WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

CHATIFY : Communication System using Blockchain and Cryptography

Varuni Kulkarni, Shivani Mishra, Pragati Nawadkar, Prof.Kumud Wasnik

Computer Science And Technology Usha Mittal Institute Of Technology Mumbai, India

ABSTRACT:

Blockchain is one of advance technology that helps overcomes various threats, making it possible for crucial oper- ations to get decentralised while helping us keep things quite safe. This paper proposes a novel approach for building a secure communication system by integrating blockchain tech- nology and advanced cryptographic techniques. The aim is to improve performance by replacing existing encryption techniques with encryption algorithms like AES and Keccak-256 security. Researchers in the field of distributed ledger technology and SDN organisations have focus on various encryption algorithms in cryptography are vulnerable to data loss, the integration of blockchain and cryptography for secure communication not only addresses current challenges but also anticipates future threats, making it a dynamic and forward-looking field of research and application. The project includes a comprehensive examination and comparison of existing research in this area. The solutions proposed by previous studies have been categorised based on different approaches to resolving congestion issues. The first approach is the utilisation of SDN network enhancements, which is summarised in the executive summary of congestion problem solutions.The second approach involves employing the most secure and simple algorithms possible.These solutions have demonstrated promising outcomes in terms of security and robustness, primarily due to their high capacity. Furthermore, we also talk about how to set up our system and the problems we might face when doing it. Through this research, we aim to help make communication safer, so networks can be stronger and more trustworthy in the future.

Keywords: Blockchain, Cryptography, Keccak256, AES

INTRODUCTION

Decentralized apps use direct connections between users, so if one computer fails, it doesn't collapses the whole system. Cryptocurrency, which lacks privacy, is a big deal in today's tech world. It is distributed/decentralised technique that adheres 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 sequence of blocks, making data manipulation virtually next to impossible. The OpenFlow protocol is a key factor in the development of SDN(Software- defined networking) solutions. Two types of encryption are used in today's world: homogeneous encryption and asymmet- ric encryption. This term comes from the fact that identifier is used for both encryption and decryption. DES, AES and RSA are the three main types of encryption algorithms. In today's digital world, ensuring secure and trustworthy communication channels is essential. However, traditional methods often strug- gle to offer strong security against different risks like data breaches, unauthorized entry, and tampering. To address these challenges, there is a need for a decentralized communication system that utilizes the power of blockchain technology and cryptography. With our decentralized system, the data would be stored on multiple nodes, so it would be much less likely to be lost in the event of a server failure. But with decentralized system, Each message would be timestamped and signed with a digital signature, making it possible to trace the source of any message. Additionally, cryptographic techniques such as asymmetric encryption, digital signatures, and hash functions should be employed to secure the communication channels and protect sensitive information from unauthorized access and tampering. We believe that our proposed system would be a valuable contribution to the field of secure communication. It would provide a more secure, private, transparent, scalable, and efficient way for people to communicate.

This Paper consist of below contents:

II. Existing System,
III. Proposed System,
IV. Literature Survey,
V. Methodology,
VI. Result and Analysis,
VII. Conclusion
VIII. Future Scope,

Reference

EXISTING SYSTEM

In contrast to conventional centralized chat applications, where all data resides on a central server, this system adopts a decentralized application model. In this innovative approach, user data is stored in blocks linked together in a chain, mitigating the risk of a network collapse in the event of server failure or data breaches. Within the existing system, a crucial role is played by the smart contract, which facilitates and executes agreements among users in the network. This contract, generated through blockchain-based code, validates individuals' certificates based on agreements endorsed by network nodes. Before enabling message exchange, the smart contract conducts essential checks. It initially verifies the identity and associated public key, both pre-stored on the blockchain. The primary goal of this approach is to establish secure communication between network entities. Users must exclusively communicate with identities validated by the smart contract, treating any other interactions as potentially malicious. To utilize the system for communication, users need to register their identity and associated public key, with this information securely stored on the blockchain. Additionally, the system ensures data integrity and immutability, transparent and auditable transactions, resilience to DDoS attacks, enhanced privacy and security, scalability and efficiency, community governance, consensus mechanisms, and interoperability and integration. These features collectively make the system well-suited for providing secure and resilient communication solutions in various contexts..

PROPOSED SYSTEM

In this project, user data is securely stored in interconnected blocks forming a decentralized application, eliminating the need for a central server and creating a peer-to-peer network. The data within these blocks is highly secure, employing ro- bust 256-bit encryption and hash functions. Attempting to alter information within a block becomes an incredibly challenging task for hackers, as changes would need to be made across all copies of that block throughout the blockchain network. Furthermore, even though blocks exist on all nodes, access to the contained information is restricted to the respective individual associated with that data. The implementation of the Advanced Encryption Standard (AES) algorithm enhances both security and speed, surpassing the Data Encryption Standard (DES) algorithm. In the existing system, Public Key Infrastructure (PKI) and asymmetric key cryptography introduce computational complexity, key management issues, varying key sizes, performance degradation, and susceptibility to man-in-the-middle attacks. In this proposed system, on the other hand, leverages the AES and Keccak-256 algorithms, along with symmetric key cryptography. This strategic choice contributes to increased speed, efficiency, low computational requirements, simplicity, scalability, proven security, reduced key management complexities, offline capabilities, and im- proved compatibility.

System Architecture

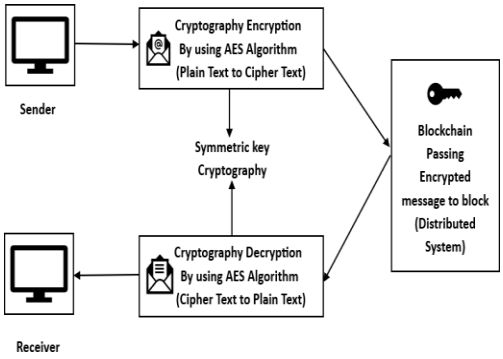

Fig. 1. Architecture Overview of Communication System using Blockchain and Cryptography

Image source: "Survey Paper on Communication System Using Blockchain and Cryptography" by Prof. Shivaji Vasekar, Akash Adhav, Anirudha Adekar, Kshitij Kanake, Shubham Gondhali.

Flowchart

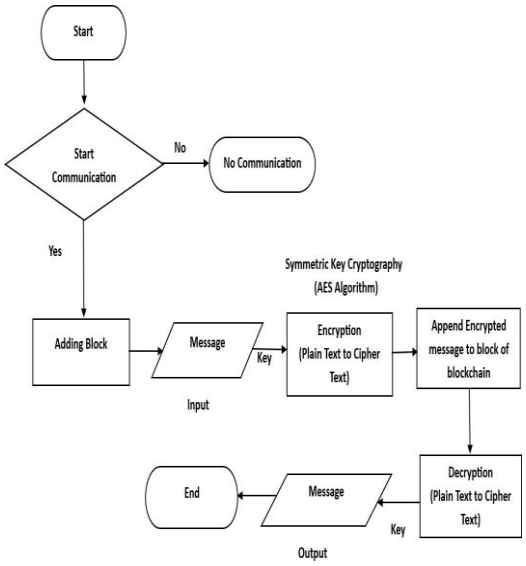

Fig. 2. Flowchart of Communication System using Blockchain and Cryptography

Image source: ”Survey Paper on Communication System Using Blockchain and Cryptography” by Prof. Shivaji Vasekar, Akash Adhav, Anirudha Adekar, Kshitij Kanake, Shubham Gondhali.

LITERATURE SURVEY

This table consist of all papers that we have referred for reference

Authors	Paper name &year	Advantage	Disadvantage	Observations
Prof. Shivaji Vasekar, Akash Adhav, AnirudhaAdekar, Kshitij Kanake, ShubhamGondhali	Survey Paper on ommu-nication system using lockchain and Cryp-tography, 2022	Immutability, Decentral- ization, peer-to-peer nature of blockchain ensures that there is nosingle pointof failure,enhancing system resilience.	Energy con-sumption: substantial ompu- tational power is needed tomaintain their security andconsensus mecha- nisms.	This project has the powerto transform the traditional industry. Also, byeliminating centralizationin networking, it helps toimprove thesecurity.
Aqsa Rashid, Asif Masood, Haider Abbas, Yin Zang	Blockchain-based public key infrastruc-ture 2021	Peer-to-peer network,Great accuracy	Regulatory and legal consid- erations, Chances ofhuman errorand com-putational error	All user transaction information is recorded on the blockchain, which has strict securitystandards.
Elias Ghribi, Tala Talaei Khoei, Hamed Taheri Gorji, Prakash Ran-ganathan,Naima Kaabuch	A Secure Blockchain-based Commu-nication Approach for UAV Networks, 2020	Integrity and authenticity, Decentral-ized system,Cryp-tography techniques, uch as digital signatures, ensure theintegrity and authenticity.	Complexity, Dependenceon network connectiv- ity, system’s reliance onnetwork onnectivitymay pose challenges in environ-ments withunreliable.	DES Algorithm is slow and time-consuming compared to AES algorithm. Using PKI and DESalgorithm forsmart contract transactions.
Kahina Kharef,Guy Pujolle	Secure Peer- to-Peer Commu-ication based on Blockchain, 2019	Confidentiality Message Integrity and Au-thentication, Reliability	Smart contract execution affects per-formance negatively, Scaling issues	Shows the immutability of blockchain to provide a solution to high problematics in the fieldof centralizedPKI.

Authors	Paper name &year	Advantage	Disadvantage	Observations
J Guru Lakshmi, SaiRamya, G. Swapna, D. Than-mayi, K. Chandana, T. Sai Lakshmi	Blockchain based Secure Commu-nication Appli- cation Proposal: Crytotch,2018	Decentralized applications,Great accuracy, Trans-parency, Enhanced privacy andconfidential-ity	Scalability issues, Irreversible transactions	DES algorithmsecures files in blocks, RSAalgorithm isasymmetric cryptography.

TABLE I
LITERATURE SURVEY COMMUNICATION SYSTEM USING BLOCKCHAIN AND CRYPTOGRAPHY

METHODOLOGY

In this project we are using two major cryptographic algo- rithms :

Advanced Encryption Standard (AES):

AES, or Advanced Encryption Standard, functions as a sym- metric encryption algorithm designed to safeguard data using a key, working on 128-bit data blocks. The encryption process involves key expansion, where round keys are generated from the encryption key. Subsequent rounds, typically 10 for AES- 128, include operations like SubBytes, which replaces bytes using a substitution table, ShiftRows for rearranging block data, MixColumns (except in the final round) to mix data within columns, and AddRoundKey, which XORs the round key with the block. The final round skips the MixColumns step, resulting in the ciphertext—an encrypted version of the plaintext. Decryption involves performing inverse operations using the same key.

Keccak-256:

Keccak-256, a cryptographic function in the SHA-3 Family and utilized in Solidity, computes a hash of fixed-length output from any number of inputs. It operates in a one-way direction, and its hash cannot be reversed. When a string like ”Hello World” undergoes the keccak256 hashing function, it produces a unique 32-byte hash. Even minor alterations to the input string, such as capitalization changes, yield entirely different hash digests. This consistency in producing the same outcome regardless of input size or modifications makes Keccak-256 valuable in various applications.

RESULTS AND ANALYSIS

In the context of distributed databases, the blockchain serves as a ledger where all user transaction data is meticulously recorded. Functioning as a decentralized peer-to-peer network, the blockchain lacks a central authority, with data being distributed across multiple nodes. Upon starting into the blockchain, each transaction is encapsulated within a block, accompanied by essential metadata including a block number, transaction data, and a cryptographic hash value computed based on the block’s contents. The major algorithms being used here are AES and Keccak-256 which is advanced version of SHA family.

Using Advance Encryption Standard(AES) algorithm within a secure communication system utilizing cryptography and blockchain technology, the process unfolds as follows. Ini- tially, a symmetric encryption key is generated to ensure confidentiality during message transmission. This key serves as the foundation for encrypting the message using the Ad- vanced Encryption Standard (AES). The encrypted message is then packaged into a blockchain transaction, leveraging the immutable and decentralized nature of the blockchain to ensure secure transmission. Subsequently, network nodes validate the transaction to uphold the integrity and authenticity of the communication. Finally, upon receipt, the recipient retrieves the encrypted message from the blockchain and decrypts it using their private key, paired with AES decryption, thus enabling access to the original content.

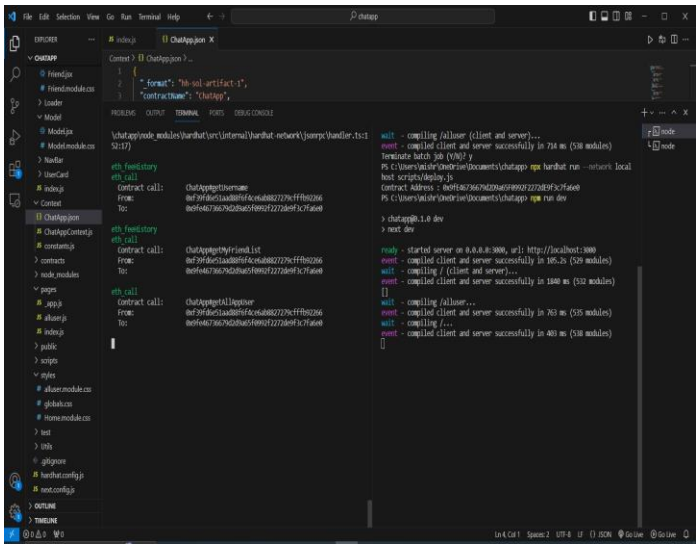

Fig. 3. Backend Output of communication System using Blockchain and Cryptography

This cohesive ap- proach guarantees end-to-end security, blending cryptographic principles with blockchain's distributed ledger technology to safeguard communication channels effectively.

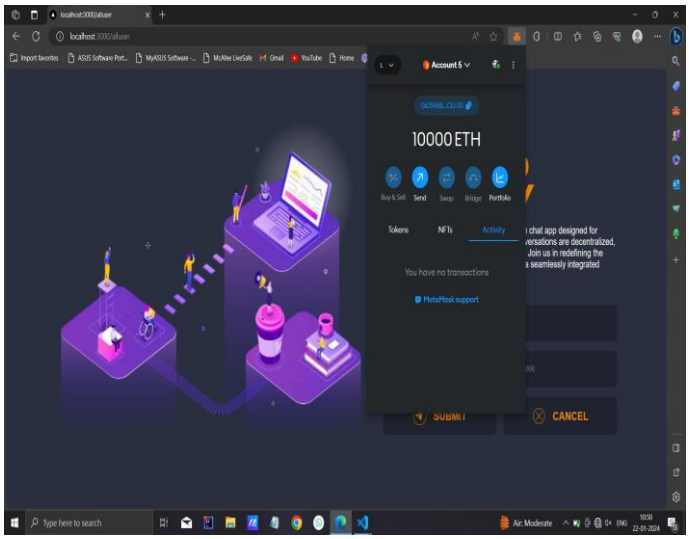

Fig. 4. Result of connectivity of ommunication System using Blockchain and Cryptography

CONCLUSION

This project focuses on addressing the security of digital data communication across networks using blockchain and cryptography.The aim is to improve performance by replacing existing encryption techniques with encryption algorithms like AES and Keccak-256 security.Researchers in the field of distributed ledger technology and SDN organisations have focus on various encryption algorithms in cryptography are vulnerable to data loss.the integration of blockchain and cryptography for secure communication not only addresses current challenges but also anticipates future threats, making it a dynamic and forward-looking field of research and appli- cation.The project includes a comprehensive examination and comparison of existing research in this area. The solutions proposed by previous studies have been categorised based on different approaches to resolving congestion issues. The first approach is the utilisation of SDN network enhancements, which is summarised in the executive summary of congestion problem solutions.The second approach involves employing the most secure and simple algorithms possible.These so- lutions have demonstrated promising outcomes in terms of security and robustness, primarily due to their high capac- ity.It's important to acknowledge several

limitations that must be addressed for successful implementation. Scalability issues inherent in blockchain technology, resource-intensive computational requirements, regulatory complexities, interoperability challenges, and the ongoing vulnerability of the human ele- ment all pose significant obstacles to overcome. Despite these limitations, the dynamic and forward-looking nature of this field makes it ripe for continued research and innovation, with the potential to revolutionize digital communication security in the years to come.

FUTURE SCOPE

Certainly, for future implementations, it is possible to replace existing encryption techniques with more advanced encryption algorithms like Triple DES, RSA, Blowfish, and others. These algorithms offer stronger security and improved performance compared to some traditional encryption meth- ods.

REFERENCES

1. A Secure Blockchain-based Communication Approach for UAV Net- works Authors:Elias Ghribi, Tala Talaei Khoei, Hamed Taheri Gorji, Prakash Ranganathan, and Naima Kaabouch School of Electrical En- gineering and Computer Science (SEECS) University of North Dakota Grand Forks, ND, USA
2. Secure Data Encryption And Decryption using Crypto-Stego Au- thors:M.Venkatesh ,G.Satish,K.Ram Sudeep , M.Sudarshan
3. Blockchain and Cryptography Communication System Authors: J. Guru Lakshmi, K. Sai Ramya, G. Swapna, D. Thanmayi, K. Chandana, T. Sai Lakshmi
4. H. Shakhatreh, A. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. Shamsiah Othman, A. Khreishah, and M. Guizani, "Un- manned Aerial Vehicles: A Survey on Civil Applications and Key Research Challenges", vol.7,pp. 48572-48634.
5. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Consulted., 165: 55-61.
6. Zhu, Y., Gan, G.H., Deng, D. Security Research in Key Technologies of Blockchain
7. Liu, X.F. Research on blockchain performance improvement of Byzan- tine fault-tolerant consensus algorithm based on dynamic authorization. Zhejiang University.
8. Blockchain-enabled End-to-End Encryption for Instant Messaging Ap- plication Raman Singh ,Ark Nandan Singh Chauhan, H.Tewari Univer- sity.
9. The messenger that puts security and privacy first, https://threema.ch/en,Last accessed on 08-03-2021.
10. Nikos Filippakis, "Implementing Signal's Double Ratchet algorithm",https://nfil.dev/coding/encryption/python/double-ratchet- example/, Lastaccessed on 11-04-2022.