ledger technology". They analyze the different possible applications of Blockchain technology, especially as it relates to financial markets. Finally, they addressed regulatory developments in the EU and the US as well as the legal challenges. The article concludes on the need for the adoption of a regulatoryframework which is flexible enough to encourage innovation while protecting consumers and end users.

[10] Bitcoin as a consensus game and determines that it relies on separate consensus about the rules and about game state. An important aspect of Bitcoin's design is the mining mechanism, in which participants expend resources on solving computational puzzles in order to collect rewards. This mechanism purportedly protects Bitcoin against certain technical problems such as inconsistencies in the system's distributed log data structure. It considers the economics of Bitcoin mining, and whether the Bitcoin protocol can survive attacks, assuming that participants behave according to their incentives. It shows that there is a Nash equilibrium in which all players behave consistently with Bitcoin's reference implementation, along with infinitely many equilibria in which they behave otherwise. We also show how a motivated adversary might be able to disrupt the Bitcoin system and "crash" the currency.

[11] The rise of cryptographic currency can be seen as both an upset for the financial cycle (as the blockchain convention can be carried out in numerous areas outside the financial degree) and an advancement of the moneyrelated framework. In noting the introductive citation, the eventual fate of digital forms of money will rely upontheir capacity to keep their worth stable. As the hypothetical model previously determined, cryptographic formsof money are more a danger for the monetary dependability than a danger for the fate of national banks. Nonetheless, one of the significant parts of a 'perfect world' is to be unusual. Despite the fact that the volume of digital currencies are minuscule and don't challenge national banks these days, we ought not disparage the IT upset in the money related field. Perhaps the significant impacts of the digital currencies ought to be found external to the financial area attributable to the blockchain openings offered in numerous areas

[13] The essential methodologies for finding understanding are explained. A short relationship with unified systems has been done and its characteristics and deficiencies have been delineated. Also, its applications in various spaces are analyzed exhaustively. A diagram of at present live applications in these spaces like bitcoin for advanced cash is made, and the work of blockchain in these applications is analyzed. We moreover spread out its future expansion and shortcomings including nonappearance of rule and potential security deserts. This assessment is appropriate to both the amateur and instructed peruser, as the need, fundamental things and the thought driving the advancement and the general applications and shows are discussed exhaustively.

[14] This paper gives an outline of the idea of blockchain innovation and its capability to upset the universe of banking through working with worldwide cash settlement, brilliant agreements, mechanized financial records and advanced resources. In such manner, it gives a concise outline of the center parts of this innovation, just as the second-age contract-based turns of events. From that point we talk about central questions that should be considered in growing such record based advances in a financial setting.

[15] Bitcoin, Litecoin, Dogecoin, et al 'digital currencies' have delighted in a fleeting ascent in prominence and use as a method of performing exchanges on the Internet and past. While acquiring market valuations of billions of dollars and creating a lot of mainstream press in doing as such, little has been scholastically distributed on the Computer Science/Information Systems (CS/IS) establishments of this marvels. This paper portrays these establishments. In doing as such, it is trusted that the achievement of the digital money installment frameworks can be utilized to exhibit how PC hypothesis can be incorporated into different controls with sensational outcomes. It covers the fundamental innovations empowering blockchain innovation and digital currency. The paper talks about the subject of cryptography and how it gives security, preparing power necessities and how the critical thinking hash is made more enthusiastically dramatically and how distributed organization truly alters the innovation by making a hack-verification framework.

[16] Epitomes depicted in this incorporate an electronic exchange administration organization (additionally alluded to thus as a unified electronic exchange (CET) administration). As per an epitome, a monetary administration framework has numerous CET sites for different dealers. All exchanges through any CET site are executed and overseen by the monetary administration framework. Shippers may redo their sites to incorporate a marked look and feel.

The shipper sites are important for a CET administration for which a client can enlist. Enlisted clients would thenbe able to view and pay solicitations from any vendors having CET sites, regardless of whether buys were madeon the web or disconnected. Clients indicate inclinations for the CET Service including picking existing client accounts from which the monetary administration framework is to pay solicitations in the interest of the client. This dispenses with

the requirement for the client to open and finance a different installment account as in customary techniques.

A framework, containing: at any rate one memory putting away PC executable guidelines. The arrangement of guarantee 1, wherein the installment contains one of (I) a money installment or (ii) a pre-loaded card installment.Less responsive Only for officials with through information on blockchain.

[17] Coupling blockchain with the Internet of Things could give a lively, decentralized way to deal with and manage the rapidly growing number of coordinated contraptions. Enabling unique reconfiguration of blockchain limits could provoke a system prepared for enduring advancing conditions. Study blockchain plan as a cycle with flexible perspectives helps with inspecting what limits can be picked to self-administer in an autonomous system. In this paper, we gave a less troublesome perspective of blockchain plan segments for a 173 IoT structure, explicitly for the acquiring of sensor data. Regardless of the way that we actually can't totally explore a system for key spread for our system, we have arranged the design we need to unite blockchain with IoT and the cloud.

[18] Blockchain affects the present innovation by upsetting the monetary business through usage of digital formsof money utilizing decentralized control. This has been trailed by stretching out Blockchain to traverse a few different enterprises and applications for its abilities in confirmation. With the latest thing of seeking after the decentralized Internet, numerous techniques have been proposed to accomplish decentralization considering various parts of the current Internet model going from foundation and conventions to administrations and applications. This paper explores Blockchain's abilities to give a hearty and secure decentralized model for the Internet. The paper directs a basic audit on late Blockchain-based techniques able for the decentralization of things to the Internet. We distinguish and examine two exploration parts of Blockchain that give a high effect inunderstanding the decentralized Internet concerning current Internet and Blockchain challenges while keeping different plans in contemplation. The principal viewpoint is the agreement calculations that are essential parts for decentralization of the Blockchain. We recognize three key agreement calculations including PoP, Paxos, andPoAH that are more satisfactory for arriving at agreement for such gigantic scope Blockchain-empowered design for Internet. The second viewpoint that we examined is the consistency of Blockchain with different arising Internet advances and the effect of Blockchain on those advances. Such arising Internet advancements in mixes with Blockchain would assist with defeating Blockchain's set up blemishes in a manner to be more streamlined, productive and material for Internet decentralization.

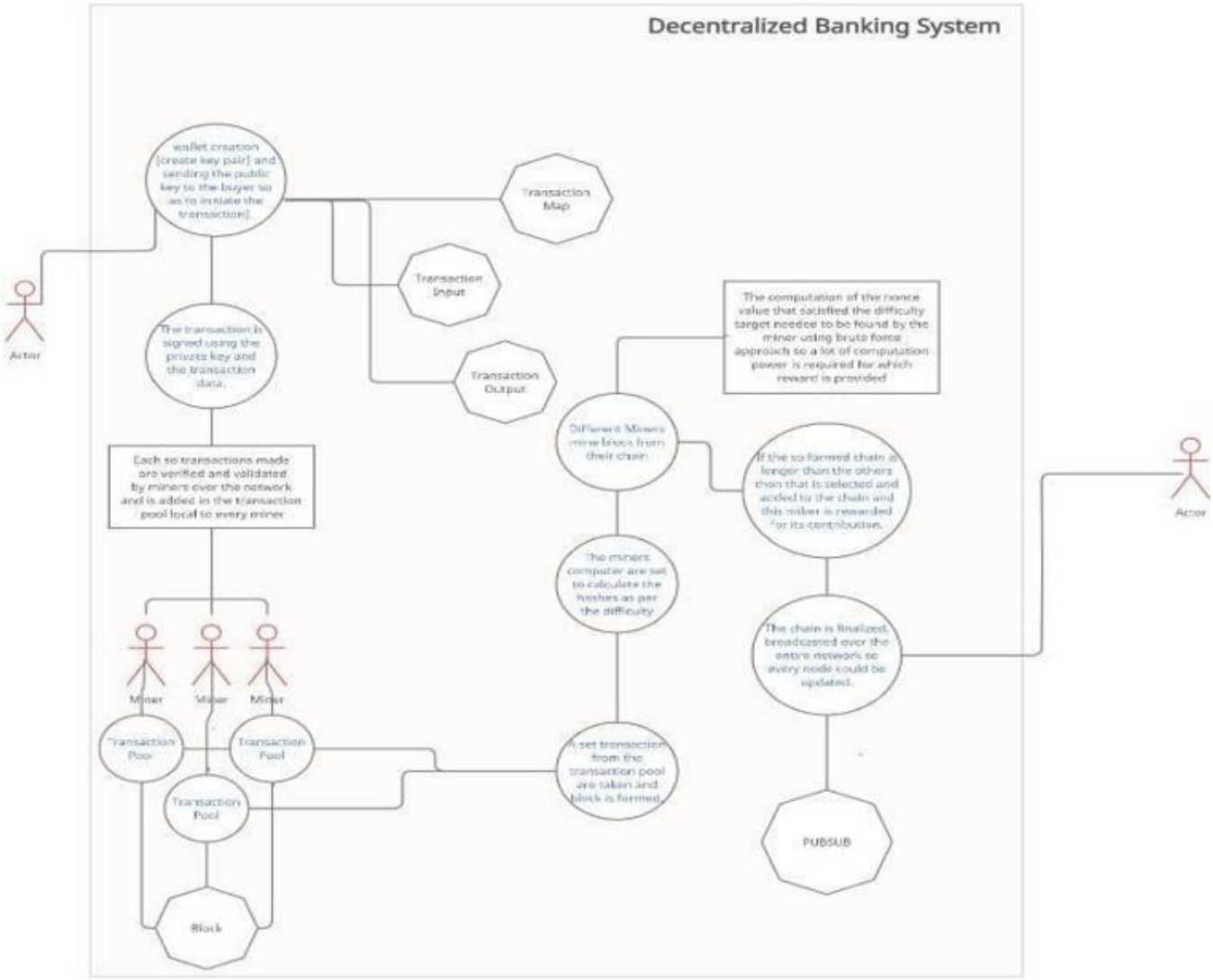
A. Existing Model

The Current Banking Technology is a centralized system and it is the major drawback of this technology.It is necessary to work with a third-party organization or with the central administrator. It means that the system works with an intermediary as a head and only responsible to make the decisions. Each system has the database and it is important to protect this database, because when the system is working with thethird-party organizations, there is a hacking risk of the database or the data may turn up in the wrong hands. The process of database security might take a lot of time and might cost a lot of money. If the system is centralized, it can be changed or deleted, because the decision is made by one person.

Moreover if the transaction is made the transaction is known to the third-party and that information if thethird party is not trusted than the information could be leaked and their could be privacy breaches as well as the person doing a transaction would not want anyone to know about a particular transaction thus this is an issue which is faced by current banking systems biggest challenges faced by these web applicationsare:

- Security issues are prevalent as they are favourite targets to attackers.
- Managed databases causes unreliability and breakdown issues
- There are large transactions requiring database storage costs.
- Maintenance costs are also very high
- It is very hard for a user to trust an online system
- Lack of 2 step verification causing transactional mistakes.
- The reward systems require real money or absent reward system.

B. Proposed Work



So, basically the entire application is composed of the following main components:-

➢ *Block*

- Have data, timestamp, lastHash, hash, nounce, difficulty.
- Genesis: This is the starting Block for the chain with fixed hash Value as it is the start.
- Mine Block: This will ensure a node to mine blocks to contribute to the chain.
- Adjust Difficulty: This will help to adjust the difficulty as per the computational power present inthe network.

➢ *Wallet*

- Balance, keyPair, publicKey: This is necessary as the key Generation of the wallet will ensureprivacy and provide pseudo-anonymity to the user.
- Before releasing the transaction into the network the transaction information is signed by thesender.
- Create Transaction: This will create the transaction with the appropriate checks likeamount available and validity of the wallet.
- Public Key: This will act as the account number for the network the person can make atransaction using this as the account number of the receiver and the sender.

➢ *Transaction*

- Transaction Id: A unique random Id is provided to every transaction to ensure thevalidity.
- Valid Transaction: This will check whether the transaction is valid given the accountnumber and whether the amount is present in the account.
- Update: If the transaction is already there in the transaction pool and more amountis transferred to the person then the value will be updated.
- Reward Transaction: As the person which has used the computational power to add ablock successfully in the current chain is to be rewarded with the miner Reward.

➢ *Transaction Pool*

- Transaction Map: Local map unique to every node is created transactions
- Set Map: This will add a transaction with input and output

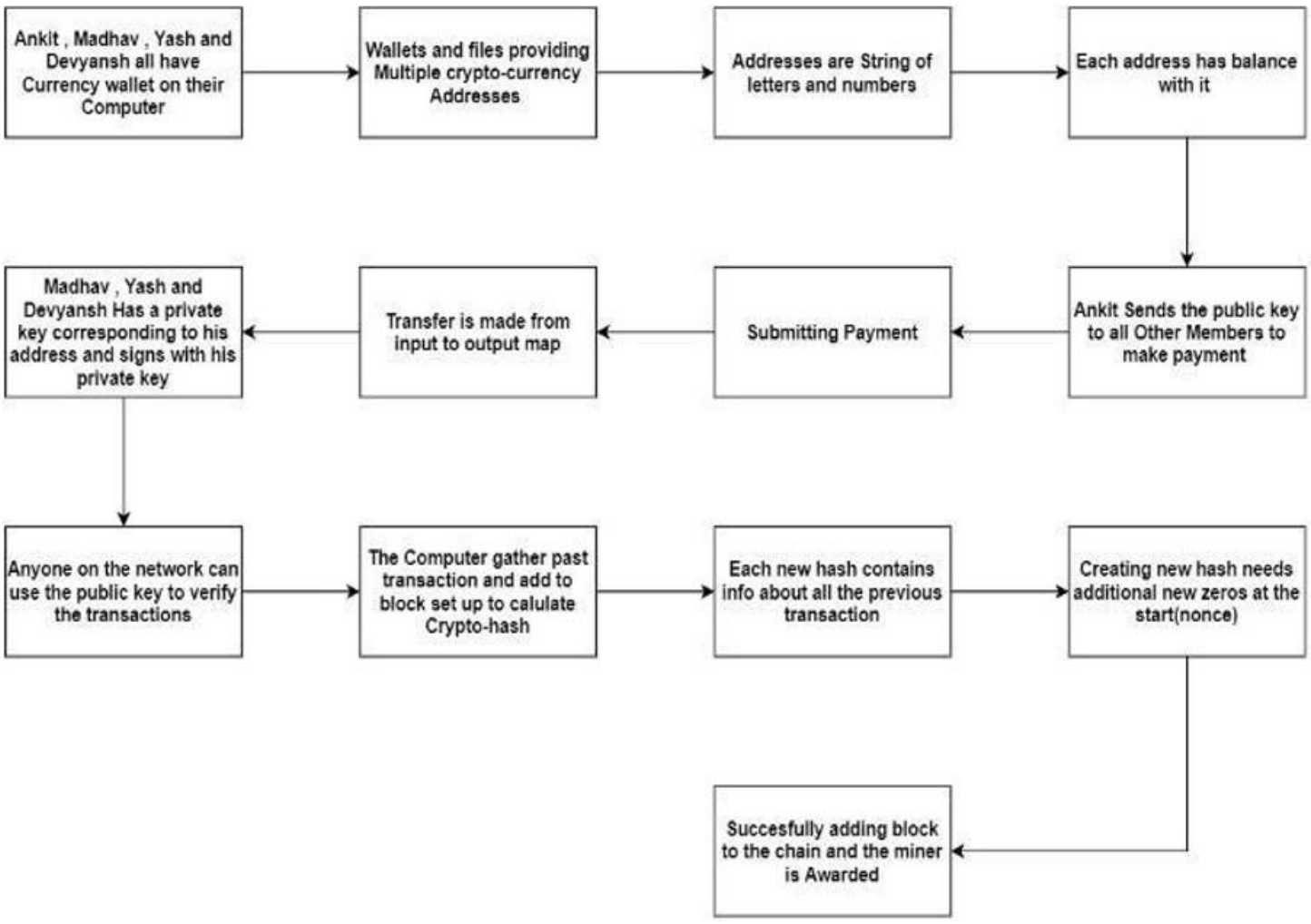
info. and set the keyas the ID of the transaction.
- Existing Transaction: Will check whether this transaction is already on theblock and needs to be cleared.
- Valid Transactions: This will check all the transactions in the pool whether theyare valid as per the key and the amount.
- Clear: This will clear the transaction from the broadcasted transaction.
- Clear Transaction: remove the transaction from the local pool as they arealready existing transactions.

➢ *Miner*
- Blockchain: Need the currently broadcast chain to add new blocks
- Wallet: If successfully added to the chain wallet is required to give a miner reward.
- Pubsub: Broadcast channels created using redis which will allow to take the information of the chain newly updated and bring any policy changes into the notice of the network nodes
- Mine Transaction: Mine the transaction(verifying and validating) to add these in the localtransaction pool.

➢ *Chain : Chain of thr blocks*
- AddBlock: adding a new block to the chain(proof-of -work)
- Is Valid Chain: to check whether the chin is valid no double spending attack
- Replace Chain: replacing the chain if a longer valid chain is there.
- Valid Transaction: check the validity of the transaction.
- Valid Transaction Data: here the data within the the transaction is seen

➢ *Pubsub*
- Channels: for chain, or policy changes
- Handle message in Channels: if policy is accepted or chain ois changed the message handler willinform the subscriber
- Subscribe Channels: Will allow the nodes to join the network.
- Broadcast Chain: Will broadcast the newly updated chain over the network
- Broadcast Transaction: This will broadcast transactions to the chain.

C. Workflow of the application

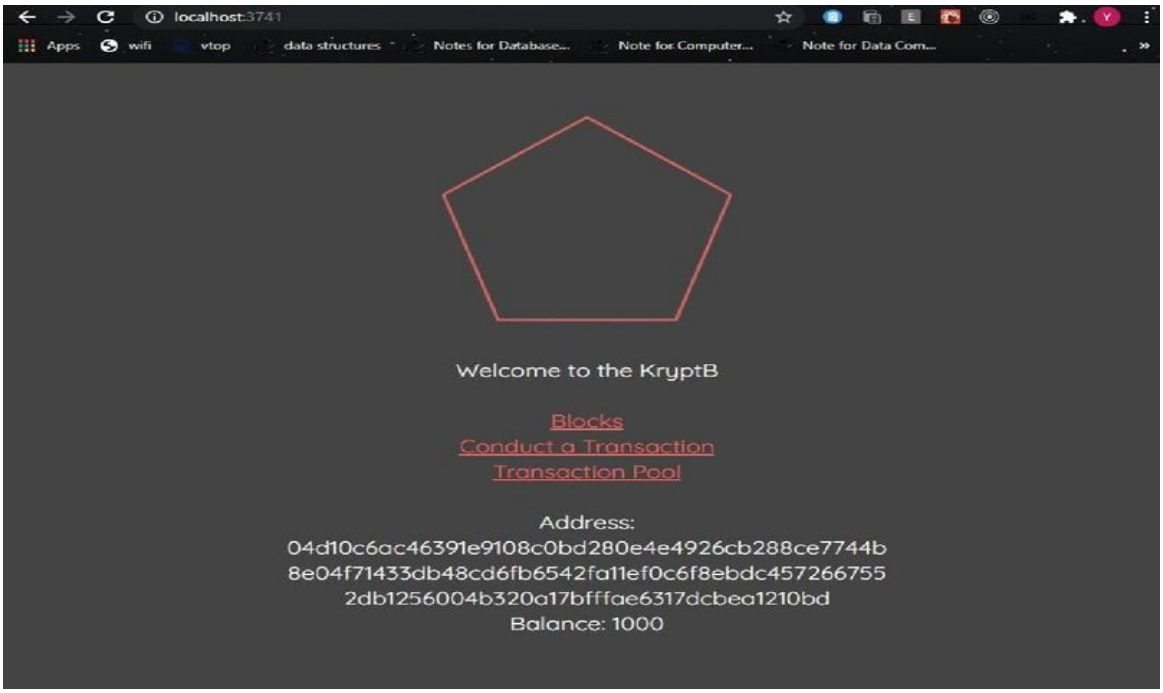


ISSN No:-2456-2165

III. RESULTS AND IMPLEMENTATION

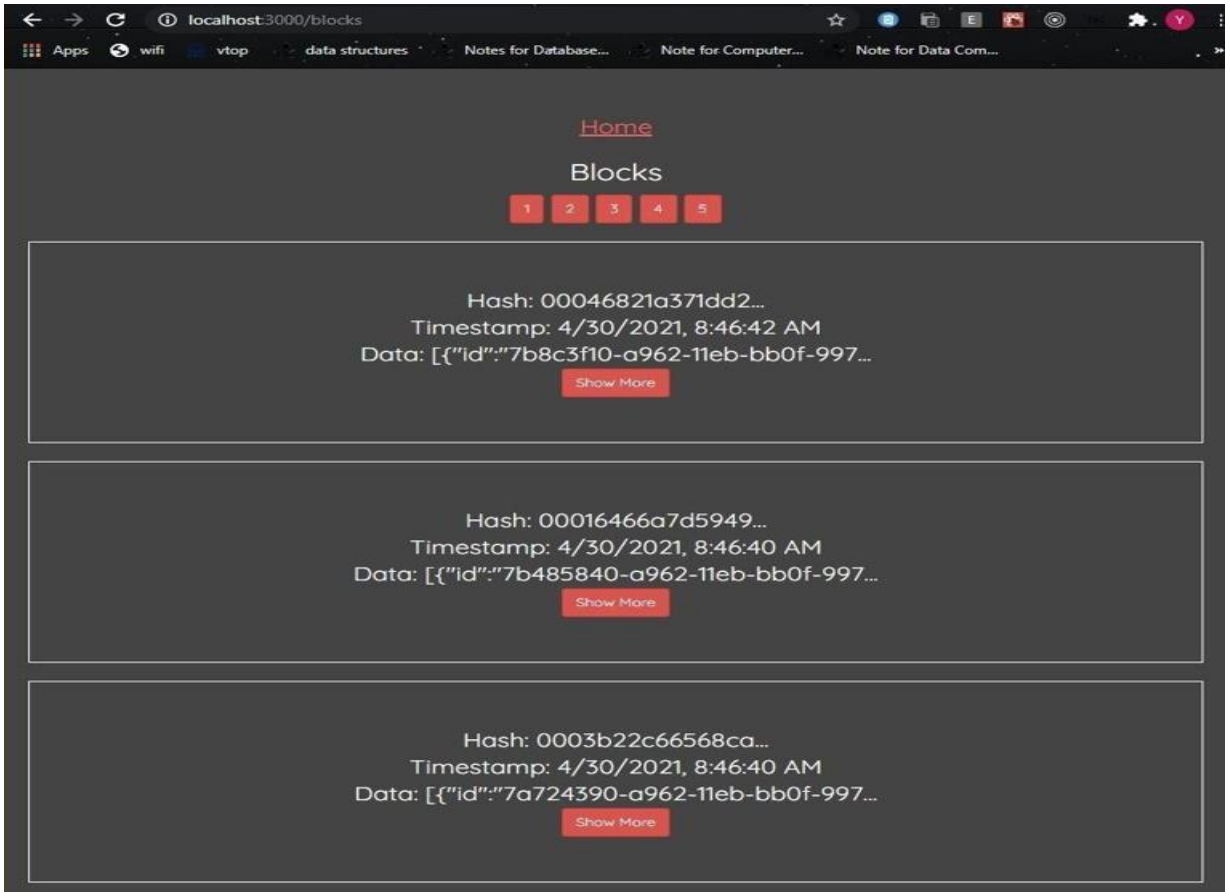
A. Home Page

Here we can see that the anonymous user identity is maintained and we have assigned a unique public key tothe user.



B. View of Blockchain

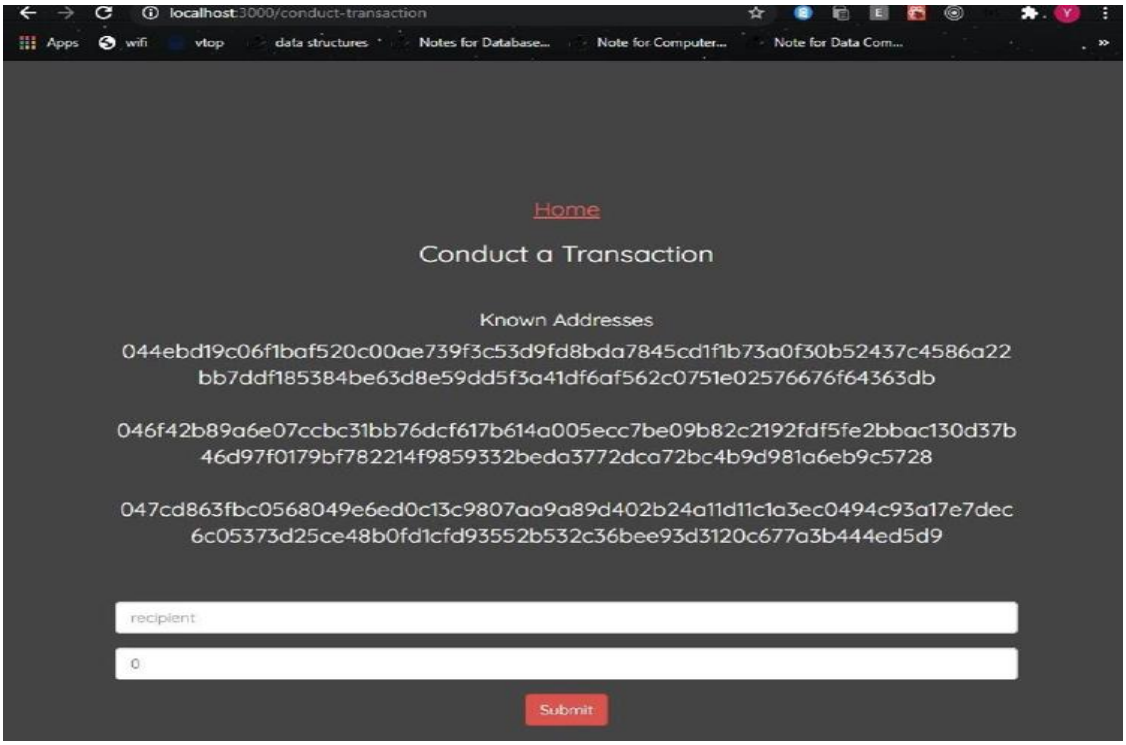
Here we can view the blockchain along with the associated blocks so here we ensure the transparency in thesystem by making the public key of the users and the transaction being added to the chain with their respective hash and previous hash value.



ISSN No:-2456-2165

C. Blockchain Transaction

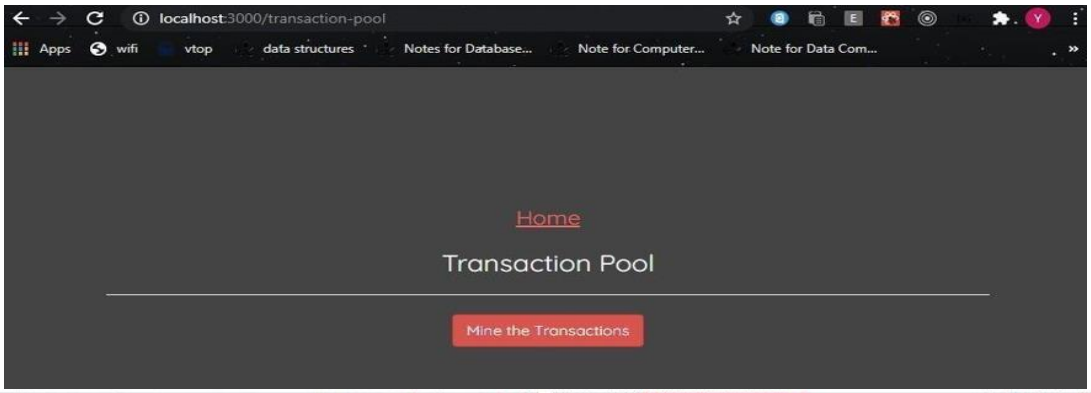
Here the public key of the user and his available balance is shown. Users can navigate to therest of the pages via the home page.

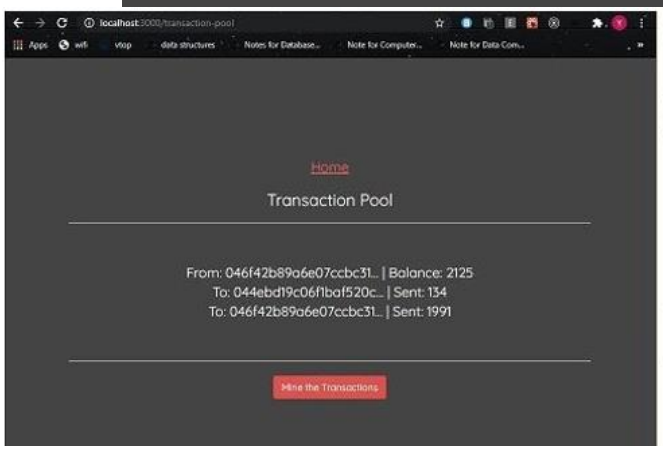


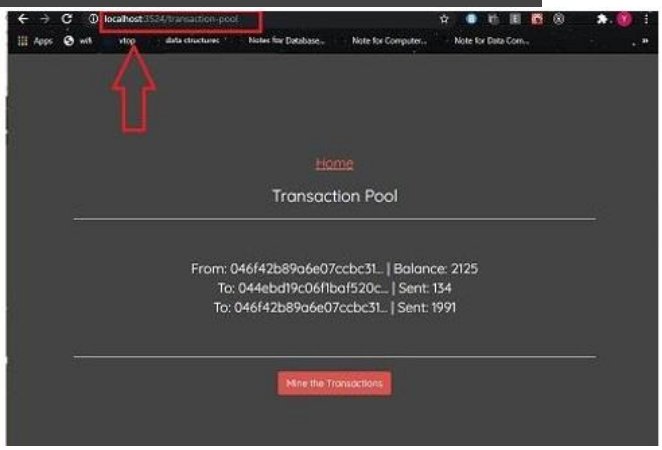
D. Transaction Pool and Mining

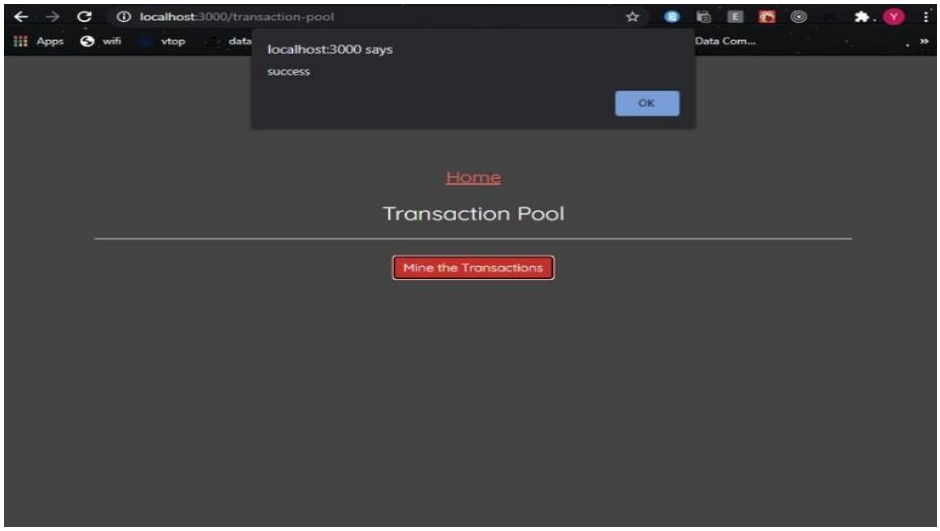
Here we have local Transaction Pool where all the miners have the valid transactions so far done(but not added tothe main consensus chain) using this transaction data the miners are going to calculate the nonce and mine the block and after successful mining these transactions will be cleared from their local transaction pool

The below figures will gave a better understanding on the procedure for block mining

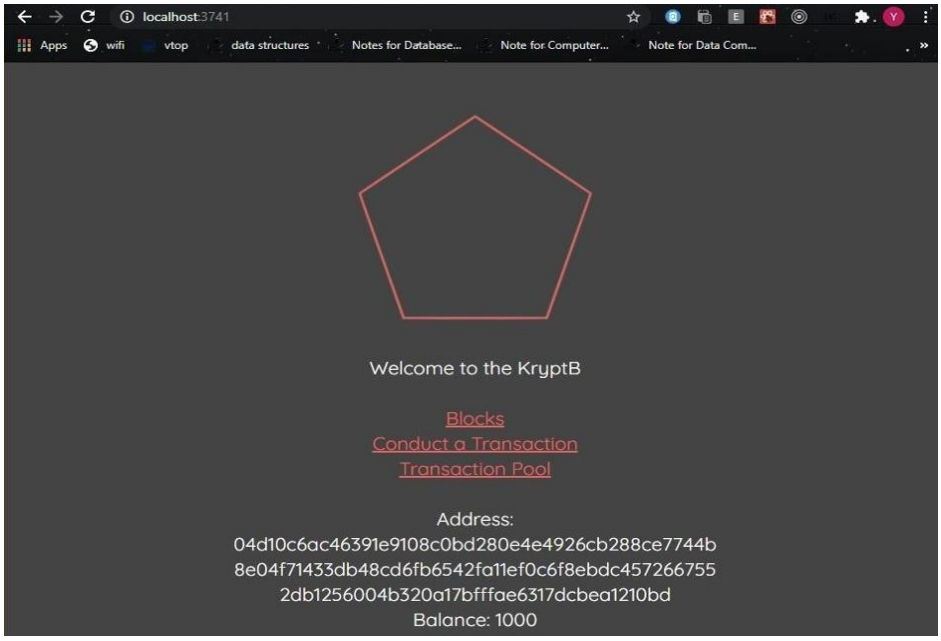






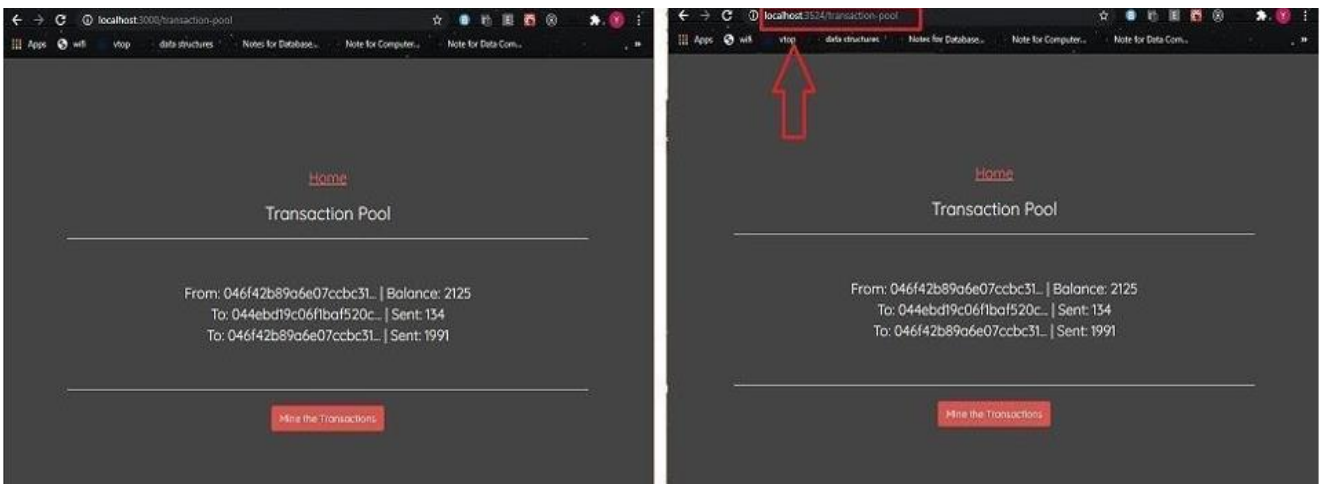


E. New node joining the network



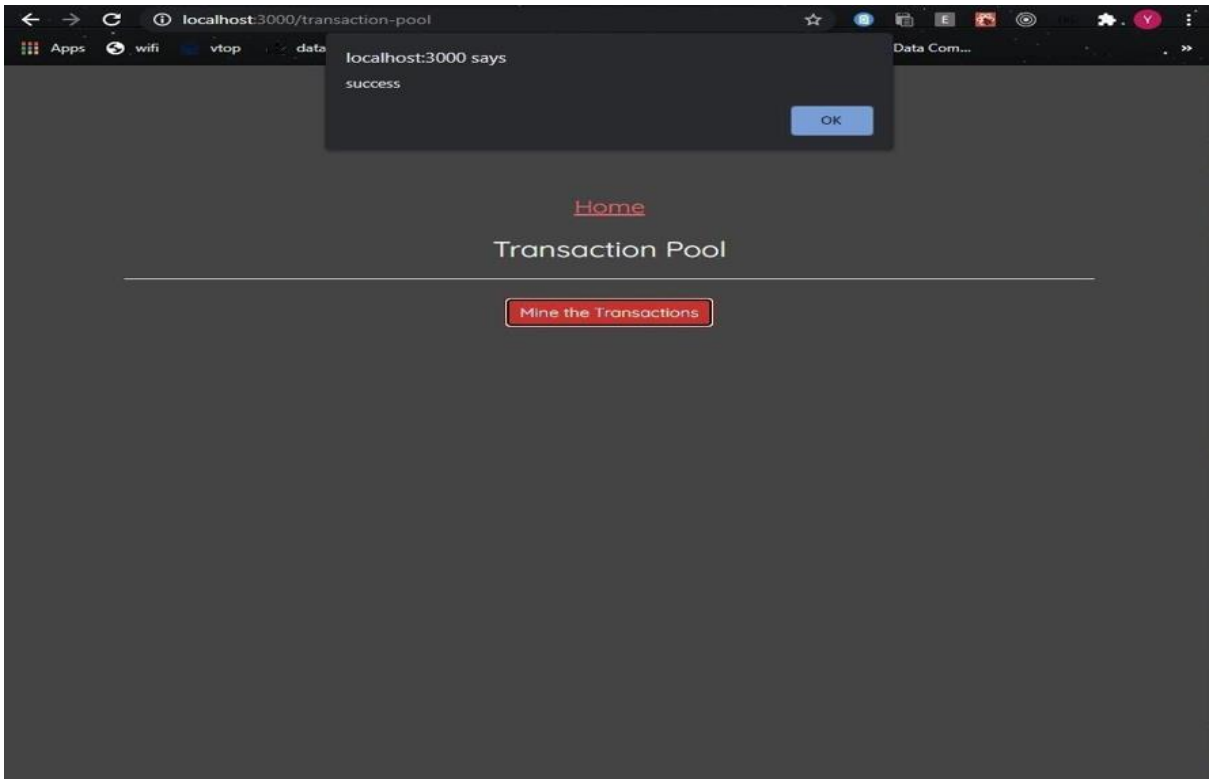
As you can see the new node has joined the network and is allotted a public key and private key pair alongwith a starting balance of 1000.

F. As the transaction are being broadcasted they can be visible in both the active node over the network



ISSN No:-2456-2165

G. Transaction being mined by localhost 3000 which resulted in clearing of transaction pool



H. The mined bock added to the local blockchain onto the system (along with miner's award)

Here after the successful mining we can see that the miner is awarded with a miner reward this is tokeep them enthusiastic about mining and also valuing their computation expense.

IV. PERFORMANCE ANALYSIS

S no	Citation	Benefits	Proposed Work Benefits
1.	Acceptance of Financial Transactions using Blockchain Technology and Cryptocurrency: A Customer Perspective Approach by Hayder Albayati, KyoungKim, Jae Jeung Rho.(2020)	This paper intends to estimate the usability of blockchain technology by investigating behaviouralelements that affect customers' intention towards blockchain-based cryptocurrency transactions. The findings indicate two powerful constructs (regulatory support and experience) that encourage customer's trust toward blockchain-based applications. The surveyed people agreed significantly, feeling secure and they can trust the Blockchain-based applications when it is regulated and ensured by the local government. Also, at a certain level of experience, users feel trusted using blockchain-based applications, the increases in trustsupported technology adoption. As such, governments and businesses can dedicate efforts to enhance customers' trust and ultimately promote better acceptance of blockchain technology and its application	In our proposed model we have ensured that the customer privacy is preserved as we have offered a key pair to the user so the user can use the public key to communicate with other nodes and the private key for digital signatureand verification of the node over the network,to ensure the trust of the user over our system.

2.	Antonopoulos, A.M., 2017. Mastering Bitcoin: Programming the open blockchain, 2nd ed. O'Reilly Media, Sebastopol, CA.	The report argues that Bitcoin will require the emergence of governance structures, contrary to thecommonly held view in the Bitcoin community thatthe currency is ungovernable.	We considered the economics of Bitcoin mining, and whether the Bitcoin protocolcan survive attacks, assuming that participants behave according to their incentives. Therefore, we implemented the bitcoin concept in establishment of Decentralized Banking
3.	BlockChain Based Banking Application Miss. Patil Snehal A.1,Mr.Mohire Abhishek S.2, Miss. Vibhute Aishwarya Ulhas3, Miss. Shaikh Rabana Sharif4, Miss. MaliJyoti Ashok5 April 2019	The proposed paper helps us to analyze counteracting moneylaundering and financing of terrorism in the country and around the world apartfrom it explanation of proof of stake and we are also given a redumental undersatndng of how consensus is made and mechanism is explained	The Bitcoin digital currency depends for its correctness and stability on a combination of cryptography, distributed algorithms, and incentive drivenbehavior. We examined Bitcoin as a consensus game and determined that it relies on separate consensus about the rules and about game state.
4.	Murem S. Sharpe (1987), "System for centralized processing of accounting and payment functions.", USA patientsAmmous, S., 2018. The bitcoin standard: the decentralized alternativeto central banking. John Wiley & Sons, Hoboken, NJ.	Embodiments described herein include an electronic transactionservice network (also referred toherein as a centralized electronic transaction (CET) service). Merchants may customize their web sites to include a branded look and feel. Registered customers can then view and pay invoices from any merchants having CET web sites, whether purchases were made onlineor offline. Customers specify preferences for the CET Service including choosing existing customer accounts from which the financial management system is to pay invoices on behalf of the customer. This eliminates the need for the customer to open and fund a separate payment account as intraditional methods.	Here to make our web application more responsive for large users we have redis serverso the main reason for using this server is that the entire data being processed using cache memory which deals with faster fetching of the data hence results in better response and performance in case the load increases. Here we have tried to make the application as user friendly as possible as the user in the home page will share the services and the user can choose whichever service he/she wants.
5.	Hassani, H., Huang, X., & Silva, E. (2018). Banking with blockchain-ed bigdata. Journal of Management Analytics,5(4), 256-275	The proposed model provides evidence of selectedbanks adopting blockchain technology in isolation or small groups. They found the need for extensiveresearch and development into several aspects of banking with blockchain to overcome the challenges which are currently hindering its adoption in banking across the globe.	Here the problem in the proposed modelis scalability so we are addressing the scalability of the system which will ultimately improve the reliability of our system.
6.	Cocco, L., Pinna, A., & Marchesi, M.(2017). Banking on blockchain: Costssavings thanks to the blockchain technology. Future internet, 9(3), 25.	The paper studies the actual performance of the Bitcoin system, also highlighting its major limitations,such as the significant energy consumption due to the high computing power required, and the high cost of hardware. It also estimates the electrical powerand the hash rate of the Bitcoin network, over time.	The key problem which can be observed in thecurrent blockchain transaction based system isthat the return transaction would result in generation of new public key which is to be remembered by the user as well as the ledger instead we are transferring the amount to the same public key of the user.
7.	Cryptocurrencies: Core Information Technology and Information System Fundamentals Enabling Currency Without Bordersby Anthony Serapiglia, Constance Serapiglia and Joshua McIntyre.(2015)	This paper describes the foundations such as cryptocurrencies have enjoyed ameteoric rise in popularity and use as a way of performing transactions on the Internet and beyond . In doing so, it is hoped that the success of the cryptocurrency payment systems can beused to demonstrate how computer theory can be integrated into other disciplines with dramatic results. It covers the main	The paper failed to discuss the topic of cryptography and how itprovides security, processing power requirements and how theproblem solving hash is made harder exponentially and how peer-to-peer.We have incorporated these standard metrics along with the ones mentioned in the paper to produce a new system.

8.	The blockchain revolution: An analysis of regulation and technology related to distributed ledger by Hossein Kakavand and Nicolette Kost De Servers(2017)	They analyze the different possible applications of Blockchain technology,especially as it relates to financial markets. Finally, they addressed regulatory developments in the EU andthe US as well as the legal challenges. The article concludes on the need for the adoption of a regulatory frameworkwhich is flexible enough to encourage innovation while protecting consumers and end users.	Through the deployed tactics of the cited paper, we have made use of Blockchain to produce a system which provides anonymity to its users on a regulatory basis by providinga public key. We have taken measures considered in developing such ledger-based technologies in a banking context.
9.	Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet ofMoney by Peters, G. W., &Panayi (2016)	This paper provides an overview of the core aspectsof this technology, as well as the second-generationcontract-based developments. From there we discuss key issues that must be considered in developing such ledger-based technologies in a banking context	In our proposed model we have implementedthe ledger-based technology in a banking context for safe,secure and anonymous transactional processes.
10.	The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries by Joshua A. Kroll, Ian C. Davey, and Edward W. Felten(2013)	The paper examines Bitcoin as a consensus game and determines that it relies on separate consensus about the rules and about game state. An important aspect of Bitcoin's design is the mining mechanism, in which participants expend resources on solving to be delivered on a best effortbasis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with these computational puzzles in order to collect rewards. This consensus mechanism purportedly protects Bitcoin against certain technical problems such as inconsistencies in the system's distributed log data structure. It considers the economics of Bitcoin mining, and whether the Bitcoin protocol can survive attacks, assuming that participants behave according to their incentives. It shows that there is a Nash equilibrium in which all players behave consistently with The greater part ofour cash is digitized as of now, regardless of Bitcoin's reference implementation, along with infinitely many equilibria in which they behave otherwise. We also show how a motivated adversary might be able to disrupt the Bitcoin system and "crash" the currency.	Using the unique and innovative idea wehave tried to implement the same but in practical sense we have used the nonce value which will be ultimate deciding factor for rewarding the miner here we have used the proof of work algorithm which allows users to find out the nonce value using the CPU and whichever useris the first to compute the nonce and addblock to the chain is rewarded
11.	Nicolas BARBAROUX & Adrien LUTZ, University of Saint-Etienne (France) GATE Lyon-St Etienne,UMR CNRS 5824:A Decentralized BankingSystem: the 21st utopia	The paper describes the eventual fate of digital forms of money will rely upon their capacity to keep their worth stable. As the hypothetical modelpreviously determined, cryptographic forms of money are more a danger for the monetary dependability than a danger for the fate of nationalbanks	Digital forms of money have become more used in this era, so it becomes a necessity toprocure and secure the anonymity and sanctuary of individual customers or transactors on a ledger-based system. The proposed model provides a framework and backbone for the same.

12.	Nakamoto S. (2008) : Bitcoin: A Peer-to-Peer Electronic Cash System.	Proposed model of a peer-to-peer network using proof-of- work to record a public history of transactions that quickly becomes computationally impractical for anattacker to change if honest nodes control a majority of CPU power hasbeen introduced. The network is robust in its unstructured simplicity. Nodes work all atwith little coordination. They do not need to beidentified,since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalidblocks by refusing to work on them. Any needed rules and incentives canbe enforced with this consensus mechanism	Understanding this paper has motivated us to develop a mechanism through which we can adjust the difficulty as per the computational power present over the network to make our application more reliable. Apart from it, wehave also thought of using the mechanism tobroadcast to vote for the changes in the blockchain
13.	Gupta S. Lauppe P. and Ravishankar S.,Yale University, 2017 FedCoin, a blockchain backed Central Bank cryptocurrency :FedCoin, a blockchainbacked Central Bank cryptocurrency	An effective Fedcoin would make monetary orders, credit card companies, and Bitcoin old, while changing the country's mechanism for money.This report presents a proof-of-idea national bank digital currency, and the accompanying codebase reproduces clients making exchanges on digital media.	The cited paper describes the dawn of “Fed Coins” leaving behind all paper works of cashand cheques, be it money too. Therefore our paper proposes such a model (”Decentralized Banking”) which provides a framework or backbone for exchange of Digital Currencies.
14.	L. Cocco, A. Pinna, M. Marchesi Banking on blockchain:Banking on blockchain: costs savings thanks to the blockchain technology Future Internet	Blockchain innovation has the probability to upgrade the worldwide financial infrastructure, enhancing the efficiency of current financial frameworks. This paper takes a gander at the difficulties and opportunities of executing blockchain innovation across banking and capital business sectors. They considered that mining equipment has developed over the long run, passingbox CPU, GPU, FPGA, and ASIC. In particular, they thought about two of its highlights: the hash rate and the force utilization. Utilizing two fitting curves, they ponder the possibilities of this problematic innovation. The registered the "best hash rate per $",R(t)and the "best force utilization function", P(t).We defined three amounts: "financial efficiency" (EE), "operational efficiency"(OE), and "efficient service" (SE).	This paper has brought out the energy loss in the computation for an unsuccessful miner which could cost him a lot and gradually it will lose interest in mining and would result in loss of nodes over the network so to address we can use the energy from CPU to be adjusted in charing or in a electric heater to utilize this residual energy thus preventing energy loss

V. FUTURE WORK AND CONTRIBUTION TO DEVELOPMENT

Looking forward, this technology cannot just be limited top currency transactions as it has applications far and wide beyond the scope of monetary transactions. It can be used to draw up smart contracts which for a change canbe trusted while doing online transactions. It can be used to form decentralized "democratic" organisations. This type of applications can be used in medical fields for a decentralized EHR(Electronic Health Record) system When it comes to blockchain technology, possibilities are truly endless. Here, we have used the technology of blockchain for digital transaction but the same could be extended for the health records, voting systems, supply chain so using this distributed immutable ledger we can use this tech as a form of new cloud as the ledger will store the data but the records will be immutable so any person can store his/her personal data on the blockchain permanently.

Our exploration and extraordinary issue papers' primary commitment is delineating the perplexing and multi- layered job of Blockchain in the financial turn of events. We propose a system introducing advancement as a reliant variable and five fundamental classes of factors addressing different cultural, mechanical, business, and strategy related contemplations.

The introduced idea is Decentralized Banking interconnected with recommended causal connections, introducing a few intriguing ways prompting advancement and recommending promising future exploration roads. We acceptthat our structure might help the Banking sector and guide future exploration endeavors in the Blockchain for Development field. Furthermore, a clear and noteworthy explanation may guide this issue.

Decentralized Banking System is a real life demonstration of the trust system that can be placed on blockchain technology. It provides an unhackable environment to carry out valuable transactions which can be of any nature. Conducting such transactions over the internet is always a point of concern for the users as their security can neverbe guaranteed. Blockchain however, does provide that proof of concept that can be widely trusted and be implemented for real world use.

ACKNOWLEDGEMENT

We take immense pleasure in thanking **Dr. G. Viswanathan**, our beloved Chancellor, VIT University and respected Dean, **Dr. R. Saravanan**, for having permitted us to carry out the project.

We express gratitude to our guide, **Prof. Pramod Kumar Maurya**, for guidance and suggestions that helped us to complete the project on time. Words are inadequate to express our gratitude to the faculty and staff members who encouraged and supported us during the project. Finally, we would like to thank our ever-lovingparents for their blessings and our friends for their timely help and support.

REFERENCES

[1]. Albayati, H., Kim, S. K., & Rho, J. J. (2020). Accepting financial transactions using blockchain technology and cryptocurrency: A customer perspective approach. Technology in Society, 62, 101320.
[2]. Antonopoulos, A. M. (2017). Mastering Bitcoin: Programming the open blockchain. " O'Reilly Media, Inc.".
[3]. Cocco, L., Pinna, A., & Marchesi, M. (2017). Banking on blockchain: Costs savings thanks to the blockchain technology. Future internet,9(3), 25.
[4]. Devanbu, Premkumar, Gertz, Michael, Martel, Charles, & Stubblebine, Stuart G. 2001. Authentic third-party data publication. Pages 101– 112 of: Data and Application Security. Springer
[5]. Gupta, S., Lauppe, P., & Ravishankar, S. (2017). Fedcoin: A Blockchain-Backed Central Bank Currency.
[6]. Hassani, H., Huang, X., & Silva, E. (2018). Banking with blockchain-ed big data. Journal of Management Analytics, 5(4), 256-275.
[7]. Holmberg, U., Sjögren, T., & Hellström, J. (2010). Comparing Centralized and Decentralized Banking.
[8]. Kakavand, H., Kost De Sevres, N., & Chilton, B. (2017). The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. Available at SSRN 2849251.
[9]. Kosba, Ahmed, Miller, Andrew, Shi, Elaine, Wen, Zikai, & Papamanthou, Charalampos. 2015. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. Tech. rept. Cryptology ePrint Archive, Report 2015/675, 2015. http://eprint. iacr. org
[10]. Kroll, J. A., Davey, I. C., & Felten, E. W. (2013, June). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries.In Proceedings of WEIS (Vol. 2013, p. 11).
[11]. McLeod, S. (2017). Bitcoin: The utopia or nightmare of regulation. Elon L. Rev., 9, 553.
[12]. Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 4.
[13]. Patel, R., Sethia, A., & Patil, S. (2018, September). Blockchain–Future of Decentralized Systems. In 2018 International Conference on Computing, Power and Communication Technologies (GUCON) (pp. 369-374). IEEE.
[14]. Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transactionprocessing and smart contracts on the internet of money. In Banking beyond banks and money (pp. 239-278). Springer, Cham.
[15]. Serapiglia, A., Serapiglia, C. P., & McIntyre, J. (2015). Crypto currencies: Core information technology and information system fundamentals enabling currency without borders. Information Systems Education Journal, 13(3), 43.
[16]. Sharpe, M. S., Bryson, E., Manduley, F., Riordan, I. E. M., & Flesser, B. D. (1987). U.S. Patent No. 4,713,761. Washington, DC: U.S.Patent and Trademark Office.

[17]. Song, J. C., Demir, M. A., Prevost, J. J., & Rad, P. (2018, June). Blockchain design for trusted decentralized IoT networks. In 2018 13th Annual Conference on System of Systems Engineering (SoSE) (pp. 169-174). IEEE.
[18]. Wang, H., Ma, S., Dai, H. N., Imran, M., & Wang, T. (2020). Blockchain-based data privacy management with nudge theory in openbanking. Future Generation Computer Systems, 110, 812-823.
[19]. Zarrin, J., Phang, H. W., Saheer, L. B., & Zarrin, B. (2021). Blockchain for decentralization of the internet: prospects, trends, andchallenges. Cluster Computing, 1-26.