iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.42442

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 10 Issue V May 2022- Available at www.ijraset.com

Survey Paper on Communication System Using Blockchain and Cryptography

Prof. Shivaji Vasekar[1], Akash Adhav[2], Anirudha Adekar[3], Kshitij Kanake[4], Shubham Gondhali[5]

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 a ledger which allows messaging to take place in a decentralized manner. Decentralized application for the communication and resource sharing is need in today's world, where keeping data on a centralized server can be risky and a very expensive experience. With the help of some consensus, we can implement different ways to share resources and communicate. Together with Blockchain and Decentralized Applications, we can create a secure and very reliable messaging application that overcomes the drawbacks of traditional messaging applications.***
Keywords: Blockchain, Cryptography, Communication System, Secure Hash Algorithm, Encryption and Decryption

I. INTRODUCTION

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 stores 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. 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 to view as a very secure encryption and hashing functions(256 bits) are used. Also if a hacker tries to make changes to the information in block then, they will have to make changes to all the copies of that block on whole blockchain network and that can be quite impossible.

II. OBJECTIVE

To develop more secure and transparent communication System.
To provide more efficient system that works even if a node in the network fails. To provide more secure environment for chatting.

III. RELATED WORK

Blockchain technology started to be used before enough academic studies show the way for better solutions and standardization. The development has been conducted mostly out of the academia.
Communication applications that aim to satisfy the data security concern are started to be developed. These applications are using asymmetric ciphers, consensus algorithms and blockchain technology. Decentralized messaging nodes use P2P network for connection. There are applications like filecoin (https://filecoin.io), (https://www.uport.me), ujomusic (https://ujomusic.com) which use IPFS and blockchain, but they are not used for communication. In order to increase communication safety, there are also some academic studies. In a recent study, multi-link concurrent communication model based on trust degree and novel integrated factor communication tree (IFT) algorithm are proposed to improve reliability. It is shown that, a routing scheme based on the IFT algorithm for the communication of the blockchain can increase communication efficiency by ensuring the reliability. Even E-chat and CrypViser seem to be communication applications, it seems that sending crypto coins is the main purpose.
To our knowledge, an academic study about this topic and an open source communication application which uses Communication System using blockchain and cryptography was not proposed or implemented before. This system will aim solutions.

IV. PROBLEM STATEMENT

The systems we currently use have a centralized approach to resource sharing and communication. Here, all the data is stored on a centralized server. This may lead to loss of data if the server collapses. Also, there are countless counterfeit information and product publishing on social networking without any known root transgressor (like on WhatsApp, hike). The information shared can be hacked which is stored on the centralized server.

V. SCOPE

To develop software that can provide not only the features provided by currently available chat applications but also be able to overcome the drawbacks that they have. The resultant software will be more secure and reliable than the currently available ones.

VI. PROPOSED SYSTEM

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 to view 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 block are on all nodes, they cannot access the information in it, only the person for whom the information if can access it.Hashing Algorithm:
We are using SHA-256 Algorithm because its secure and and trusted industry standard. The collision while generating hash value are incredibly unlikely and avalanche effect which states that slight change in the input makes a large difference in output.

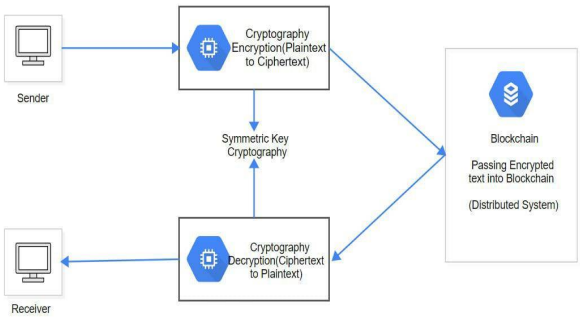
A. Cryptography Algorithm

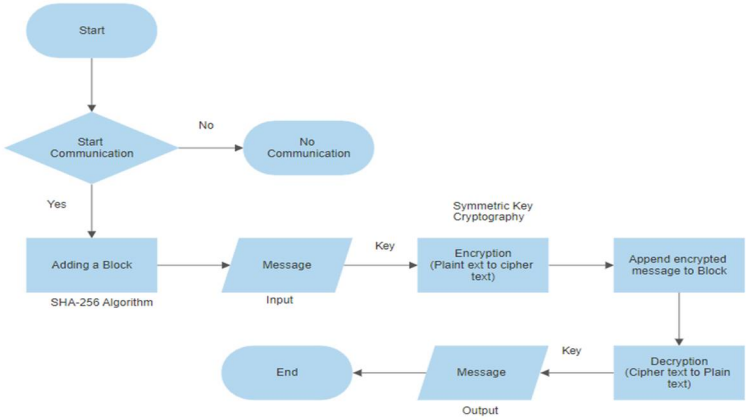
Cryptography is a method of developing techniques and protocols to prevent a third part from accesing and gaining knowledge of the data from the private messages during a communication process.

B. AES Algorithm

The AES algorithm (also known as the Rijndael algorithm) is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits. Since the AES algorithm is considered secure, it is in the worldwide standard.

VII. SYSTEM ARCHITECTURE





A. Advantages

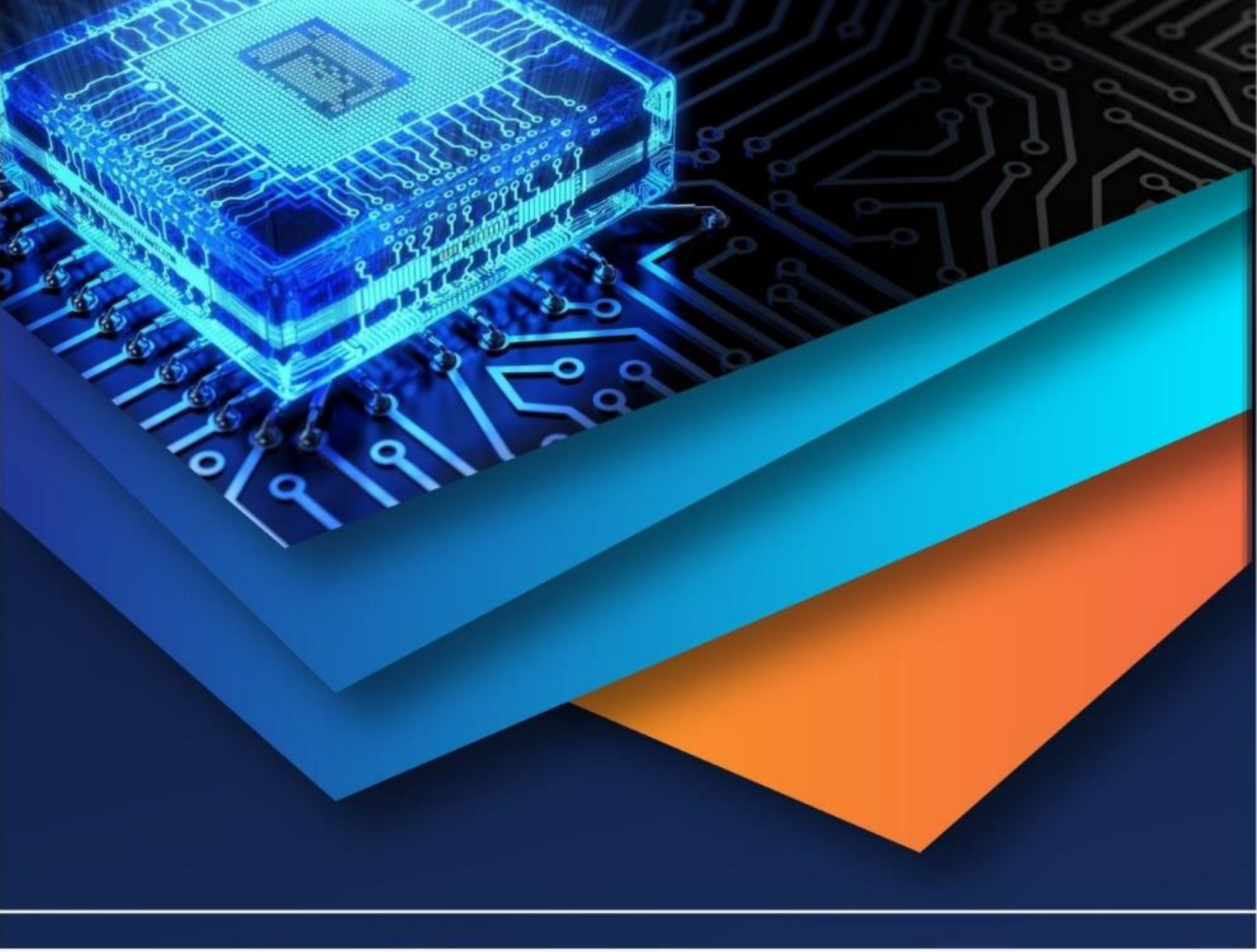
1) *Immutability:* Since records are stored on a large number of participants, it is nearly impossible to tamper transactions in a public blockchain.
2) *Efficiency:* It takes plenty of time to propagate transactions and blocks as there are a large number of nodes on public blockchain network.
3) *Decentralization:* Consensus algorithms in blockchain are used to maintain data consistency in decentralized network.

VIII. CONCLUSION AND FUTURE WORK

In this project, we are developing an application that makes use of blockchain in a very efficient way. Blockchain has shown its potential for transforming traditional industry. Also, by eliminating the centralized approach, we can assure the safety and availability of data and communication. Decentralized applications tend to make the interaction between two people more efficient and simple. The chatting process nowadays have a mediating node, while our software does not have any mediating device/node i.e., every person is connected by peer-to-peer network.

REFERENCES

[1] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, ―An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends‖, 2017 IEEE 6th International Congress on Big Data.
[2] S. Nakamoto, ―Bitcoin: A peer-to-peer electronic cash system,‖ 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[3] G. W. Peters, E. Panayi, and A. Chapelle, ―Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective,‖ 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn. 2646618
[4] G. Foroglou and A.-L. Tsilidou, ―Further applications of the blockchain,‖ 2015.
[5] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, ―Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,‖ in Proceedings of IEEE Symposium on security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.
[6] Technical White Paper: WhatsApp Encryption Overview,http://www.cdn.whatsapp.net/security/WhatsApp-Security- Whitepaper.pd, Accessed on 23-02-2021.
[7] P. Rosler, C. Mainka and J. Schwenk, "More is less: On the end-to-end security of group chats in Signal, WhatsApp, and Threema", IEEE European Symposium on Security and Privacy (EuroS&P), pp. 415-429.
[8] https://faq.whatsapp.com/general/security-and-privacy/were-updating-our-terms-and-privacy-policy/, Accessed on 09-03-2021.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY