iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** I **Month of publication:** January 2023

DOI: https://doi.org/10.22214/ijraset.2023.48650

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue I Jan 2023- Available at www.ijraset.com

Decentralized Chat Application using Blockchain Technology

Keshav Khalkar[1], Nikhil Dhake[2], Sarwesh Kelzarkar[3], Tejas Shinde[4]
P K Technical College of Engineering, gate no 714, Kadachiwadi, Chakan, Pune-4105501
Computer Department Savitribai Phule Pune University.

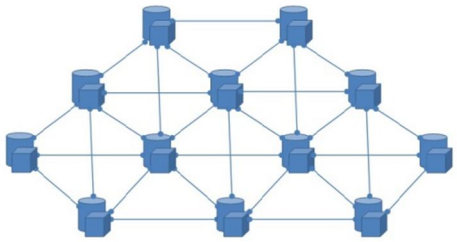
Abstract: ***Decentralized application make use of peer-to-peer networks, this ensures that no network failure can occur due to central node failure. Blockchain serves as an immutable ledger which allows messaging to take place in a decentralized manner. A decentralized application for communication and resource sharing is need in today's world, where keeping data on a centralized server can be risky and costly experience. With the help of various consensus, we can implement different ways to share resources and communicate. Together with Blockchain and Decentralized Applications, we can create a secure and reliable messaging application that overcomes the drawbacks of traditional messaging applications.***
Keywords: Blockchain, Bitcoin, Consensus, Mining, Security, Internet of Things, Hyperledger.

I. INTRODUCTION

In today's generation chatting over messaging platforms are a part of an individual's lifestyle. Today's most of the communication happens over social media platforms. All these platforms also provide users the option to share multimedia attachments leveraging their communication protocols over sockets. All these chat or messaging platforms are processed through centralized servers. All the user's message or information (maybe confidential) is being processed by the central server before transmitting the same to intended recipients. The issue with these kinds of system is that all the information are visible at processing servers even if the messages or information transmitted are claimed to be end to end encrypted. The author has created a messaging or rather say a simple chat application and has explained experimentally shown how the transmitted messages are visible at processing servers. Nevertheless, the system of the centralized system has scalability issues when compared to decentralized computing systems. In this work, the author has proposed a blockchain based solution based on ethereum platform using Whisper Protocol to the issues that exist in traditional messaging or chat applications.

As we all know, traditional chat applications are centralized i.e., all the data is stored on a centralized server. Therefore major problem of this structure is, if the central server fails then whole network collapses. For example, WhatsApp server stored all the data on a central server, if in case that server is destroyed then there can be a loss of user data, or they can even leak the user information stored on the server.

To overcome this, our project makes the use of decentralized Application approach (dApps). In our application all the user data is stored on a block which is connected to other blocks forming a chain. As the name suggests, a decentralized application does not have a centralized server. It is basically a peer-to-peer network. Also the data that is stored in block is almost impossible toview as a very secure encryption and hashing functions (256 bits) are used. Also is a hacker tries to make changes to the information in block then, he/she will have to make changes to all the copies of that block on whole blockchain network and that can be quite impossible. Though blockare on all nodes, they cannot access the information in it, only the person for whom the information if can access it.



Decentralized
nodes are only connected to peers

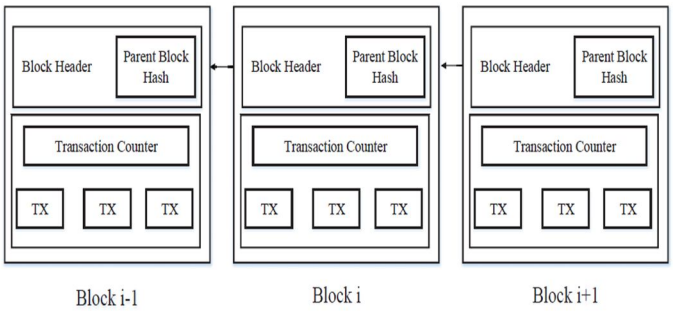


Figure 1.1 Decentralized Application Structure

Decentralized Application consists of multiple nodesconnected to each other in a mesh topology type network.They are connected to each other in a Peer-to-Peer fashion.Blockchain is a sequence of blocks, which holds acomplete list of transaction records like conventionalpublic ledger.

The four main components of any blockchain ecosystemare as follows:

1) A node application
2) A shared ledger
3) A consensus algorithm
4) A virtual machine

a) *Node Application:* Each Internet-connected computer needs to install and run a computer application specific to the ecosystem they wish to participate in. Using the case of Bitcoin as an example ecosystem, each computer must be running the Bitcoin wallet application.
b) *Shared Ledger:* This is a logical component. The distributed ledger is a data structure managed inside the node application. Once you have the node application running, you can view the respective ledger (or blockchain) contents for that ecosystem.
c) *Consensus Algorithm:* This, too, is a logical component of the ecosystem. The consensus algorithm is implemented as part of the node application, providing the _rules of the game‘ for how the ecosystem will arrive at a single view of the ledger.
d) *Virtual Machine:* The virtual machine is the final logical component implemented as part of the node application that every participant in the ecosystem runs. To understand the capabilities added to an ecosystem by including a virtual machine let‘s take a quick look at what a virtual machine is.

II. LITERATURE SURVEY

Nakamoto, Satoshi [2]. In this paper, the complete mechanism of blockchain technology for a electronic cash system that basically allows online payments to be sent directly from oneparty to another without going through a financial institution is presented. It explains a network system which is distributed i.e. peer to peer network which resulted to be a solution for double spending and the Proof of Work algorithm for carrying out safe and secure transactions.

Judmayer, Aljosha et.al [3] presented an overview of blockchain technology in technical point of view also introduced the concepts of cryptographic currencies and the consensus ledgers. This paper mainly focused on the Bitcoin cryptographic currencies saying that the current scientific community is relatively slowly to this emerging and fast- moving field of blockchain technology reason as not sufficient resources available other than bitcoin. It explained deeply about bitcoin and why it has gained a huge market and interest in today’s technology and also highlights the challenges in the area of digital assets management and presents a discussion of Bitcoin usability, privacy, and security challenges from the user’s perspective, the concept, characteristics, need of Blockchain and how Bitcoin works. It attempts to highlightsrole of Blockchain in shaping the future of banking, financialinstitutions.

Zibin Zheng et al. [4] provided an overview of blockchain architecture firstly and compared some typical consensus algorithms used in different blockchains. Also discussed various blockchain based applications that are covering numerous fields like financial services, reputation system, IOT so on. Furthermore, technical challenges of blockchain technology such as scalability of security problems waiting to be overcome and recent advances are briefly listed and possible future trends for blockchain.

III. BACKGROUND AND RELATED WORK

Software has evolved from a technology tool for solving specific problems to an industry that is omnipresent in most of today's corporate activities over the previous 60 years. Software engineering is defined as "the use of a systematic, disciplined, quantifiable methodology to the development, operation, and maintenance of software; that is, the application of engineering to software," according to IEEE Standard 610.12 [10]. The Software Engineering Body of Knowledge (SWEBOK) provides a complete description of the core SE Knowledge Areas (KAs) , which are also taken into account in this research. Software requirements, software process, software testing, software quality, software maintenance, software configuration management, and engineering management are examples of knowledge areas.

A few (optional) studies have audited the utilization of blockchain, e.g., applications and shrewd agreement improvement. One of the latest orderly planning concentrates on blockchain innovations was performed.. In this review the creators mean to distinguish and plan different spaces of exploration connected with blockchain and perceive potential headings for future examination. Additionally,it led a methodical writing audit of blockchain and savvy contract advancement. Specifically, the creators identified strategies, methods, apparatuses and challenges looked during the creation and testing of blockchain-arranged programming. Their examination recommends future exploration on the best way to adjust standard testing procedures to blockchain-arranged programming and how to gauge code measurements for code improvement. Both past investigations answer questions connected with the more extensive utilization of blockchain innovation, yet they don't analyze specifically its use in further developing SE exercises. To be sure, they didn't investigate the commitments that blockchain angles can bring to SE.Specifically, comparable to the use of blockchain to SE, to the best of our information, there give off an impression of being extremely restricted optional investigations. The more intently related study is a methodical planning study directed by Tariq and Colomo-Palacios]. This concentrate on wrote about the purposes of blockchain in programming and illustrated the benefits that this new innovation can bring to the SE field. The consequences of this study demonstrate that savvy contacts can computerize the verification of undertakings that normally require human-in-the circle. Shrewd agreements execute tests, produce results and naturally reward programming engineers. Also, blockchain can improve the trust between parties in rethinking programming improvement.

IV. CONCULISON

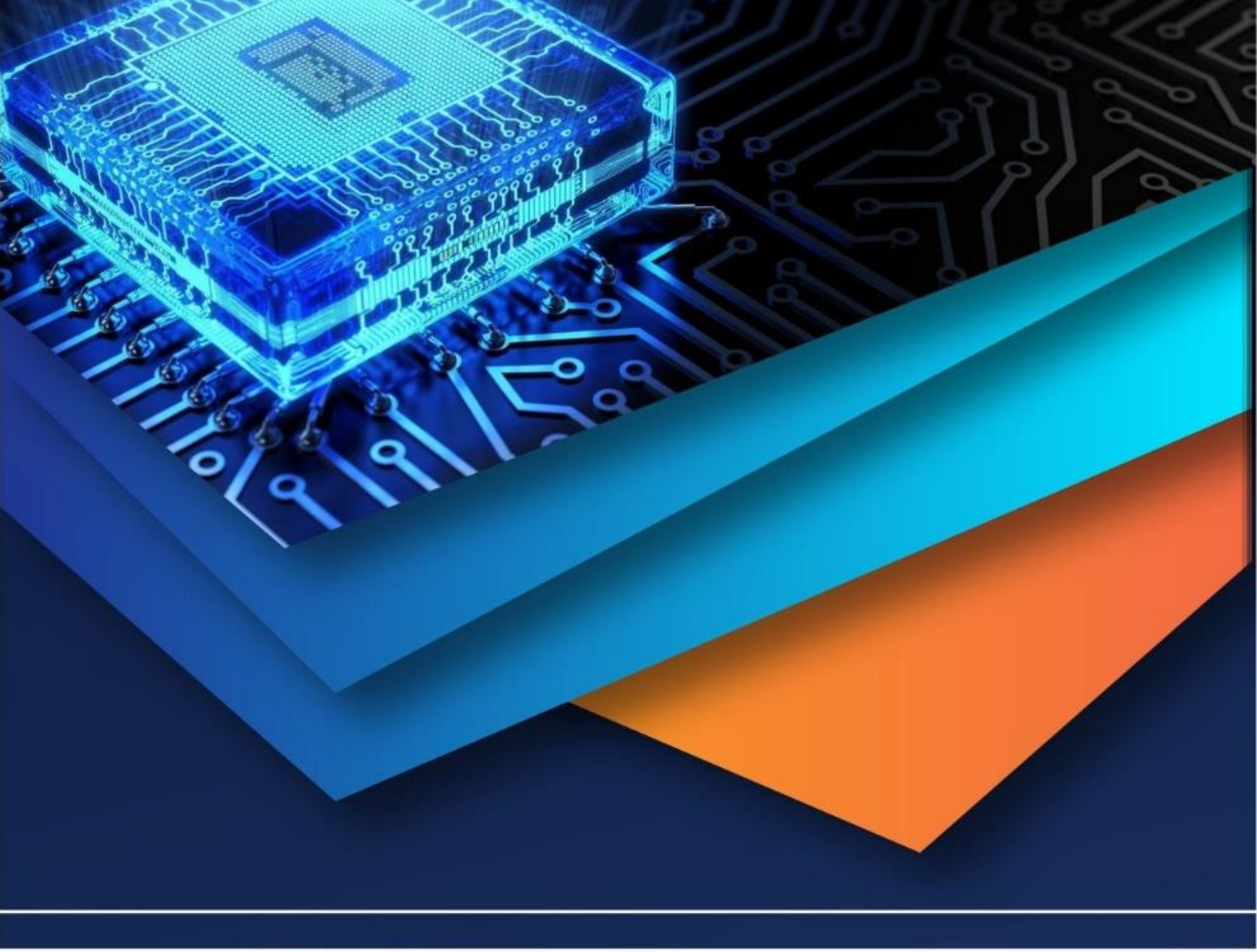
Blockchain is a powerful tool for resolving complex issues quickly. Its ability to provide security in an open environment makes it attractive for usage in a variety of other fields, including health care, IoT applications, and finance. E-commerce retailers and delivery partners can use consortium blockchains to avoid fraud during transit by continuously updating package positions on the blockchain. One of the most innovative potential uses of blockchain could be to avoid fraud in chit funds, which are used to save money in Indian society. It can also serve as a ledger for disadvantaged farmers to share resources. We give a state-of-the-art survey of blockchain technology in this study.

We began by discussing the background, classification, architecture, and several sorts of consensus.

Property	Public	Private	Federated
Consensus	• Costly PoW	• Light PoW	• Light PoW
Mechanism	• All miners	• Centralised organisation	• Leader node set
Identity	• (Pseudo) Anonymous	• Identified users	• Identified users
Anonymity	• Malicious?	• Trusted	• Trusted
Protocol & Efficiency	• Low efficiency	• High efficiency	• High efficiency
Consumption	• High energy	• Low energy	• Low energy
Immutability	• Almost impossible	• Collusion attacks	• Collusion attacks
Ownership &	• Public	• Centralised	• Semi-Centralised
Management	• Permissionless	• Permissioned whitelist	• Permissioned nodes
Transaction Approval	• Order of minutes	• Order of milliseconds	• Order of milliseconds

REFERENCES

[1] Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System." March 2009.
[2] Ridhanshi Bhatia, Praveen Kumar, Shilpi Bansal and Seema Rawat. "BLOCKCHAIN –THE TECHNOLOGY OF CRYPTO CURRENCIES." In ICACCE-2018.
[3] XIAO FAN LIU, XIN-JIAN JIANG2, SI-HAO LIU AND CHI KONG TSE. "Knowledge Discovery in Cryptocurrency Transactions: A Survey". In Digital Object Identifier 10.1109/ACCESS.2021.3062652.
[4] Vaibhav Shakya, PVGN Pavan Kumar, Lakshay Tewari and Pronika. "Blockchain based Cryptocurrency Scope in India." IEEE Xplore Part Number: CFP21K74-ART; ISBN: 978-0-7381-1327-2. (ICICCS 2021)
[5] FAIJAN AKHTAR, JIAN PING LI, MD BELAL BIN HEYAT, SYED LUQMAN QUADRI, SHAIK SOHAIL AHMED, XIAO YUN, AMIN UL HAQ. "POTENTIAL OF BLOCKCHAIN TECHNOLOGY IN DIGITAL CURRENCY: A REVIEW." 978-1-7281-4242-5/19/$31.00 ©2019 IEEE.
[6] Suman Ghimire and Dr. Henry Selvaraj. "A Survey on Bitcoin Cryptocurrency and its Mining." 978-1-5386-7834-3/18/$31.00 ©2018 IEEE.
[7] Ujan Mukhopadhyay, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu and Richard Brooks. "A Brief Survey of Cryptocurrency Systems." white paper 2016.
[8] Jae Min Kim, Jae Won Lee, Kyungsoo Lee and Junho Huh. "Proof of Phone:A Low-cost Blockchain Platform" Self-published.
[9] Yong Yuan and Fei-Yue Wang. "Blockchain and Cryptocurrencies: Model, Techniques, and Applications" 2168-2216-2018 IEEE.
[10] Wenzheng Li and Mingsheng He. "Comparative Analysis of Bitcoin, Ethereum, and Libra" 978-1-7281-6579-0/20/$31.00©2020 IEEE.
[11] Antea Knezevic, Zvonimir Musa and Tihana Babic. "Cryptocurrency as the currency of the future: a case study among ALgebra University College students." MIPRO 2020, September 28 - October 02, 2020, Opatija, Croatia.
[12] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten. "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies" 2015 IEEE Symposium on Security and Privacy. DOI 10.1109/SP.2015.14.
[13] Dr. R. Raju, M. SaiVignesh and K. Infant Arun Prasad. "A Study of Current Cryptocurrency Systems" In 2018 INTERNATIONAL CONFERENCE ON COMPUTATION OF POWER, ENERGY, INFORMATION AND COMMUNICATION (ICCPEIC). 978-1-5386-2447-0/18/$31.00 ©2018 IEEE.
[14] CHANDRAMOULI SUBRAMANIAN,ASHA A GEORGE,ABHILASH K A AND MEENA KARTHIKEYAN.”BLOCKCHAIN TECHNOLOGY BOOK”.
[15] ”ONLINE PAYMENT USING BLOCKCHAIN” RESEARCH PAPER.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY