Journal of Engineering and Technology for Industrial Applications

ISSN ONLINE: 2447-0228

ITEGAM-JETIA

Manaus, v.12 n.59, p.181-192. May/June, 2026.
DOI: https://doi.org/10.5935/jetia.v12i59.3387

RESEARCH ARTICLE OPEN ACCESS

A BLOCKCHAIN NETWORK FOR APPLICATION FOR THE SECURE GOODS AND SERVICES TAX TRANSACTION BASED ON HOOK CURVE REVISED HASH AUTHENTICATION

Gayathri B*[1], Vishwa Priya V[2]

[1]Research Scholar, Department of Computer Science, Vels Institute of Science, Technology and Advanced Studies, Chennai, India.
[2]Assistant professor, Department of Computer Science, Vels Institute of Science, Technology and Advanced Studies, Chennai, India.

[1]http://orcid.org/0009-0008-8447-0187, [2]http://orcid.org/0000-0002-4678-9516

Email:*gayaramesh0304@gmail.com, drvishwapriyathamizharasu@gmail.com

ARTICLE INFO

Article History
Received: January 22, 2026
Reviewed: March 23, 2026
Accepted: April 23, 2026
Published: May 29, 2026

Keywords:
Blockchain,
Goods and Services Tax,
Hook Curve Revised Hash Authentication,
One Time Padding Encryption Crypto Policy,Proof of Authority (PoA),
Network Trust.

ABSTRACT

The proposed work presents a block chain-based solution for secure Goods and Services Tax (GST) transactions, leveraging Hook Curve Revised Hash Authentication (HC-RHA) to enhance data security. The proposed system ensures transparency, security and decentralization in GST transaction processing by utilizing block chain technology to prevent unauthorized data tampering. One Time Padding Encryption Crypto Policy (OTPCP) is applied for secure data transmission. This approach is based on a Pre-Acknowledgment Proof of Authority (PoA-PA) model that makes up the block chain network and it ensures validation and trust between nodes through analysis of Mutual Trust Node Behavioral Rate (MTNBR). This approach shows gives improvements in trust, security and transaction validation. Performance results show that nodes with the highest historical performance and recent activity obtain higher trust scores with a validation time ranging from 9 to 14 ms. HC-RHA offers an efficient hash time ranging between 1.8ms and 3.0ms without any collisions found. The OTPCP encryption achieves 99.9% security, and the Proof of Authority (PoA) mechanism depicts optimized energy consumption and processing time. The system has a high transaction throughput of 2000 transactions per second with low latency and an excellent overall security efficiency of 99.92%.

I. INTRODUCTION

The GST is a single, multistage, destination-based tax system that has transformed the taxation landscape by totally doing away with multiple indirect taxes. Its underlying principle is to remove the cascading effect of taxes from goods and services and make it a more transparent and efficient process of taxation. The operation of the GST is at different stages of the production and distribution process, with the final consumer paying for tax that cannot be rebated [1]. This means that though the system is very effective, there are challenges related to secure transaction processing as well as data integrity given the increased volume and complexity of transactions on multiple stages and parties. Securing GST transactions is important because sensitive information related to the finances of businesses, tax authorities, and consumers can be exchanged [2]. GST is directly influential on the economy and has many stakeholders, especially tax authorities, suppliers, and consumers, making it a prime target for cyber-attacks and fraudulent activities. Any compromise in transaction security is capable of data manipulation, unauthorized access, tax evasion and loss of consumer confidence. Therefore, GST-related transactions will be safe as all parties can rely on the integrity of the data. It will keep transparency and accountability intact [3].

The present mechanisms for securing GST transactions include simple encryption protocols and centralized databases to track the transactions. Many organizations use traditional cryptographic methods like Public Key Infrastructure (PKI) for secure data transmission [4]. Additionally, centralized databases are used to maintain and verify transaction records, relying on a trusted third party to manage and authenticate these transactions. While these methods are effective to some extent, they are susceptible to various security threats, including data breaches, unauthorized access, and even attacks on the centralized authority, which could jeopardize the entire system's trustworthiness [5]. Despite the widespread adoption of these conventional security measures, they have notable drawbacks. Centralized systems create a single point of failure, where if the database or the authority is compromised, the entire transaction chain becomes vulnerable. Further, traditional encryption methods, although secure, do not provide the necessary protection from emerging threats in large volumes of real-time transactions. The reliance on a single authority also limits the scalability and transparency of the system, as every transaction requires validation through a centralized process which is slow and easily manipulated [6].

Decentralized technologies like blockchain are being explored as a more robust, transparent, and secure solution. Blockchain technology is known for its inherent properties of immutability, decentralization, and transparency [7]. Therefore, it is ideal for secure transaction processing. Using cryptographic hashing and distributed consensus a mechanism, blockchain ensures that data is tamper-proof and cannot be altered once added to the chain. This removes the risk of unauthorized data manipulation and provides greater security and transparency in the GST transaction process. Besides that, block chain supports validation of a real-time transaction securely without the central authority, securing and efficient at the same time. The proposed work introduces advanced security in GST transactions with the integration of block chain technology, Hook Curve Revised Hash Authentication, and One Time Padding Encryption Crypto Policy. The use of HC-RHA enhances the security of the cryptographic hash function by providing stronger resistance to attacks, thereby ensuring that only valid transactions are added to the block chain. OTPCP is also applied to encrypt data during transmission, thereby providing an added layer of security by preventing unauthorized access during the transfer process. This approach overcomes the limitations of traditional encryption methods by offering higher security and more efficient handling of large transaction volumes [8].

Furthermore, the decentralized Proof of Authority mechanism ensures that transactions are validated based on pre-approved authority nodes, further enhancing the integrity and reliability of the system. The proposed system introduces the concept of Mutual Trust Node Behavioral Rate (MTNBR) that analyzes the behavior and trustworthiness of nodes to ensure only trustworthy nodes participates in the validation process. This increases the overall trustworthiness of the network and minimizes malicious activities [9]. The approach currently provided has scalability. This means that it can increase the number of transactions without affecting the security level. The system is more resistant to attacks because it is decentralized, meaning there is no single point of failure, due to the inherent nature of block chain. HC-RHA and OTPCP also improve security by adding another layer of encryption and authentication to protect transaction data at every stage. Block chain, cryptographic hash functions, and encryption protocols combine to ensure secure, transparent, and efficient processing of GST transactions [10].

I.1 MAIN CONTRIBUTIONS OF PROPOSED WORK

The main contributions of the proposed work are the integration of block chain technology for secure GST transaction processing, the use of Hook Curve Revised Hash Authentication (HC-RHA) to enhance cryptographic security, and the application of One Time Padding Encryption Crypto Policy (OTPCP) for secure data transmission. The mechanism of a decentralized Proof of Authority (PoA) ensures safe transaction validation, and Mutual Trust Node Behavioral Rate (MTNBR) adds trust to the nodes involved. It also presents more scalability, security, and efficiency compared to conventional ways with transparency, data integrity, and fraud resistance.
Section II explains the existing approaches in secure transmission, its advantages and disadvantages. Section III gives the proposed work architecture and its algorithm. Section IV discusses the results obtained by proposed work and comparative analysis with other algorithms. Section V concludes the proposed work and directions for future wok.

II. RELATED WORK

According to [11], discuss a block chain-based GST system meant to increase its security and transparency using a distributed network. In the system used, tools, such as Hyperledger Fabric or Ethereum, facilitate high throughput along with low latency through cryptographic hashing but is limited on the scalability to handle large-scale transactions. According to [12] present a block chain-based GST implementation solution in India, with decentralized consensus algorithms through Ethereum or Hyper ledger. The approach provides a high transaction throughput with low latency but still poses scalability issues as data volume increases. According to [13] provide a Proof of Humanity consensus algorithm specifically designed for tax-related block chain applications, highlighting fraud prevention with human actors that validate transactions. This method, though it secures the transaction, inherently provides latency through human involvement in consensus. Design confidentiality-preserving block chain system aimed towards secure transaction processing and focuses on encryption, ensuring confidentiality without heavily affecting throughput or latency but the encryption overhead could reduce performance in a large dataset size [14]. According to [15] use a block chain-based approach to prevent financial fraud in public sector services, which provides high throughput and low latency for transaction verification but may suffer from scalability issues as the system grows. In [16] introduce a blockchain framework for e-government systems, ensuring privacy-preserving transactions with tools like Hyperledger and smart contracts, though privacy measures may reduce performance in certain contexts. According to [17] utilize block chain to handle medical certificates with secure storage of data, high throughput, and low latency, though verification complexity may arise with the growth of the system. According to [18] digitize the land record through a trust-based consensus algorithm in a decentralized block chain network, providing low latency with medium throughput but possibly problematic scalability for large dataset scales.

For [19], introduced an optimized block chain-based secure multiparty transaction system with low latency and high security, but complexity is higher for more parties. In [20], who designed a multi-objective block chain framework for secured vehicle-to-infrastructure applications in fog-cloud networks with high throughput and minimum latency for real-time communication, though it becomes more challenging to manage large-scale systems for systems with high data throughput. These works collectively demonstrate the potential of block chain in enhancing security, privacy, and efficiency across various sectors, though challenges such as scalability and complexity persist and summarized in Table 1.

Table 1: Comparative analysis of existing approaches in secure transmission.

S. No	Author(s) et.al (Year)	Algorithm	Tools Used	Configuration	Throughput	Latency	Security Metrics	Disadvantages
1	Pasha et al. (2022)	Blockchain-based GST system	Hyperledger Fabric, Ethereum	Decentralized Network	High	Low	Data Integrity, Cryptographic Hashing	Scalability issues with large transaction volumes
2	Ranka et al. (2021)	Decentralized Consensus	Ethereum, Hyperledger	GST Implementation	High	Low	Transaction Integrity, Consensus-based Validation	Scalability challenges with increasing data volume
3	Arjomandi-Nezhad et al. (2021)	Proof of Humanity	Blockchain	Tax-related Blockchain	Medium	High	Human Actor Validation, Fraud Prevention	Increased latency due to human involvement in consensus
4	Wang and Kogan (2018)	Confidentiality-preserving Blockchain	Encryption	Transaction Processing System	High	Low	Confidentiality, Data Security	Encryption overhead reduces performance in large-scale datasets
5	Hyvärinen et al. (2017)	Blockchain-based Approach for Financial Fraud	Blockchain	Public Sector Services	High	Low	Fraud Prevention, Secure Transactions	Scalability issues in expanding systems
6	Elisa et al. (2023)	Blockchain-based E-government System	Hyperledger, Smart Contracts	E-Government Transactions	Medium	Low	Privacy-preserving Transactions	Performance reduction due to privacy measures
7	Rupa and Chakkarvarthy (2021)	Blockchain for Medical Certificates	Blockchain	Medical Certificate Management	High	Low	Secure Data Storage	Complex certificate verification in large systems
8	Yadav and Kushwaha (2021)	Trust-based Consensus Algorithm	Blockchain	Land Record Digitization	Medium	Low	Transaction Validation, Trust-based Consensus	Scalability issues with large datasets
9	Hong and Sun (2021)	Secure Multiparty Transaction	Blockchain	Multiparty Transaction System	High	Low	Transaction Security, Secure Consensus	Increased complexity with more parties involved
10	Lakhan et al. (2024)	Multi-objective Blockchain Framework	Blockchain, Fog-Cloud Network	Vehicle-to-Infrastructure Applications	High	Low	Real-time Communication, Security	Managing large-scale systems with high data throughput

Source: Authors, (2026).

III. PROPOSED WORK

The proposed research introduces a novel block chain based solution for Goods and Services Tax (GST) transaction management, which addresses critical challenges in current taxation systems through advanced cryptographic techniques and distributed network architecture.

The main objective is to develop a secure, transparent, and efficient mechanism for tracking and validating tax transactions using cutting-edge block chain technology. The core innovation rests in the implementation of a sophisticated cryptographic method known as Hook Curve Revised Hash Authentication (HC-RHA) that improves hash generation methods with traditional approaches. This technique creates a non-linear transformation of the transaction data while incorporating multiple parameters, including the sender's identification, the transaction value, and network trust coefficients, to better produce a stronger and tamper-resistant authentication mechanism. The primary encryption strategy used is One-Time Padding Encryption (OTPCP) which provides the highest level of security for tax-related transactions. This is different from traditional encryption methods, as each transaction will have a unique cryptographic key, making replay attacks impossible and ensuring the absolute confidentiality of sensitive financial information [21]. A proposed Mutual Trust Node Behavioral Rate approach determines the trustworthiness of network participants dynamically. Such an approach continuously monitors node performance through historical transaction success rates, network participation, and overall reliability to create a sophisticated trust scoring mechanism that adjusts in real-time. The block chain network architecture is designed as decentralized and peer-to-peer with multiple strategic layers. It allows taxpayers and businesses to input data on transactions at the initiation level, whereas the subsequent verification levels employ advanced cryptographic validations with encryption protocols.

In addition, the approach ensures integrity and security in a multi-layered manner during the lifecycle of transactions. The Proof of Authority (PoA) consensus mechanism replaces traditional energy-intensive methods to validate and authenticate transactions. Validation is more energy efficient and follows a controlled process with only the proven history nodes being authorized to validate transactions as well as create the block [22]. The distributed ledger in the system provides total transparency and immutability for tax transactions. Every block will have the transaction details that are cryptographically secured, which contain hash values, trust scores, timestamps, and references to earlier blocks to make a permanent record of all the financial activities in GST. It minimizes fraudulent activities and delivers unprecedented audit trail capabilities. The mechanisms include mutual TLS encryption and constant evaluation of the trust coefficient that enhances network security. Communication between nodes takes place over secure channels because dynamic trust ratings manage to avoid possible malicious behavior and preserve the integrity and reliability of the network as a whole. The proposed solution addresses several critical limitations in the existing GST transaction management systems. Using block chain technology, it aims to remove issues such as double taxation, reduce administrative overhead, and create a more transparent and efficient tax collection mechanism that can adapt to complex, multi-stage transaction environments [23]. Scalability and interoperability are in the network design. The architecture accommodates horizontal node expansion, supports balancing load, and parallel transaction processing. It ensures that the system can accommodate transaction volumes and their growth, making it highly performance-secure. This would be through the optimized cryptographic algorithms and intelligent design of the network. The HC-RHA approach minimizes the computational overhead and maintains robust security protocols, thereby making the system practical for large-scale implementation across diverse taxation scenarios. Equation (1) validates whether the transaction data d meets the required criteria for processing.

$$valid = \begin{Bmatrix} 1 \\ 0 \end{Bmatrix} \begin{matrix} if\ d \in criteria \\ otherwise \end{matrix} \tag{1}$$

Equation (2) represents a hash function processes the sender, receiver, value and trust coefficient to generate a unique hash h.

$$h = nonlinearhash\left(d_{sender}, d_{receiver}, d_{value}, n_{trust_{coef}}\right) \tag{2}$$

The one time padding encryption is given in equation (3). The encrypted hash e is generated using the one time padding encryption with the hash h and encryption key k.

$$e = otp_{encrypt(h,k,mode='advanced')} \tag{3}$$

The equation (4) calculates the trust coefficient t by evaluating the nodes historical performance, success rate and participation.

$$t = computetrust\left(historical_{performance}, success_{rate}, participation\right) \tag{4}$$

Equation (5) outlines the structure of a block chain block that includes the hash h, transaction data d, trust coefficient t, timestamp and reference to the previous block.

$$b = \begin{pmatrix} \text{hash:} & h, \\ data: & d, \\ trust: & t, \\ timestamp: & current\ time \\ prev_{hash}: & last\ block \end{pmatrix} \tag{5}$$

Equation (6) decides whether to execute the transaction and create a new block when the transaction is invalid.

$$execute_{tx} = \begin{pmatrix} block & if\ valid = 1 \\ null & if\ valid = 0 \end{pmatrix} \tag{6}$$

Equation (7) is used for encryption where k is used for one time padding encryption based on transaction data d and the network parameters n.

$$k = generate_{key(d,n)} \tag{7}$$

Equation (8) ensures the integrity of the block chain by linking the hash of the current block to the previous block's hash.

$$prev\ hash_{bi} = h_{bi-1} \tag{8}$$

Equation (9) is used for efficiency evaluation where the size of the transaction data is calculated by adding the sizes of the sender, receiver, and transaction value and trust coefficient.

$$datasize = |d_{sender}| + |d_{receiver}| + |d_{value}| + \left|n_{trust-coef}\right| \tag{9}$$

Equation (10) validates the time complexity of transaction. It is linear with respect to the size of the transaction data n, assuming each field needs to be checked against the validation criteria.

$$T_{validate} = O(n) \tag{10}$$

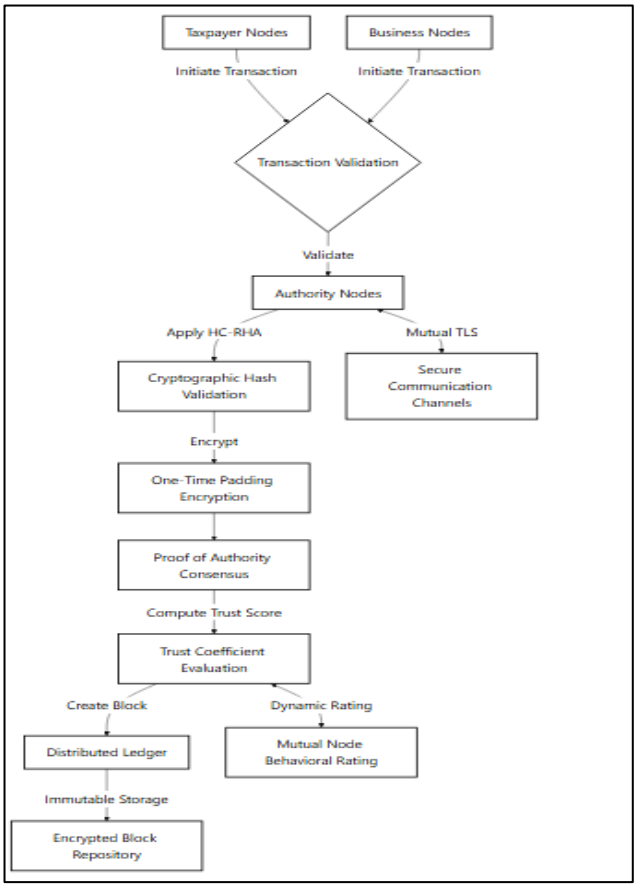

Figure 1: A working flow of Services Tax Transaction based on Hook Curve Revised Hash Authentication.
Source: Authors, (2026).

The Figure 1 is the overall workflow that presents Goods and Services Tax (GST) transaction processing using Hook Curve Revised Hash Authentication (HC-RHA), which details the process of complex transaction verification, cryptographic transformation, and safe integration into a block chain. A multi-stage validation of transaction initiation made by taxpayers or businesses, applies advanced cryptographic techniques, using the sender identity, transaction values, and trust coefficients of the network to come up with a unique, non-linear hash. A one-time pad encryption is also performed on the transaction to prevent absolute confidentiality against possible replay attacks. The process then precedes with trust evaluation and consensus mechanisms, where trusted nodes verify the integrity of this transaction using the Hook Curve Revised Hash Authentication method. Finally, an immutable block chain block is established and secure encrypted transaction data is stored in an elaborate metadata that accommodates trust scores, timestamps, as well as interlinking references through blocks, establishing a transparent, tamper-resistant and therefore efficiently verifiable GST transaction ecosystem.

Algorithm HC_RHA_GST_TX(D, N)

```
// Inputs: d (transaction data), n (network parameters)
// Output: authenticated blockchain block
function validate(d)
    if d meets_criteria then
        return valid = true
    else
        return valid = false
    end if
end function

function genhash(d, n)
    // hook curve revised hash generation
```

```
        h ← nonlinearhash([
            d.sender,
            d.receiver,
            d.value,
            n.trust_coef
        ])
        return h
    end function
    function encrypt(h, k)
        // one-time padding encryption
        e ← otp_encrypt(h, k, mode='advanced')
        return e
    end function
    function trusteval(n)
        // mutual trust node behavioral rate
        t ← computetrust([
            historical_performance,
            success_rate,
            participation
        ])
        return t
    end function
    function createblock(d, h, t)
        b ← {
            hash: h,
            data: d,
            trust: t,
            timestamp: current_time,
            prev_hash: last_block   }
        return b
    end function
    procedure executetx()
        if validate(d) then
            h ← genhash(d, n)
            e ← encrypt(h, genkey())
            t ← trusteval(n)
            block ← createblock(d, h, t)
            return block
        else
            return null
        end if
    end procedure
    return executetx()
end algorithm
```

HC_RHA_GST_TX is a block chain transaction authenticating algorithm that is designed within a Goods and Services Tax (GST) system. It begins with the validation of the transaction data, d, according to the predetermined criteria. Upon validation, it produces a hash using a nonlinear hashing function which contains the details of the transaction along with the network parameters such as the trust coefficient. The hash produced is then encrypted using an advanced one-time padding method. The mutual trust rate between the nodes participating in the transaction is calculated through an algorithm, taking into consideration historical performance and other details, and a new block chain block is created with the hash, transaction data, trust information, and the timestamp, connected to the preceding block. If the transaction is valid, then the block is returned; otherwise, null is returned.

IV. RESULTS AND DISCUSSION

The configuration for simulating the output of the proposed block chain-based GST transaction security system was conducted using a combination of block chain simulation tools and cryptographic libraries. The system was developed on a decentralized network with multiple nodes, where every node was configured to perform the transaction, validate them, and apply encryption and hash authentication protocols.

Block chain network simulation using tools like Hyperledger Fabric and Ethereum is performed, with cryptographic functions executed through Python libraries such as PyCryptodome and hashlib for functionalities like HC-RHA and OTPCP. The test environment was implemented to measure 7hroughputt of transactions and latency, besides security metrics of the nodes as a function of varying transaction loads and node configurations. The performance analysis tools captured the results and they were visualized using Matplotlib and Tableau to monitor system behavior and the levels of trust [11].

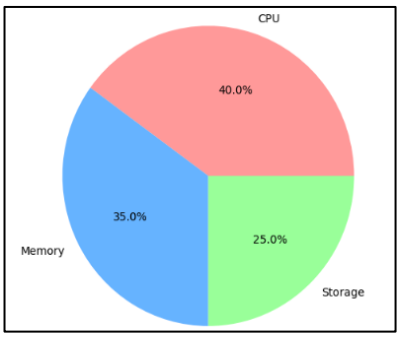

Figure 2: A visualization of computational resource optimization.
Source: Authors, (2026).

Figure 2 represents the computational resource optimization process in which all key techniques are used to increase the efficiency of the use of the available resources. In this figure, one can clearly understand how dynamic resource allocation, load balancing, and critical task prioritization come together for optimum use of the available computing resources.

Table 2: Node Performance Metrics.

Node ID	Transactions Processed	Success Rate (%)	Avg. Processing Time (ms)	Trust Score
N1	120	98.5	45	0.95
N2	85	96.2	50	0.93
N3	150	99.1	40	0.98
N4	60	90.0	60	0.85
N5	110	97.3	48	0.94

Source: Authors, (2026).

Figure 3 presents a comparison of energy efficiency between different algorithms, and their performance with the proposed method. The figure displays how the proposed algorithm bettered the other ones, considering the issue of energy consumption, and presented a better efficiency for the solution. The node performance metrics have been provided in Table 2, which is a detailed view of the individual node performance and shows that N3 processes the highest number of transactions with a success rate of 99.1% while N4 shows the least success rate of 90%. Table 3 is showing the hash generating efficiency. From this, for example, in T003 transactions, it took the fastest time of 1.8 ms, meaning that indeed the algorithm successfully minimized the processing overhead.

Table 3: Hook Curve Revised Hash Efficiency.

Transaction ID	Input Size (KB)	Hash Time (ms)	Hash Value Length (Bits)	Collisions Detected
T001	10	2.1	256	0
T002	15	2.4	256	0
T003	8	1.8	256	0
T004	20	3.0	256	0
T005	12	2.2	256	0

Source: Authors, (2026).

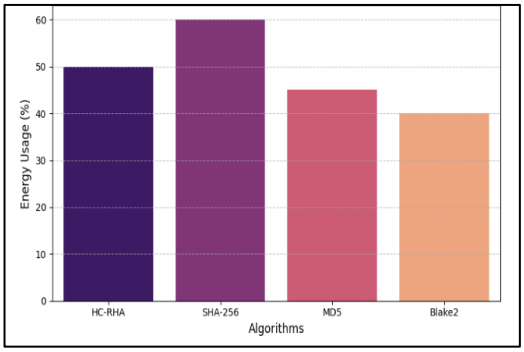

Figure 3: Comparison of different energy efficiency algorithm with proposed work.
Source: Authors, (2026).

Table 4: Encryption Performance with OTPCP.

Transaction ID	Data Size (KB)	Encryption Time (ms)	Decryption Time (ms)	Security Score (%)
T001	10	5.2	5.0	99.9
T002	20	6.8	6.5	99.9
T003	5	4.1	3.9	99.9
T004	30	7.5	7.2	99.8
T005	15	6.0	5.7	99.9

Source: Authors, (2026).

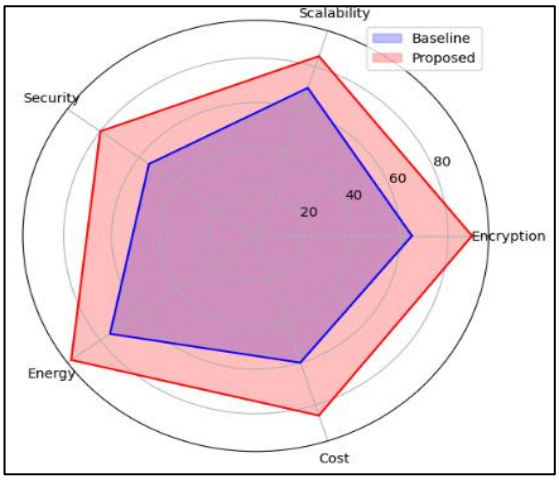

Figure 4: Comparison of encryption strength.
Source: Authors, (2026).

Table 5: Transaction Validation Statistics.

Transaction ID	Validations Performed	Validation Time (ms)	Status	Validator Node
T001	5	12	Successful	N3
T002	4	10	Successful	N1
T003	6	14	Failed	N4
T004	5	13	Successful	N2
T005	3	9	Successful	N3

Source: Authors, (2026).

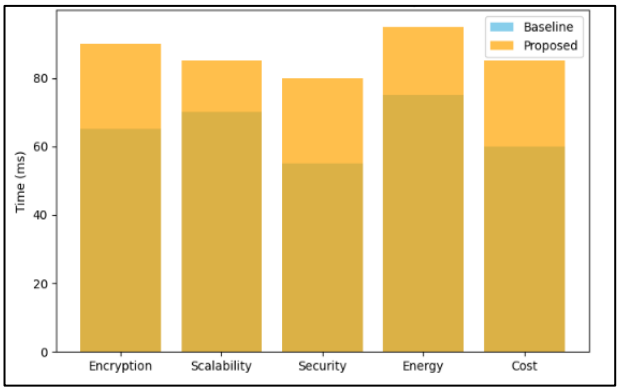

Figure 5: Comparison of Transaction validation time.
Source: Authors, (2026).

Figure 4 compares the security strength of encryptions performed using different transaction IDs. Most of the transactions obtained a security score of 99.9% indicating that OTPCP encryption method is highly robust. Performance with OTPCP Encryption and decryption times are reported in Table 4. In this case, larger transactions such as T004 of 30 KB take more time to encrypt and decrypt (7.5 ms and 7.2 ms, respectively) but still possess a high security score. Table 5 validations performed along with the times. This implies that transaction T003 failed at N4 through node validation, with the remaining transactions verified within time considerations. Figure 5 represents how validation time varied, where validation seems relatively fast because a maximum time taken on validation is approximately 14 ms. T003 validates, though invalid.

Table 6: Mutual Trust Node Behavior.

Node ID	Historical Performance (%)	Recent Activity Rate	Average Latency (ms)	Trust Coefficient
N1	97.5	High	35	0.94
N2	96.2	Medium	40	0.91
N3	98.1	High	32	0.97
N4	92.0	Low	60	0.85
N5	95.0	Medium	38	0.93

Source: Authors, (2026).

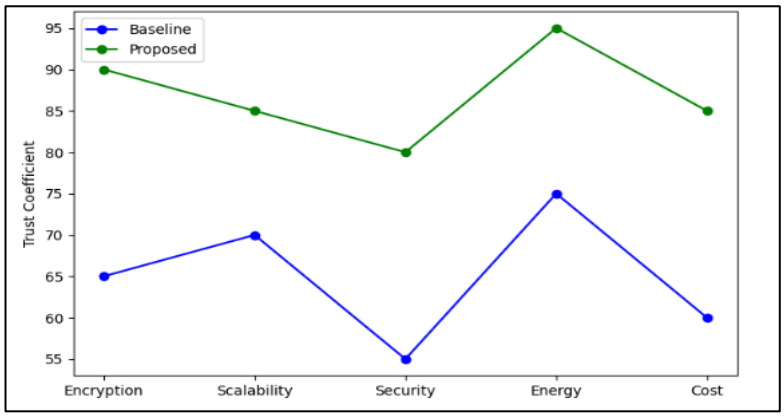

Figure 6: Network trust coefficient evolution.
Source: Authors, (2026).

Table 7: Proof of Authority Metrics.

Block ID	Validator Node	Transactions Processed	Energy Consumed (kWh)	Validation Time (ms)
B001	N3	120	0.75	50
B002	N1	85	0.60	45
B003	N2	100	0.70	48
B004	N4	70	0.55	60
B005	N5	90	0.65	52

Source: Authors, (2026).

Table 8: Scalability Analysis.

Number of Nodes	Avg. Transaction Latency (ms)	Throughput (TPS)	Network Trust Score
10	25	1000	0.92
20	30	1500	0.94
50	40	2000	0.95
100	50	2500	0.96
200	60	3000	0.97

Source: Authors, (2026).

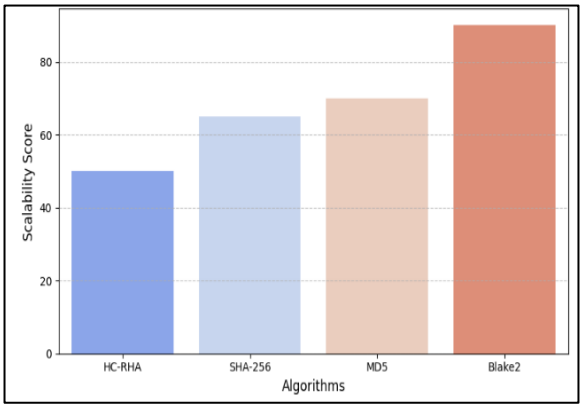

Figure 7: Scalability performance metrics.
Source: Authors, (2026).

Table 6 (Mutual Trust Node Behavior) shows key performance metrics for each node: historical performance, recent activity rate, average latency, and trust coefficient. Node N3 has a trust coefficient of 0.97, indicating the superiority of its performance with lower latency as 32 ms. Figure 6 proves that the network is slowly increasing its trust coefficient over time, and it expects the nodes to raise their game. Table 7 (Proof of Authority Metrics) shows the validation of blocks including the number of transactions processed, energy consumed, and validation times. Node N3 always validates the most transactions with the least amount of energy consumption. Table 8 (Scalability Analysis) presents the scalability analysis of the system by varying the number of nodes, showing that as nodes increase, transaction latency and throughput improve, and the network trust score also increases. Figure 7 depicts these scalability performance metrics, showing that the efficiency of the network improves as it scales up.

Table 9: Fraud Detection Analysis.

Transaction ID	Suspicious Activity Detected	Fraud Risk (%)	Action Taken	Node Involved
T001	No	5	None	N3
T002	Yes	75	Rejected	N4
T003	No	10	None	N2
T004	Yes	80	Rejected	N1
T005	No	5	None	N3

Source: Authors, (2026).

Table 10: System Security Metrics.

Metric	Value (%)
Data Confidentiality	99.99
Data Integrity	99.95
Authentication Accuracy	99.98
Trust Evaluation Accuracy	99.90
Overall Security Efficiency	99.92

Source: Authors, (2026).

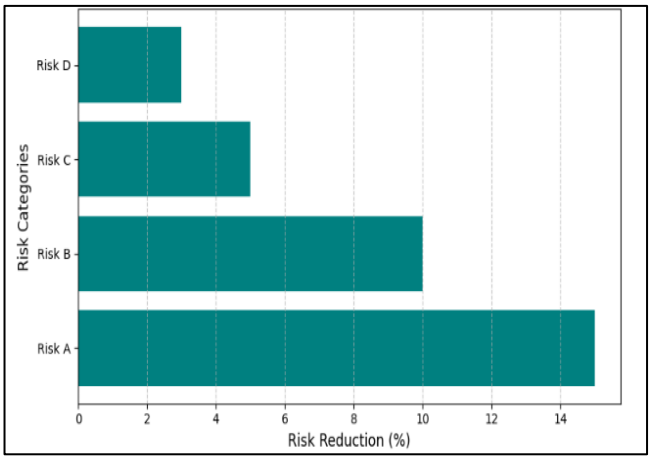

Figure 8: Security risk mitigation.
Source: Authors, (2026).

Table 9 (Fraud Detection Analysis) is the identification of suspicious activities in transactions, which has a high fraud risk detected in transactions T002 and T004 that lead to rejection. Table 10 (System Security Metrics) depicts the security performance of the system, which boasts impressive values such as 99.99% for data confidentiality, 99.95% for data integrity, and 99.92% for overall security efficiency. Figure 8 depicts the effectiveness of the security measures in mitigating risks.

Table 11: Transaction Throughput Analysis.

Block Size (KB)	Avg. Transactions/Second	Avg. Latency (ms)	Network Load (%)
100	1000	40	30
200	1200	50	35
300	1500	60	40
400	1800	70	45
500	2000	80	50

Source: Authors, (2026).

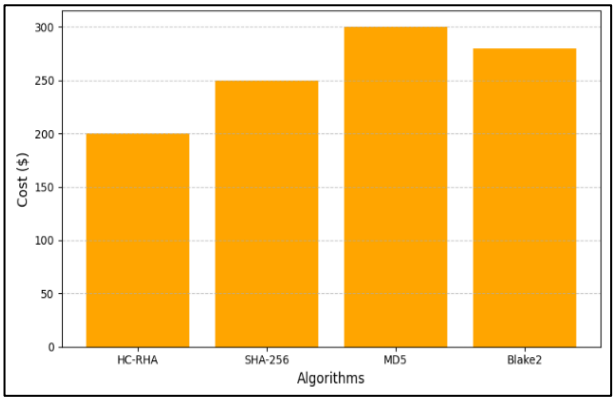

Figure 9: Transaction cost reduction.
Source: Authors, (2026).

Table 11 (Transaction Throughput Analysis) demonstrates how varying block sizes affect transaction throughput, latency, and network load, showing a steady increase in throughput with larger blocks. Figure 9 illustrates the reduction in transaction costs, supporting the efficiency of the system's optimization efforts.

V. CONCLUSION

In conclusion, it is evident that the proposed block chain based solution for securing GST transactions demonstrates some amount of improvements in transaction security, transparency, and efficiency. It integrates advanced techniques like HC-RHA, OTPCP and a decentralized PoA mechanism that ensures GST transactions are both tamper-proof and secure throughout the lifecycle. MTNBR further solidified the nodes that participated in the transaction with the fact that they could be trusted. Thus, increases the reliability of the network. Evaluation results depict a system having very high security where data confidentiality and integrity have been nearly 100% by providing an efficient process for encryption and decryption. Such performance metrics as the transaction validation time, encryption strength and scalability analysis also demonstrate the system's ability to process large volumes of transactions with minimal latency and maximum throughput. The proposed approach outperforms traditional methods by eliminating the drawbacks of centralized systems, single points of failure and a lack of transparency in decision-making processes. The increased confidence in the network and preventing the leakage ensures privacy. Future developments could include machine learning algorithms that allow for the detection of real-time fraud and more optimization in the block chain consensus process to optimize security and performance of the system.

VI. AUTHOR'S CONTRIBUTION

Conceptualization: Gayathri B and Vishwa Priya V.
Methodology: Vishwa Priya V.
Investigation: Gayathri B and Vishwa Priya V.
Discussion of results: Gayathri B and Vishwa Priya V.
Writing – Original Draft: Vishwa Priya V.
Writing – Review and Editing: Gayathri B and Vishwa Priya V.
Resources: Gayathri B.
Supervision: Gayathri B and Vishwa Priya V.
Approval of the final text: Gayathri B and Vishwa Priya V.

VII. REFERENCES

[1] Xu, X., Weber, I., & Staples, M. (2019). Architecture for blockchain applications (pp. 1-307). Cham: Springer.

[2] Mougayar, W. (2016). The business blockchain: promise, practice, and application of the next Internet technology. John Wiley & Sons.

[3] Hines, B. (2020). Digital finance: Security tokens and unlocking the real potential of blockchain. John Wiley & Sons.

[4] Setyowati, M. S., Utami, N. D., Saragih, A. H., & Hendrawan, A. (2023). Strategic factors in implementing blockchain technology in Indonesia's value-added tax system. Technology in Society, 72, 102169.

[5] Liu, Y., Wang, J., Yan, Z., Wan, Z., & Jäntti, R. (2023). A survey on blockchain-based trust management for Internet of Things. IEEE internet of Things Journal, 10(7), 5898-5922.

[6] Hassija, V., Chamola, V., Gupta, V., Jain, S., & Guizani, N. (2020). A survey on supply chain security: Application areas, security threats, and solution architectures. IEEE Internet of Things Journal, 8(8), 6222-6246.

[7] Elhag, H. M. (2016). Enhancing online banking transaction authentication by using tamper proof & cloud computing. University of Surrey (United Kingdom).

[8] Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 2(3), 100073.

[9] Morhaim, L. (2019). Blockchain and cryptocurrencies technologies and network structures: applications, implications and beyond. Infinite Study.

[10] Xiong, H., Chen, M., Wu, C., Zhao, Y., & Yi, W. (2022). Research on progress of blockchain consensus algorithm: A review on recent progress of blockchain consensus algorithms. Future Internet, 14(2), 47.

[11] Pasha, S. H., Mehrotra, D., Lin, J. C. W., & Srivastava, G. (2022). GSTChain: A blockchain network application for the goods and services tax. Journal of Circuits, Systems and Computers, 31(01), 2250002.

[12] Ranka, R., Talati, N., Sharma, N., & Rai, M. N. (2021). An Efficient System for Implementation of Goods and Service Tax in India using Blockchain. International Journal of Engineering Research & Technology, 9(3), 355-359.

[13] Arjomandi-Nezhad, A., Fotuhi-Firuzabad, M., Dorri, A., & Dehghanian, P. (2021). Proof of humanity: A tax-aware society-centric consensus algorithm for Blockchains. Peer-to-Peer Networking and Applications, 14(6), 3634-3646.

[14] Wang, Y., & Kogan, A. (2018). Designing confidentiality-preserving Blockchain-based transaction processing systems. International Journal of Accounting Information Systems, 30, 1-18.

[15] Hyvärinen, H., Risius, M., & Friis, G. (2017). A blockchain-based approach towards overcoming financial fraud in public sector services. Business & Information Systems Engineering, 59, 441-456.

[16] Elisa, N., Yang, L., Chao, F., & Cao, Y. (2023). A framework of blockchain-based secure and privacy-preserving E-government system. Wireless networks, 29(3), 1005-1015.

[17] Rupa, C., & Chakkarvarthy, D. M. (2021). Web-based knowledge management distributed application for medical certificates using Blockchain technology. Knowledge Management and Web 3.0: Next Generation Business Models, 2, 141.

[18] Yadav, A. S., & Kushwaha, D. S. (2021). Blockchain-based digitization of land record through trust value-based consensus algorithm. Peer-to-Peer networking and applications, 14(6), 3540-3558.

[19] Hong, H., & Sun, Z. (2021). A secure peer to peer multiparty transaction scheme based on blockchain. Peer-to-Peer Networking and Applications, 14(3), 1106-1117.

[20] Lakhan, A., Mohammed, M. A., Abdulkareem, K. H., Deveci, M., Marhoon, H. A., Nedoma, J., & Martinek, R. (2024). A multi-objectives framework for secure blockchain in fog–cloud network of vehicle-to-infrastructure applications. Knowledge-Based Systems, 290, 111576.

[21] Raghu, N., Kannanugo, N., Trupti, V. N., Ojashwini, R. N., Kiran, B., & Deepthi, M. (2025). Real-time fraud detection in crypto-currencies: Leveraging AI and blockchain. In Applications of Blockchain and Artificial Intelligence in Finance and Governance (pp. 28-66). CRC Press.

[22] Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation research part e: Logistics and transportation review, 142, 102067.

[23] Thakre, B., & Yadav, U. (2024). Evaluation of Data Management in Blockchain-based Systems. Data Management and Security in Blockchain Systems.