Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.6, May : 2024

SECURE COMMUNICATION USING BLOCKCHAIN TECHNOLOGY

Mr.K.S.S. Srinivas, MCA Student, Department of Master of Computer Applications, Vignan's Institute of Information Technology.
Mr. G. Ravi Kumar, Assistant professor, Department of Information Technology, Vignan's Institute of information Technology.

ABSTRACT
The blockchain is a ground-breaking technology that eliminates these risks and allows sensitive operations to be decentralized while maintaining a high level of security. It does away with the requirement for reliable middlemen. All network nodes have access to the blockchain, which records every transaction that has ever been completed. Our endeavour is focused on delivering a blockchain-based secure communications solution. In this project, we outline the reasons why blockchain technology would improve communication security and suggest a model design for blockchain-based messaging that preserves the security and performance of data stored on the blockchain. A smart contract is used to validate the user's certificate and authenticate their identities and associated public keys. The technology is a complete blend of encryption and blockchain for networks of communication.
Keywords: Blockchain, Cryptography, Hashing, hash keys, public key, Private key.

I. Introduction

Blockchain functions as a decentralized network where data is organized into blocks and linked together sequentially. Each block contains a set of records, and these blocks form a chain, constituting a public database. The connection between blocks is secured through cryptographic techniques, which are essential for the integrity of the blockchain. Cryptography, derived from the Greek words "Kryptos" meaning "hidden" and "Graphein" meaning "to write," is the foundation of ensuring privacy and security in communication processes. It involves designing protocols to prevent unauthorized access to private information during communication.

II. Literature

Blockchain has garnered significant attention from both engineers and investors due to its vast economic prospects and its utilization in diverse applications, including cryptocurrency. Various strategies have been proposed for enhancing Bitcoin's functionality, such as decentralized domain name services like Bit DNS, which evolved into Namecoin. Bitcoin boasts the most substantial computational power safeguarding its blockchain data. However, integrating new features into Bitcoin is challenging due to the need for consensus-breaking modifications. Bitcoin transactions lack a standardized method for transmitting data payloads, leading to exponential growth in blockchain size and placing strain on storage space and network bandwidth. Security concerns restrict the inclusion of only a limited number of functions in regular transactions. Peer-to-peer (P2P) systems offer solutions to many issues beyond traditional client-server models but also introduce challenges, such as establishing trust within P2P networks.
Ethereum's blockchain serves as a platform for decentralized applications known as smart contracts. Ethereum addresses are unique identifiers whose ownership remains constant, facilitating activity tracking and analysis. Smart contracts are executable code deployed on the blockchain, enabling automatic agreement execution between parties without interference. In the digital economy era, data flows increasingly among enterprises and across various platforms, necessitating measures for data

traceability, individual certification, and secure communications. Our research explores the potential of blockchain technology for addressing these needs.

III. Conclusion

Blockchain technology has emerged as a focal point for development among global organizations, with numerous startups dedicating resources to its advancement in recent years. This study examines the fundamental role of cryptography within blockchain and assesses current challenges. Initially, it provides an overview of blockchain infrastructure, simplifying its complexities. Subsequently, it explores the integration of cryptography within blockchain development. Lastly, it analyzes existing security vulnerabilities within the blockchain ecosystem. The research highlights how digital encryption technology underpins the entire blockchain system, ensuring high-level security as messages traverse through the communication system via cryptography and blockchain protocols.

References

[1]. Nakamoto, S. (2008) Bitcoin: A peer to peer electronic cash system. Consulted., 165: 5561.
[2] Zhu, Y., Gan, G.H., Deng, D. (2016) Security Research in Key Technologies of Blockchain. Information Security Research., 12: 10901097.
[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: 118.
[5] Shen, Y., Wang, G. (2017) Improved preimage attacks on RIPEMD160 and SHA160. Ksii Transactions on Internet & Information Systems., 12: 727746.
[6] Wang, H.Q., Wu, T. (2017) Cryptography in Blockchain. Journal of Nanjing University of Posts and Telecommunications., 37: 6167.
[7] Yuan, Y., Wang, F. (2016) Current Status and Prospects of Blockchain Technology Development. Acta Automatica Sinica., 42: 481494.
[8] Miyaji, A. (1994) Elliptic Curves Suitable for Cryptosystems. Ieice Transactions on Fundamentals of Electronics Communications & Computer Sciences., 77: 98105.
[9] He, P., Yu, G., Zhang, Y.F. (2017) Prospective review of blockchain technology and application Computer Science., 44: 17.
[10] Zhai, S.P., Li, Z.Z. (2018) The data block chain of the key technologies Consistency. Computer Technology and Development., 8: 16.
[11] An, Q.W. (2017) Research and application of key technologies for decentralized transactions based on blockchain. Donghua University.