iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50702

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 IV Apr 2023- Available at www.ijraset.com

Blockchain and Cryptography Communication System

J. Guru Lakshmi[1], K. Sai Ramya[2], G. Swapna[3], D. Thanmayi[4], K. Chandana[5], T. Sai Lakshmi[6]
[1, 2, 3, 4, 5]*Department of Computer Science and Engineering, BWEC, Andhra Pradesh, India*
[6]*M.Tech (Asst.Professor)*

Abstract: ***Blockchain is an innovative technology that overcomes these threats, allowing sensitive operations to be decentralized while maintaining a high level of security. Eliminate the need for trusted intermediaries. The blockchain is accessible to network nodes and keeps track of all transactions that have taken place. The goal of our work is to offer a secure communication solution based on blockchain technology. In this project, we explain why blockchain should secure communications and offer a blockchain-based messaging design pattern that maintains the performance and security of data stored on the blockchain by using a smart contract to protect identity and associated verify public key and validate a user certificate. The system is entirely a combination of blockchain and cryptography for communication systems.***
Keywords: Blockchain, Cryptosystem, Encryption Standards, Software Defined Network, Security, Privacy.

I. INTRODUCTION

Cryptocurrency, a type of low-privacy technology, is a well-known factor in today's technology space. Because it is entirely based on cryptographic techniques. It is a distributed/decentralized technique that follows consensus rules and maintains an immutable ledger for storing transaction history. Blockchain data is pre-stored in a ledger divided into blocks, each containing hash data and transaction details. Each block in the blockchain system is connected to the next in the form of blocks, making data manipulation virtually impossible. Few arbitrage algorithms examine and verify data on all transactions en bloc, ensuring that each event is accurate and true. Distributed ledger technology facilitates decentralization by allowing people to work together in a decentralized network. There are almost no security vulnerabilities since the activity log would have to be modified by a single user. However, blockchain and similar platforms have serious security problems. Who can participate in blockchain networks and who has access to data can vary.Public or private networks are often referred to as public or private, which indicates who can access it, and authorized or unauthorized, which indicates how users access the network. Blockchain is a distributed ledger that resembles a linked list data structure format. However, the blockchain is distributed while linked lists are pointer-oriented. Software-defined networking (SDN) is the new trend in network architecture that is dynamic, controllable, cost-effective and flexible, making the ideal for today's real-time, high-bandwidth applications. The controller handles network control and forwarding, chooses the shortest path in the event of a network node failure, and allows direct programming of network management and abstraction of the underlying infrastructure for apps and services. The OpenFlow protocol is a key element in the development of SDN solutions. Two types of encryption are used in today's world: homogeneous encryption and asymmetric encryption. This term comes from the fact that the identifier is used for both encryption and decryption. DES, AES and RSA are the three main types of encryption. While there are other types of encryption that do more than can easily be explained, we'll focus on the three most common types of encryption used by customers. According to the study, we try to illustrate how blockchain plays an important role in the modern network environment. the use of SDN and the security role that this network plays in terms of privacy and security. What role does the DES algorithm play in SDN? It is used to determine how the node is failing and to trace the attack.

1) *Objective:* Development of a safer and more transparent communication system. Deploy a more efficient system that works even if a network node fails. To provide a safer chat environment.
2) *Existing System:* As we all know, traditional chat apps are centralized; H. all data is stored on a central server. Therefore, the main problem with this structure is that if the central server fails, the entire network collapses. For example WhatsApp server stores all data on central server, if this server gets destroyed user data may be lost or user information stored on server may be leaked as well. To overcome this, our project uses a decentralized application approach. In our application, all user data is stored in a block that is linked to other blocks in a chain.

3) *Proposed System:* In our application, all user data is stored in one block, which is connected to other blocks in a chain. As the name suggests, a decentralized application does not have a central server.It's essentially a peer-to-peer network. In addition, the data stored in the block can hardly be viewed, since very secure (256-bit) encryption and hash functions are used. If a hacker tries to change a block's information, they have to make changes to all copies of that block across the blockchain network, which can be downright impossible. Although blocks are on all nodes, they cannot access the information they contain, only the person to whom the information relates can access it. selections.

II. LITERATURE REVIEW

We attempt to offer a comprehensive review of all current modern research trends that have been conducted to evaluate the performance of blockchain technology in conjunction with various cryptosystem standards in the network area and other models below.

Manisha Nehe et al [1] proposes the major concerns about information security are identity, privacy, and exchange security. Data transparency, intensification of change, and fine-grained access to data information are all important features of block-chain technology, which is designed for data operational businesses that deal with vast amounts of sensitive data and are subject to frequent hacker attacks. This strategy allows for the adoption of a new blockchain architecture since data will be accessed by private and public key users, while network access will be improved through authorised keys based on the blockchain hash value.

Dr. V. Suma et al [2] since blockchain is a foundation technology, it draws a wide range of APIs that help to ensure secure data transactions across the network. The study also discusses how to use block chain to prevent misuse and corruption in the exchange of large amounts of data generated by the legislature, safety, legislation, and business software databases, among other things. Using the block chain and the RSA digital signature mechanism, the proposed system provides dependability and trust in data exchange in communication channels.

Sergey Semushin et al [3] illustrate how a wireless sensor network is an essential component of a system's architecture. Because IoT devices are inherently lowpowered and have limited resources, choosing the right encryption technique for WSN communication is critical. In this study, we examine various symmetric block-based cryptographic algorithms to remark on their capabilities, assisting in the selection of the best approach for a given application.With varying block and key lengths, we chose commonly used algorithms such as AES, DES, Triple DES, IDEA. The comparison is based on energy consumption, power consumption, memory utilisation, and throughput.

Saifullah Khan et al [4] Private/confidential data can be stored in a secure manner utilising blockchain technology. Data legitimacy, concealment, authentication, and identification can all be improved by combining encryption methods with a consensus algorithm with associated hash values. Using these two algorithm standards helps to keep data safe and secure while also protecting it from intruders and predators.

A lot of data relating to health records is maintained and transmitted on the cloud, according to Dhananjay Yadav et al [5]. To gain patients' belief, data transmitted between patients and doctors must be secure. Blockchain is a method for securing data in a more advanced manner. The blockchain divides data into bits that are difficult to decrypt, adding an added degree of security. The primary goal of this article is to provide secure and reliable storage of patient data in an effective manner.

III. SYSTEM MODEL

In order to provide a comprehensive understanding of the techniques and research, we provide a brief overview of the important scientific terms utilised in these selected survey papers in this part.

A. Blockchain Technology

Bitcoin is a system for storing data that makes it difficult or hard to change, corrupt, or deceive. A blockchain is a distributed record track of actions that have been duplicated and disseminated all over the number of distributed servers that make up the blockchain. Simply said, blockchain technology is a decentralised, distributed ledger that tracks the ownership of various content. The data on a blockchain can't be changed by nature, making it a real disruptor in industries like transactions, information security, and medicine. Blockchain is a superior, secure visual representation of events and authorized users updated even while preserving the past. We get a statistical data trace as well as a promptly right-up record, and the content can't be altered or unintentionally erased. Blockchain is the technology that allows cryptocurrencies to exist (among several other things). A Bitcoin, like the US dollar, is a virtual form of currency that uses encryption skills to regulate the generation of national currencies and authenticate the transmission of payments.

B. Cryptography

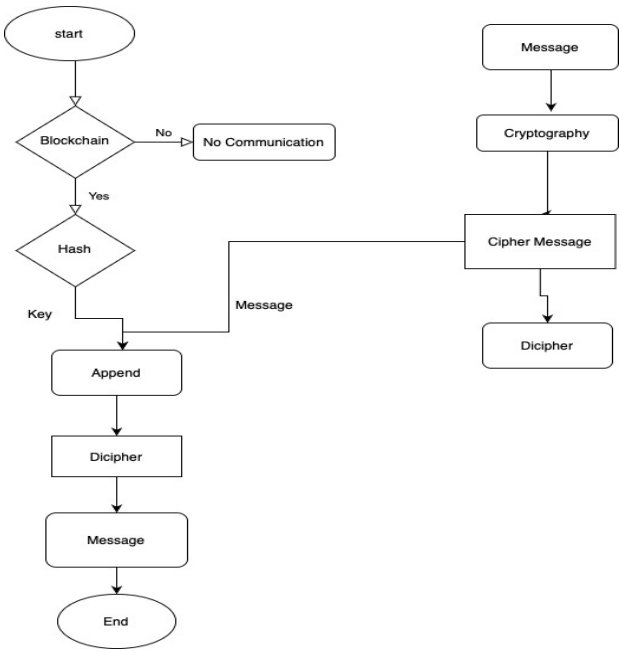
The research into encrypted communications techniques that allow only the transmitter and intended destination of a document to read its contents is known as cryptography. Encrypting and decrypting email and other pure messages is perhaps the most prevalent usage of cryptography when transporting electronic data.Kryptos and logos are the two components of cryptology. Verification, information validation such as privacy and integrity, non-repudiation of authenticity, and anonymity are the key objectives of cryptosystems, which have two components: encoding and decoding. Secret-key encryption, public-key encryption, and hash function encryption are the three forms of cryptographic algorithms.

1) *Data Encryption Standard (DES):* DES is an encryption algorithm that secures files in form of blocks. This implies that data of each of 64 bits of plain text are fed into DES, which generates entire bits of encrypted data. Encrypt and decrypt employ certain techniques and information, with slight variations. The key is 56 bits long. Encrypting sets of 64 cipher text, or 16 hexa integers, is how DES works. DES uses "values" that are purportedly 16 hexadecimal values long, or 64 bits. In contrast, the DES algorithm eliminates each 8th key bit, culminating in a block cipher of 56 bits.
2) *Advanced Encryption Standard (AES):* AES is a secure method that encrypts and decrypts using the same 128, 192, or 256-bit key (the security of an AES system increases exponentially with key length). To examine AES's overall structure, with a focus on the four procedures utilised in each round: (1) byte replacement, (2) shifting rows, (3) mixing columns, and (4) adding round keys.

C. Ceaser Cipher Model

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet.

D. Architecture



E. Modules

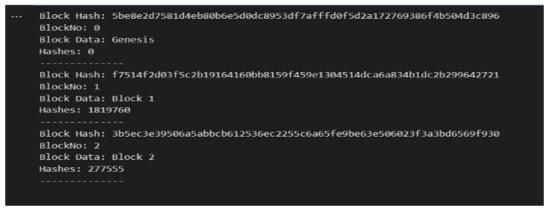
1) *Hashlib:* The Hashlib module provides a utility function to efficiently hash a file or file-like object.
2) *Datetime:* Datetime is a combination of date and time. The attributes of this class are similar to date and separate classes.These attributes include day, month, year, minute, second, microsecond, hour.
3) *RSA:* RSA encryption, Rivest-Shamir-Adelman full encryption, a type of public-key cryptography widely used to encrypt email data and other digital transactions on the Internet.
4) *ECDSA:* ECDSA stands for Elliptic Curve Digital Signature Algorithm, it is used to create a digital signature of data to verify its authenticity without compromising its security.

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 IV Apr 2023- Available at www.ijraset.com

IV. RESULTS AND ANALYSIS

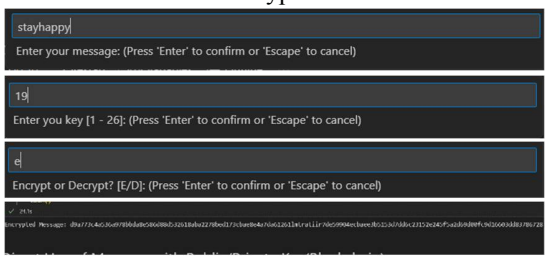
1) Cryptographic Hash Functions

2) Blockchain_Process

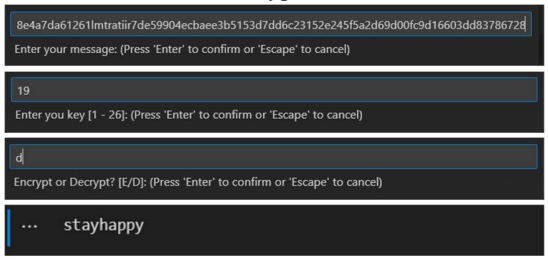


3) Cryptography Process

Encryption



Decryption



4) Public/Private Key Cryptography

5) Decrypted Message

6) Digital Signatures

V. CONCLUSION

The following findings can be drawn based on a bibliographic evaluation of several research articles and the criteria addressed. The various encryption algorithms of cryptography are prone to data loss, according to many Researchers in the field of distributed ledger technology, as well as the organisation in charge of SDN.

This article provides a detailed examination and comparison of the existing research. Existing solutions have been grouped based on different ways of resolving the congestion issue.

1) Use of SDN network enhancements is the executive summary for congestion problem solutions.

2) Using the most secure and simple algorithms possible.Some studies have proposed a hybrid technique that incorporates all of the above-mentioned solutions. However, a state-of-the-art solution to this problem is required in order to optimise software defined network use and reduce congestion.

VI. FUTURE SCOPE

For future, We can replace the encryption techniques with encryption algorithms like triple DES,RSA security, Blowfish, etc.

REFERENCES

[1] Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system. Consulted., 165: 55-61.
[2] Zhu, Y., Gan, G.H., Deng, D. (2016) Security Research in Key Technologies of Blockchain Information Security Research., 12: 1090-1097.
[3] Liu, X.F. (2017) Research on blockchain performance improvement of Byzantine fault-tolerant consensus algorithm based on dynamic authorization. Zhejiang University.
[4] Wang, X., Lai, X., Feng, D. (2005) Cryptanalysis of the Hash Functions MD4 and RIPEMD. Advances in Eurocrypt., 3494: 1-18.
[5] Shen, Y., Wang, G. (2017) Improved preimage attacks on RIPEMD-160 and SHA-160. Ksii Transactions on Internet & Information Systems., 12: 727-746.
[6] Wang, H.Q., Wu, T. (2017) Cryptography in Blockchain. Journal of Nanjing University of Posts and Telecommunications., 37: 61-67.
[7] Yuan, Y., Wang, F. (2016) Current Status and Prospects of Blockchain Technology Development. Acta Automatica Sinica., 42: 481-494.
[8] Miyaji, A. (1994) Elliptic Curves Suitable for Cryptosystems. Ieice Transactions on Fundamentals of Electronics Communications & Computer Sciences., 77: 98-105.
[9] He, P., Yu, G., Zhang, Y.F. (2017) Prospective review of blockchain technology and application Computer Science., 44: 1-7.
[10] Zhai, S.P., Li, Z.Z. (2018) The data block chain of the key technologies Consistency. Computer Technology and Development., 8: 1-6.
[11] An, Q.W. (2017) Research and application of key technologies for decentralized transactions based on blockchain. Donghua University.

Bibliography

Mrs.T.Sai Lakshmi, M.Tech,Asst. Professor, Dept of CSE,BWEC, Andhra Pradesh, India.

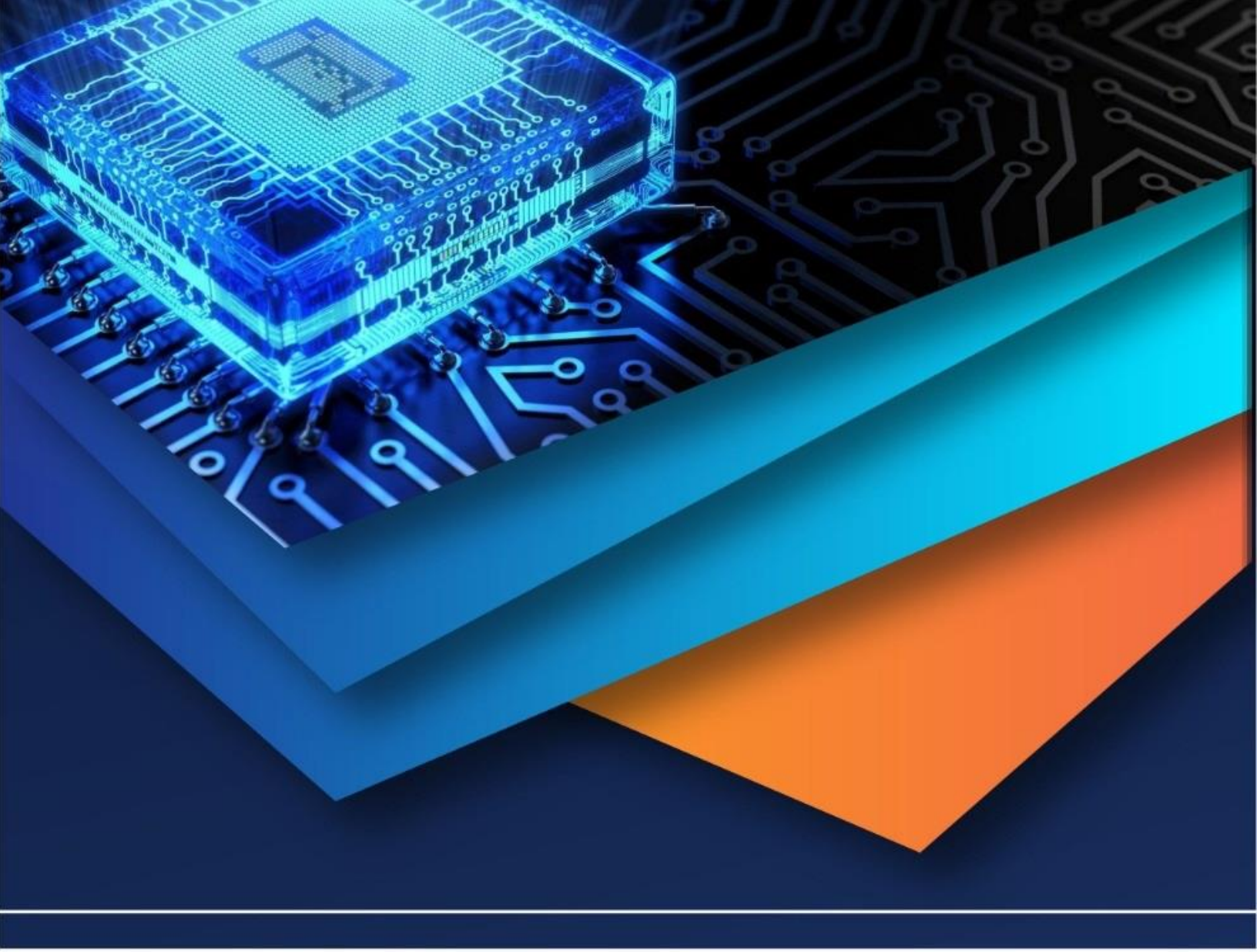
J. Guru Lakshmi (B.Tech), student, Dept of CSE, BWEC, Andhra Pradesh, India.

K.SaiRamya(B.Tech), student, Dept of CSE, BWEC, Andhra Pradesh, India

G.Swapna(B.Tech), student, Dept of CSE, BWEC, Andhra Pradesh, India

D.Thanmayi(B.Tech), student, Dept of CSE, BWEC, Andhra Pradesh, India

K.Chandana(B.Tech), student, Dept of CSE, BWEC, Andhra Pradesh, India



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY