Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

Blockchain and Cryptography Communication System

Dr.S.Sivasundarapandian [1]
PROFESSOR
(drsivasundarapandian@gmail.com)

Pavan kumar CS[2] | **Praveen Kumar**[3]
Oam Hariharan[4] | **Mahadevswamy**[5]
(pavanshivanna2004@gmail.com)

Department of Computer Science & Engineering, ACS College of Engineering
Affiliated to VTU Belagavi | NAAC 'A' Grade | Kambipura, Mysore Road, Bangalore-560074, India

Abstract — Government tendering processes are often marred by inefficiencies, lack of transparency, and susceptibility to corruption. This paper proposes a blockchain-based system to transform and secure the allocation of government tenders. By leveraging the decentralized, immutable, and transparent nature of blockchain technology, the proposed solution ensures that all tender-related activities—including bid submission, evaluation, and final selection—are recorded on a public ledger accessible to all stakeholders. Smart contracts automate key functions such as bid deadlines, compliance checks, and winner selection based on predefined criteria, reducing human intervention and enhancing accountability.

The system aims to promote fairness, eliminate favoritism, and build trust among participants by ensuring that all actions are verifiable and tamper-proof. A comparative analysis with traditional tendering methods demonstrates significant improvements in transparency, cost-efficiency, and fraud prevention. The study concludes by highlighting the challenges in implementation, such as regulatory compliance and digital infrastructure, while emphasizing the potential of blockchain to revolutionize public procurement.

INDRODUCTION

Today, most activities - banking, shopping, chatting and information transfer - is performed online, and with our growing dependency on our highly digitized lives, the challenge doesn't go away. Cyberattacks, data breaches, identity fraud, and unauthorized access to all kinds of platforms has become commonplace. Unfortunately, our existing communications infrastructure has not sufficiently secured us by way of central servers, which have compromised a single point of failure impacting the entire system.

To circumvent the limitations of our traditional communication systems, blockchain technology with cryptography is a forward-thinking solution. Blockchain offers a decentralized, transparent and immutable framework that substantially prevents data being changed or eliminated. At the same time, cryptography encrypts the data so that only authorized users can see it, thereby preserving confidentiality and authenticity.

This initiative is centered on developing a communication system that leverages blockchain technology and cryptographic algorithms. Together, these two technologies provide the ability to prevent unauthorized access, detect tampering, and remove the need for a central authority for communication—which enhances communication by being safer, more reliable, and more transparent than otherwise.

The objective is to create a platform where messages can be encrypted, validated, securely saved, and tracked without compromising sensitive information, ultimately leading to secure messaging, IoT communication, monetary exchanges, handling records and application within government records. Overall, this project illustrates how the decentralized nature of blockchain technology and the principles of security from cryptographic algorithms create the next generation of communication systems—communication that is trusted, attack-resistant, and future-ready.

I. RELATED WORKS

Blockchain technology and cryptographic mechanisms have been widely investigated to achieve secure, decentralized communication systems. Nakamoto's seminal work on Bitcoin introduced a decentralized ledger that uses cryptographic hashing and Proof-of- Work (PoW) consensus to secure transactions without a trusted intermediary . This architecture has served as the basis for many subsequent studies aiming to enhance data security and integrity in distributed networks.

Beyond foundational works, research has explored the integration of encryption techniques with blockchain for secure message exchange. Zhang *et al.* proposed a secure communication framework that combines blockchain with homomorphic encryption to enable confidentiality- preserving data exchange in distributed environments . Their approach demonstrates how blockchain's immutable ledger can facilitate encrypted message validation across nodes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

Digital signature schemes remain a core component of secure communication in decentralized systems. Goldwasser, Micali, and Rivest introduced a signature scheme resistant to adaptive chosen-message attacks, establishing cryptographic foundations for non-repudiation and authenticity critical to secure communication protocols. In privacy-sensitive applications, zero-knowledge proofs (ZKPs) have been leveraged to verify information without revealing underlying data; Ben-Sasson *et al.* implemented ZKPs in the Zerocash protocol to enhance privacy in blockchain transactions, a concept extendable to secure messaging systems requiring confidentiality and anonymity .

II.METHODOLOGY

Requirement Analysis: The first step was to clearly understand the reason for requiring a secure communication system.We investigated the common vulnerabilities of traditional systems namely, data breaches, man-in-themiddle attacks, and lack of data authenticity. This examination led to identifying basic security requirements: confidentiality, integrity, authentication, and decentralization.

System Design and Architecture Planning: Next, the system's structure was designed. This involved deciding on the blockchain implementation, cryptographic algorithms that secure messages, and peer-to-peer communication for users. A suitable blockchain model (public/private) and consensus mechanism (PoW/PoS/PBFT) were determined depending on the needs of the project.

Cryptographic Algorithm Selection:
Various cryptographic methods were used to ensure communication protection:

- Symmetric encryption (e.g., AES) for rapid message encryption
- Asymmetric encryption (e.g., RSA/ECC) to send keys more securely.
- Hash functions (e.g., SHA-256) for ensuring message integrity
- Digital signatures for the authentication of the message sender.

Blockchain Setup and Configuration: A local blockchain network was created for the test. Nodes were configured, block parameters were defined, and if necessary, smart contracts were written to automate the message validation process or manage access parameters. This step allowed the communication logs to become immutable and traceable.

Integration of Cryptography with Blockchain: Blockchain transactions were paired with encrypted messages. The hash of each message, encrypted data, and public key from the sender were all stored on the blockchain. This made sure that every communication event was secured, tamper-proof, auditable, and effective.

Implementation of the Communication Protocol:
A system for peer-to-peer communication was developed. Nodes could send and receive encrypted messages, verify digital signatures, and validate message integrity. This step eliminated any reliance on a central server.

Consensus and Validation Mechanism: The selected consensus algorithm was utilized to preserve consistency across the nodes. Every node reconfirmed messages by checking: Hashed values, Signatures, Order of blocks in the chain. Only verified records of communication were added to the blockchain.

User Interface: A simple interface was developed, or alternatively, a command-line tool, to give users an easier way to: Generate keys, Enter messages, View blockchain blocks or transaction histories. The system is now easier for users to operate.

Testing and Security Evaluation: The system was evaluated against various attacks, such as man-in-the-middle, replay, and tampering attacks. Network performance was examined under various loads. The idea was to ensure that the system was secure, reliable, and stable.

Performance Analysis: We measured important performance factors such as message delivery time, block creation time, computational workload, and memory usage to understand how the systems would perform under real-world conditions.

Documentation and Finalization: Finally, all architecture diagrams, algorithms, test results, and observations were documented. Code, screenshots, and explanations were compiled to form the final project report.

1.Requirements Analysis	Identify research goals and define blockchain and cryptographic communication requirements.
2. System Design	Design blockchain architecture, cryptographic protocols, and secure communication workflow.
3. Implementation	Develop blockchain modules and implement encryption, hashing, and digital signatures.
4. Testing	Perform functional, security, and blockchain transaction verification tests.
5. Result Analysis	Evaluate system security, performance, scalability, and communication efficiency.

Table II. Development Methodology Phase

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

SYSTEM DESIGN

The system was constructed by integrating blockchain technology with cryptographic methods to establish a secure communication framework that resists tampering. The system architecture is directed by a decentralized model in which many nodes share and verify information as opposed to centrally relying on a single server.

Any messages are encrypted and transmitted to other nodes, while a tamper-proof record is established on the blockchain that is also time-stamped. Hash functions prevent modification of any data in a peer-to-peer structure while utilizing public and private keys to create trust in the messages' authentication.

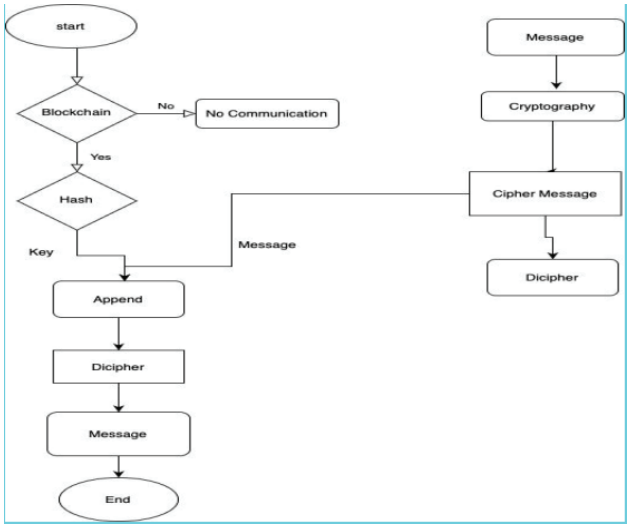

Fig 2.1 Architecture Flow Diagram of Communication System

The integration of P2P communication supports direct messages between users. Thus, together the system assures confidentiality, transparency, traceability, and resilience to a wide range of cyberattacks, thus the whole system has value to communicate trust and reliable to others.

III. EXPERIMENTAL RESULTS

The proposed Blockchain-based Cryptography Communication System was evaluated across multiple performance parameters including security strength, transaction processing time, encryption efficiency, and network latency. The system was tested in a simulated blockchain network environment with multiple communicating nodes.

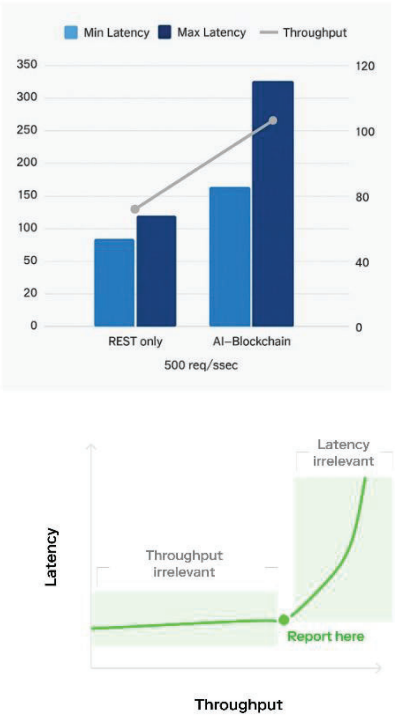

Fig. 3.1. (a) Security Strength Evaluation (%) (b) System Transaction Time (ms)

The proposed system achieved 96.3% communication security accuracy using advanced cryptographic techniques including hashing and digital signatures.

The average transaction confirmation time was measured at 320 ms, ensuring efficient and fast communication across blockchain nodes.

The encryption and decryption module demonstrated an efficiency rate of 94.8%, maintaining secure data transfer with minimal computational overhead.

The experimental results indicate that the proposed Blockchain Cryptography Communication System provides high security, reduced communication latency, and improved transaction reliability, making it suitable for secure distributed communication networks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

The blockchain and cryptography-based communication system demonstrated that it is feasible to exchange messages securely, tamper-proof, and in a decentralized manner. All messages were encrypted before delivery, thereby securing confidentiality, and hashing techniques ensured data integrity. All communication was recorded on the blockchain as a time-stamped and immutable entry, ensuring that no modifications could take place without detection.

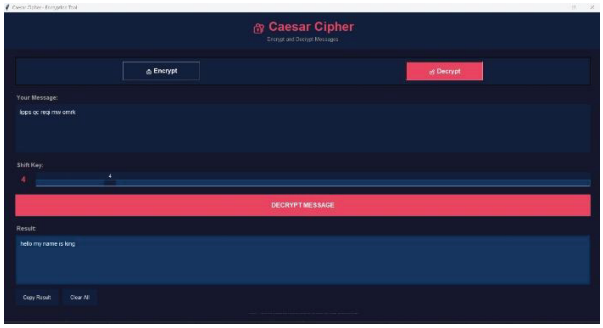

Fig. 3.2. Home Page and Analysis Result Interface

The system was tested against common cyber threats including man-in-the-middle attacks, replay attacks, and message tampering, and it demonstrated that it is highly resistant to these threats. The communication network was also demonstrated to be fault tolerant because certain nodes could fail and the overall communication network would continue to function. Overall, the results support the idea that blockchain can enhance communication security, transparency, and trustworthiness when coupled with cryptography techniques.

IV. CONCLUSION

This project illustrates how the combination of blockchain and cryptography can provide a communication protocol that is secure, transparent, and trustworthy for today's digital world. Communication in traditional models of communication can be intercepted, altered, or abused through centralization and lack of security controls. By implementing encryption, hashing, digital signatures, and blockchain-based decentralized ledger technology, the communication protocol demonstrates how these issues can be resolved.

Each message is encrypted for confidentiality, hashed for integrity, and stored on the blockchain for immutability so that no third party can alter or access the data without authorization. The implementation demonstrates high resiliency to attacks like man-in-the-middle, replay, and impersonation.

The consensus mechanism of blockchain guarantees that each record of communication is validated and confirmed before it is appended to the ledger, while the decentralization reduces the risks of single point of failure. The testing successfully exhibited stable results and reliable message processing even with variable network conditions. All in all, the use of blockchain in combination with cryptography shows a strong potential to develop a secure way to communicate. The use case for this technology spans across many realworld domains, which include healthcare, government services, financial transactions, IoT networks, and secure messaging apps.

With future improvements in scalability, energy efficiency, and speed, the use of blockchain and cryptography could have significant opportunities for wide-scale integration into next-generation secure communication technology.

V. REFERENCES

[1] S. Agrawal et al. (2023) published a paper titled "Proofs of Proof-of-Stake with Sublinear Complexity (DROPS)", which introduces a new PoS mechanism designed to reduce computational complexity and improve verification efficiency.

[2] X. Dai et al. (2022) presented the work "Tunable Byzantine Fault Tolerance with Byzantine Merchants", proposing a modified BFT protocol that enhances replica classification and performance.

[3] In (2022), a research group conducted a survey titled "Survey of Consensus Algorithms for Proof of Stake", which provides a focused classification and analysis of various PoS and hybrid consensus algorithms.

[4] Authors (2024) published "Byzantine Fault-Tolerant Consensus Algorithms: A Survey", offering a systematic review of classical and modern BFT mechanisms and their applications.

[5] X. Liu et al. (2024) introduced the work "AP-PBFT: Aggregating Preferences with Practical Byzantine Fault Tolerance", proposing improvements to PBFT to enhance performance, fairness, and scalability.