DEVELOPING A SECURE AND TRANSPARENT BLOCKCHAIN SYSTEM FOR FINTECH WITH FINTRUST FRAMEWORK

Avinash Singh[1], Vikas Pareek [1], Ashish Sharma [2]

[1] Department of Computer Science and Information Technology, Mahatma Gandhi Central University, East Champaran, Bihar- 845401, India.
[2] Department of Computer Science and Engineering, Manipal University, Jaipur, Rajasthan 303007, India

ABSTRACT

The rapid growth of Fintech has driven the adoption of blockchain technology for secure, efficient, and tamper-proof digital transactions. However, existing blockchain systems face challenges such as double-spending attacks, inefficient consensus mechanisms, and limited trust management, which hinder their scalability and security. To overcome these issues, this research proposes the Fin Trust Blockchain Framework (FTBF), a multi-layered architecture designed to provide secure, scalable, and transparent solutions for Fintech applications. FTBF integrates Zero Trust Architecture (ZTA) at its core to ensure continuous user, node, and transaction validation. To prevent double-spending attacks, the Dynamic Coin Flow Output Model (DCFOM) tracks unspent transaction outputs, ensuring the uniqueness of digital tokens. The framework also introduces a novel consensus mechanism, the Time Elapsed Stake Secure Algorithm (TESSA), which enhances scalability and energy efficiency. Additionally, the Fair Trust Rating Server (FTRS) dynamically calculates and updates trust scores for network participants, storing them on a trust score ledger for transparency and accountability. FTBF addresses key blockchainsecurity, efficiency, and trust management limitations, paving the way for next-generation Fintech solutions with enhanced scalability, resilience, and transparency.

KEYWORDS

Fintech, FinTrustBlockchain Framework, Zero trust Architecture, Consensus mechanism, Dynamic Coin output Model, Digital tokens, Trust Score.

1. INTRODUCTION

The financial technology (FinTech) business has grown rapidly in recent years, driven by technological developments to improve and streamline financial services [1]. One of the most significant technologies to emerge in this field is blockchain, a decentralized, distributed ledger system that allows for secure, transparent, and immutable record-keeping. Blockchain has disrupted established financial institutions by introducing new ways to perform transactions, secure data, and increase transparency [2]. Its use in FinTech has led to new opportunities for peer-to-peer payments, digital currencies, smart contracts, and decentralized finance (DeFi), among other innovations [3].At its core, blockchain stores data in a blockchain that is securely linked to prevent tampering [4]. Each transaction or piece of information recorded on the blockchain is validated by network participants using a consensus method to ensure its legitimacy and integrity [5]. This decentralized model eliminates the need for intermediaries like banks and payment processors, which lowers transaction costs, increases efficiency, and improves security[6]. These properties make blockchain ideal for FinTech applications that value trust,

speed, and cost-effectiveness.One of the most well-known blockchain applications in FinTech is the development and maintenance of digital currencies like Bitcoin and Ethereum [7]. These cryptocurrencies are based on blockchain technology, creating a secure, decentralized platform for exchanging value without a central authority [8]. Using digital currencies in FinTech has created new financial goods and services such as cryptocurrency exchanges, digital wallets, and decentralized apps (dApps) [9]. The significance of blockchainin facilitating secure and transparent transactions has also contributed to the emergence of DeFi, a movement aimed at replacing traditional financial intermediaries with smart contracts and blockchain-based protocols [10].Beyond cryptocurrencies, blockchain technology improves financial services such as remittances, cross-border payments, and loans. Traditional remittance methods frequently have high costs, poor processing times, and rely on intermediaries [11]. Blockchain-based solutions, on the other hand, enable faster and more cost-effective cross-border payments by eliminating middlemen and simplifying foreign exchange operations [12]. Similarly, blockchain is revolutionizing the lending business by enabling peer-to-peer lending platforms, allowing individuals to borrow and lend money directly without using traditional banks as intermediaries [13]. Smart contracts are performed automatically when predetermined criteria are satisfied, guaranteeing that all parties abide by the agreed-upon terms without manual intervention [14]. In the financial sector, smart contracts are used for various objectives, including automating insurance claims, streamlining trade financing, and improving clearing and settlement processes [15]. By eliminating the need for middlemen and automating complicated operations, smart contracts have the potential to drastically reduce costs and increase operational efficiency in the financial industry.

Despite blockchain's multiple benefits to FinTech, its adoption is not without obstacles [16].Scalability, legal ambiguity, and security concerns impede its incorporation into conventional financial institutions. The energy consumption associated with certain consensus processes, such as proof-of-work, is also an environmental concern [17]. However, ongoing improvements in blockchain technology, such as creating more energy-efficient consensus algorithms and forming clearer legal frameworks, are assisting in addressing these issues and paving the way for wider implementation [18].Blockchain technology is changing the face of financial transactions by providing a decentralized, secure, and transparent alternative to established methods. Its FinTech applications are wide, including cryptocurrencies, cross-border payments, smart contracts, and decentralized financing [19]. While obstacles persist, blockchain has enormous potential to change the financial industry, and its continuing evolution promises to drive even more innovation in the field. As blockchain technology improves and gains traction, it is expected to play an increasingly important role in the future of financial transactions, creating new opportunities for businesses, consumers, and investors alike.However, systems in FinTech face several limitations that hinder their scalability, security, and overall performance. One major issue isscalability, as many current blockchain networks struggle with handling high transaction volumes due to inefficient consensus mechanisms and limited throughput. This results in slow transaction processing times and increased costs, especially during periods of high demand. Additionally,double-spending attacksremain a critical concern, with many systems being vulnerable to fraudulent activities where the same digital token can be spent multiple times, undermining trust and security.Trust managementis another limitation, as existing systems often rely on static trust models that fail to dynamically assess and update the trustworthiness of network participants, leaving room for malicious actors to exploit vulnerabilities. Moreover, certain consensus algorithms, such as proof-of-work, consume significant energy, raising environmental concerns by addressing these issues and introducing a novel approach to continuously validate users and nodes to enhance energy efficiency and scalability while ensuring high transaction throughput. These improvements aim to make blockchain systems more secure, efficient, and scalable for FinTech applications.The key contribution of this proposed work is as

follows: to provide a comprehensive solution to the existing challenges in Blockchain systems for FinTech promoting secure, efficient and scalable digital transactions,

- A novel framework FTBF designed to enhance security, scalability and transparency in FinTech by integrating advanced blockchain.
- A dynamic trust management system based on ZTA that ensures continuous validation of users, nodes, and transactions, removing assumptions of inherent trust and strengthening the overall security posture.
- A new approach, DCFOM, is introduced to preventdouble-spending attacks by efficiently tracking unspent transaction outputs, ensuring the integrity and uniqueness of digital tokens in the system.
- A TESSA algorithm improves energy efficiency and scalability while maintaining high transaction throughput in blockchain networks.
- A dynamic system that computes and updates trust scores for all participants based on their behaviours and actions, ensuring that access and transaction approval are contingent upon the trustworthiness of entities.

The structure of this research document is organized into several key sections; following the introduction, section 2 provides the literature review, which discusses existing studies, identifies the research gap and establishes the need for the proposed framework. Section 3 presents the definition of the problem and outlines the key issues. Section 4 details the proposed methodology and explains the architectural design and components of FTBF. Section 5 outlines the implementation and experimental setup and provides the results. Finally, Section 6 concludes with a conclusion and a discussion of future work.

2. LITERATURE REVIEW

The application of blockchain technology in the financial sector has gained significant traction due to its potential to enhance security, transparency and efficiency. Several researchers have explored diverse methodologies and frameworks to address various challenges in Fintech, banking and data security.

Rjoub et al. [20] exploredusingblockchain-based financial technology (FinTech) in the banking industry to overcome transition difficulties. Their research looked at important FinTech aspects that influenced the success of Chinese banks. They suggested an adaptive neuro-fuzzy-based K-nearest neighbour's method optimized with a chaotic enhanced foraging algorithm to improve predictive accuracy. However, the study has some drawbacks, including a reliance on specific FinTech elements that may not be applicable to other banking scenarios. Furthermore, the chaotic nature of the optimization process caused possible convergence concerns, and the rolling window model encountered challenges in capturing abrupt, significant scale shifts in FinTech growth.Gai et al. [21] proposed a blockchain-based access control mechanism using a consortium blockchain, Role-Based Access Control, multi-signature protocols, and smart contracts to enable secure and efficient data exchange. Tested on the HyperLedger Fabric platform, the solution proved effective but faced challenges, including scalability issues for large networks, limited compatibility with public blockchains, and performance concerns due to the computational complexity of multi-signature protocols.

Chaudry et al. [22] developed a blockchain-based algorithm for online transactions that protects bank resources from malicious users and secures transactions using a zero-trust security method. The framework and algorithm were created based on previous research and literature reviews. The idea was to improve financial security by implementing blockchain technology and zero-

trust principles. However, scalability issues may occur as the framework evolves to handle higher transaction volumes, and reliance on blockchain consensus methods may increase latency during peak periods.Liu et al. [23] proposed a blockchain-enabled information-sharing solution for zero-trust scenarios, ensuring anonymity, data privacy, trustworthiness, and equitable participant stimulation. The approach used smart contracts for filtering falsified information and effective voting and consensus methods to prevent misinformation. Security was verified using the universal composability framework, and performance was evaluated on an Ethereum-based platform. However, reliance on Ethereum raises concerns about transaction costs and network congestion in large-scale scenarios.

Song et al. [24] introduced blockchain technology to design a four-layer architecture and multiple trust evaluation indicators based on blockchain service data. They proposed a blockchain-based FinTech trust evaluation mechanism (BFTEM), which records relevant data and multiple trust parameters during block transmission. The mechanism verifies the trust degree issued by the trust holder through a comprehensive trust value of the user. Simulation experiments showed that the BFTEM mechanism improved the security and reliability of FinTech data, enhancing trust evaluation accuracy and expanding its potential applications. However, the mechanism's vulnerability to double spending attacks and reliance on blockchain data makes it vulnerable to inaccuracies or manipulation during transmission.Wang et al. [25] introduced a Software Defined Perimeter solution within Zero Trust Architecture (ZTA) to enhance security for financial trading terminals. By relocating security protection to the user access layer, the solution eliminates VPNs, boosts remote access security, and improves transaction security. Key achievements include deep integration with transaction systems, minimal impact on terminal performance, tailored security setups, and advanced technologies like single-packet authorization and secondary authentication. However, further exploration is needed to address scalability and adaptability to rapidly emerging cyber threats.

Song et al. [26] created a Multi-Dimensional Trust Index System and Evaluation Mechanism (MDTEM) for FinTech that considers direct, indirect, recommendation, and feedback trust. To improve financial services' security, reliability, and trustworthiness, a four-level blockchain structure was developed, includingblockchain at the cloud, internet, contract, and application levels. Trust simulation research revealed that the MDTEM considerably improved the security and dependability of FinTech trust applications. However, limited trust management capabilities made conducting consistent trust evaluations in large-scale, dynamic FinTech systems difficult.Bahar et al. [27] developed a Metric-Based Feedback Methodology (MBFM) for improving corporate security by combining bug bounty programs with threat modelling. The methodology aids in identifying root causes and refining threat models, hence improving the effectiveness of security measures. The study defines the methodology's assumptions and is a foundation for future research. However, it necessitates continual updates to threat models, which presents scalability issues for large and dynamic systems.

This reviewed existing literature illustrates the diverse applications of blockchain technology and Zero Trust principles in FinTech, banking, and access control systems. While significant progress has been made in enhancing security, scalability, and efficiency, several critical gaps remain. These include challenges related to scalability in large networks, where existing frameworks often struggle to handle high transaction volumes and achieve optimal throughput. Furthermore, system latency continues to be an issue, particularly in blockchain solutions relying on heavy consensus protocols like proof-of-work, which can increase delays during peak transaction periods. Convergence issues in optimization, especially in chaotic or complex algorithms, lead to suboptimal solutions and decreased performance. Additionally, existing systems remain vulnerable to double-spending attacks, where digital tokens may be fraudulently used more than once, undermining the integrity of transactions. Limited trust management in many blockchain-

based solutions remains a concern, as many rely on static or simplified trust models that fail to assess and update participant trustworthiness dynamically. The proposed framework addresses these gaps to improve scalability and energy efficiency while enhancing system performance. These advancements aim to fill the gaps identified in the literature, providing a more secure, scalable, and efficient solution for large-scale financial systems.

3. PROBLEM DEFINITION

The growing adoption of blockchain technology in FinTechhas revealed several significant issues affecting blockchain-based financial systems' efficiency, security, and scalability. Despite the promise of decentralization and immutability, blockchain platforms have intrinsic constraints preventing widespread use. This section discusses the key concerns the FinTrustBlockchain Framework (FTBF) seeks to address, such as double-spending attacks, inefficient consensus techniques, and limited trust management. Bahar et al. [27] developed a Metric-Based Feedback Methodology (MBFM) for improving corporate security by combining bug bounty programs with threat modelling. The methodology aids in identifying root causes and refining threat models, hence improving the effectiveness of security measures. The study defines the methodology's assumptions and is a foundation for future research. However, ongoing upgrades to threat models posing scalability challenges for large and dynamic systems are required. One of the most serious security concerns in blockchain systems is the possibility of double-spending attacks, in which a single digital token is spent more than once. This occurs when malicious users leverage network slowness or computational delays in transaction validation to create duplicate tokens. Traditional blockchain frameworks use Proof-of-Work (PoW) or Proof-of-Stake (PoS) procedures to protect against such attacks. However, these approaches are computationally demanding and vulnerable to fork-based attacks that jeopardize system integrity. Blockchain networks rely on consensus methods to ensure agreement on the authenticity of transactions. Traditional systems, such as PoW, need a lot of energy, but PoS has concerns with "rich-get-richer" dynamics. These inefficiencies lead to slower transaction processing, significant computing overhead, and limited scalability.Financial transactions rely heavily on trust, particularly in decentralized blockchain contexts where participant anonymity is frequent. Existing blockchain systems frequently rely on implicit trust, which hostile nodes can exploit to launch Sybil attacks or initiate fraudulent transactions. The absence of ongoing trust evaluation and verification undermines openness and system accountability. Thus, the proposed framework addresses these issues by introducing innovative techniques to enable a secure, efficient, scalableblockchain framework for FinTech applications.

4. PROPOSED METHODOLOGY

The proposed FinTrustBlockchain Framework (FTBF) is a robust, secure, and scalable blockchain solution that aims to address the shortcomings of current blockchain-based FinTech systems. Traditional blockchain systems face a number of significant difficulties, including vulnerability to double-spending attacks, inefficient consensus techniques that result in high computing costs, and inadequate trust management, which diminishes system transparency and security. The FTBF proposes a multi-layered architecture with advanced components and unique methodologies to address these difficulties. The DCFOM reduces double-spending by tracking Unspent Transaction Outputs in real-time, ensuring that each digital token is only spent once. TESSA improves consensus efficiency by combining PoS with PoET, lowering computing overhead and energy usage. The framework uses a ZTA to manage trust, requiring every user, node, and device to undergo continuous verification before access is permitted. Additionally, the FTRS dynamically reviews and updates trust scores for users and nodes, which are then recorded in an immutable Trust Score Ledger on the blockchain. This comprehensive trust structure

ensures responsibility and deters fraudulent activities. The architectural design of FTBF in Figure 1 is based on a multi-layered blockchain architecture to ensure modularity, scalability and efficient transaction processing.

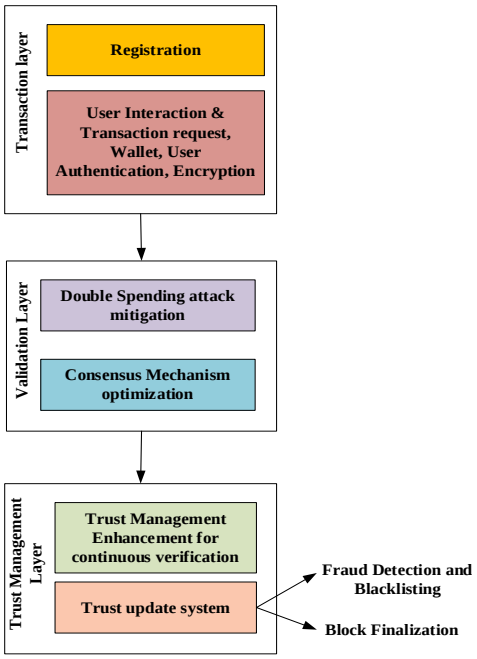

Figure 1: Architecture of Proposed Work

The architectural design of FTBF in Figure 1 is based on a multi-layered blockchain architecture to ensure modularity, scalability, and efficient transaction processing. In Figure 1, the system architecture is divided into three primary layers: (1) Transaction Layer: Handles user interactions, transaction creation, and encryption via RSA before sending the data to the validation layer. (2) Validation Layer: Ensures transaction validity, prevents double spending through the DCFOM, and employs the TESSA algorithm for energy-efficient consensus. (3) Trust Management Layer: Enforces ZTA for continuous identity verification and uses the FTRS to maintain and update trust scores recorded in the blockchain-based Trust Score Ledger. These layers work together to provide a secure, efficient, and scalable infrastructure for FinTech applications.

4.1. Transaction Layer

This layer is the entry point of user interaction with the blockchain. It facilitates transaction creation, user authentication and secure submission of transaction requests. This layer manages user interactions, transaction initiation, data encryption and secure transfer of transaction details to the subsequent validation layer. This layer establishes a safe and user-friendly environment for transaction processing by incorporating robust encryption mechanisms and user authentication protocols. Figure 2 shows the processing flow of user interaction with the blockchain.

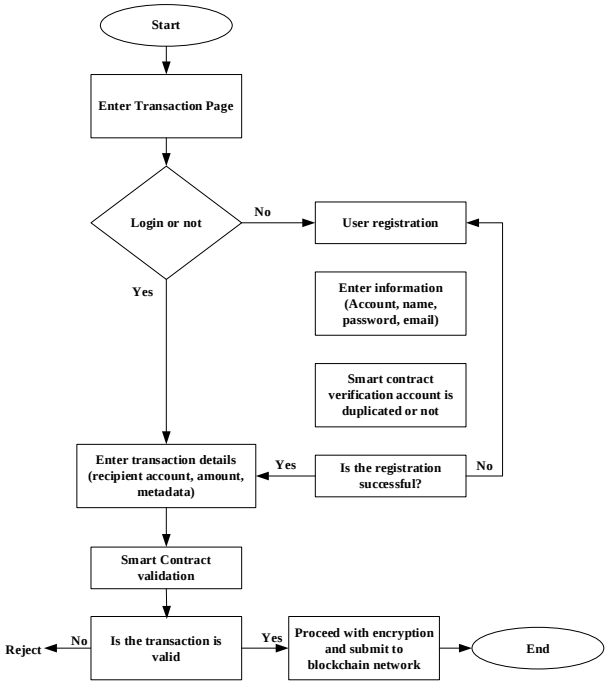

Figure 2: Initial Process of entity of blockchain

4.1.1. User Wallet and Asset Management

User Wallets are the primary interfaces for users to store, manage, and access their blockchain assets. Each user receives a secure digital wallet that stores private keys, public keys, and blockchain addresses. These wallets include multi-factor authentication (MFA) and biometric verification features to provide an extra layer of security. Users can access their wallets to monitor their transaction history, check their asset balances, and begin new transactions. Each wallet is uniquely identified by a cryptographic public-private key pair (K_{pub}, K_{priv}). The K_{pub} is openly shared and acts as an address for receiving funds, while K_{pub} is confidential and used to sign transactions.Let the balance B of a user's wallet be represented as

$$B_{user} = \sum_{i=1}^{n} UTXO_i \qquad (1)$$

Thus, user wallets play a crucial role in FTBF by storing and managing Unspent Transaction outputs (UTXOs), which represent the user's available balance. They generate and maintain the user's public-private key to enable secure encryption, decryption, and authentication of transactions. Additionally, user wallets track and display the $Buser$, providing real-time updates on available funds for seamless transactions.

4.1.2. User Authentication and Identity Verification

Before a user can initiate a transaction, the FTBF enforces a severe authentication process to ensure that only confirmed and legitimate users utilize the system. Authentication verifies the user's identity using cryptographic methods such as digital signatures and multi-factor authentication. This step is critical for preventing unwanted access and ensuring all transaction requests come from a trustworthy source. The user signs the transaction request Tusing theK_{priv}, the signature σ is generated using a signing algorithm as,

$$\sigma = Sign(T, K_{priv}) \quad (2)$$

Then, the signature σ is validated using the corresponding $Kpub$ to ensure the authenticity and integrity of the transaction request.

$$Verify(T, \sigma, K_{pub}) = True \quad (3)$$

If the verification is true, the system confirms that the transaction originated from a legitimate user.

4.1.3. Transaction Request Creation

Once a user has been authenticated, they can create a transaction request.This request provides essential transaction information, such as the recipient's blockchain address (sender K_{pub} (acting as wallet address), receiversK_{pub}), the amount to be transferred, and any necessary metadata for processing. The user is presented with a transaction preview for review and confirmation. This phase allows the user to verify the accuracy of the transaction data before submission.

4.1.4. Transaction Encryption

To ensure the confidentiality and integrity of transaction data, the FTBF uses RSA (Rivest-Shamir-Adleman) encryption. RSA is a well-known cryptographic technique for its strength and capacity to protect sensitive data. After the transaction request is confirmed, the system encrypts all transaction details, including the recipient's address, amount, and metadata, with the recipient'sK_{pub}. This encryption procedure ensures that only the intended recipient may decrypt the transaction details usingK_{priv}, safeguarding user privacy and preventing data interception. The plain text transaction T is converted into an integer m using a padding scheme, the cipher text c is generated using RSA encryption $c = m^e mod n$ where e is the public exponent of RSA key pair n is the modulus which is product of two large prime numbers. This cypher text c represents the encrypted form of transaction. The encryption ensures that the transaction cannot be intercepted or read during transmission.

4.1.5. Transaction Submission to the Validation Layer

After encryption, the transaction request is securely sent to the Validation Layer. The encrypted data is transmitted across a secure channel along with the sender's signatureσ for validation, protecting it from external risks such as eavesdropping, tampering, or interception. This transmission mechanism is enhanced by using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols to safeguard data in transit. The Transaction Layer also assigns each request a unique transaction identifier (TXID), allowing users to trace their transaction status in real-time. During the submission, the integrity of the transaction is verified using hashing. The system computes a hash $H(T)$ of transaction requests using a cryptographic hash function using RSA. The$H(T)$is stored along the transaction to ensure data integrity. If any data is modified, the computed hash will not match the stored hash, raising an alert.

4.2. Validation layer

This layer is the core processing unit of FTBF, which aims to ensure the validity of transactions, prevent double spending and achieve efficient consensus. This layer plays a vital role in verifying and validating transactions before they are permanently added to the blockchain. Through a

combination of robust functions of DCFOM and TESSA, the validation layer guarantees the system's security, integrity and efficiency.

4.2.1. Dynamic Coin Flow Output Model

DCFOM is a novel mechanism designed to track UTXOs and prevent double spending, and it monitors and maintains a time record of UTXOs within the blockchain. A DCFOM is the amount of digital cash transmitted to a crypto address or remaining after a transaction. Transactions generate new UTXOs, which can be used in subsequent transactions. Each UTXO is treated as a token, with no closing balance[28]. Transferring a UTXO from one party to another involves transferring ownership, rather than reconciling two databases. UTXO structures offer advantages over standard account models, such as increased security and the capacity to simultaneously process many transactions from a single-payer.The DCFOM reduces double-spending by tracking Unspent Transaction Outputs in real-time, ensuring that each digital token is only spent once.To facilitate reproducibility, the DCFOM implementation involves a ledger system where every transaction is cross-checked with a real-time database of UTXOs. The framework ensures that any token reuse attempt is flagged by comparing the transaction inputs against the existing set of unspent outputs. This can be implemented using a hash-based mapping of transaction outputs, enabling rapid verification of the token's state, thus preventing double spending in a transparent and traceable manner.

Consider three users: Alice, Bob, and Charlie. Their private keys, public keys, and wallet addresses are $\{\delta A, \beta A, \mu A\}$, $\{\delta B, \beta B, \mu B\}$, and $\{\delta C, \beta C, \mu C\}$, Alice has a UTXO of 15 coins. She sends 10 coins to Bob (μB) and receives 5 coins as a change to her sending address (μA). During transaction $1Tx1$, Alice must prove ownership of the input address. To verify ownership, she supplies her public key (βA) and a signature generated by signing $Tx1$ with her private key (δA). Verifying the signature using (βA) confirms that the owner has the corresponding private key for(μA). Similarly, Bob transfers 6 coins to Charlie μC from Alice's UTXO and receives a reimbursement of 4 coins. Both transactions are maintained on a blockchain accessible to all network participants. During the initial transaction, Alice recognizes that μB belongs to Bob. However, this transparency creates a potential privacy risk as Alice or others can track all transactions associated withμB, revealing Bob's balance [29].To mitigate such privacy risks, DCFOM changes the wallet address after each transaction, making it more difficult to trace transaction history or link balances to specific users. When initiating a new transaction, the DCFOM verifies whether the related outputs have already been spent. If duplicate outputs are detected, the transaction is flagged for further examination. Furthermore, the Trust Management Layer may face penalties or increased scrutiny on the user or node responsible for the duplicate outputs. This system assures no token or coin is used more than once, prohibiting fraudulent conduct like double-spending. This solution improves blockchain transaction security and anonymity by combining robust tracking and verification processes with advanced privacy measures.

4.2.2. Time Elapsed Stake Secure Algorithm

TESSA is a hybrid consensus mechanism that combines the strengths of PoS and Proof of Elapsed Time (PoET) to achieve fast, energy-efficient and secure consensus. The PoS component selects validators based on the proportion of participants' tokens or stakes. This method ensures that users with a higher stake are more likely to be chosen as validators. By rewarding stakeholders, PoS inherently encourages active participation and honest behaviour within the network, reducing the risk of Sybil attacks and improving overall network security[30].PoS mechanisms offer faster transaction confirmation than PoW mechanisms, in addition to their low energy consumption. In a blockchain network, transaction confirmation is based on transaction

throughput and block confirmation time. Transaction throughput (TXs) is important for network performance, especially when there are many pending transactions[31]. TXscan be calculated as

$$TXs = \frac{Block_{size}}{Tx_{size} \times Block_{time}} \quad (4)$$

On the other hand, the PoET component introduces unpredictability and randomness into the selection process. Based on Intel's Software Guard Extensions (SGX), Intel proposes Sawtooth Lake, which uses "proof-of-elapsed-time" (PoET) to regulate the building of new blocks [32]. In PoET, each participant is given a random waiting period, and the person whose timer runs out first is chosen as the validator for the following block. This unpredictability prevents any person from controlling the validation process, maintaining fairness and impartiality[33]. In contrast to PoW, PoET does not require energy-intensive mining, making it a more sustainable approach to consensus. TESSA improves consensus efficiency by combining Proof of Stake (PoS) with Proof of Elapsed Time (PoET), lowering computing overhead and energy usage. The implementation of TESSA involves setting up a hybrid consensus model where nodes participate in validating transactions by staking tokens for PoS while using TEEs to generate random timers for leader election in PoET. The PoS mechanism determines validators based on token holdings. PoET ensures that leader selection is secure and energy-efficient by utilizing trusted execution environments that generate unpredictable wait times, reducing the overall computational burden. When a new block is validated, TESSA uses a combination of PoS and PoETto select a validator, enabling the network to strike a balance between efficiency and justice. The chosen validator verifies the transactions within the block to ensure they meet all required conditions, such as the absence of double spending, sufficient account balances and proper cryptographic signatures. Once the transactions are verified, the validator finalizes the block and adds it to the blockchain. This process is faster and more energy efficient than traditional PoW mechanisms. For reproducibility, the setup involves defining a protocol for node selection based on pre-set criteria for PoS and configuring the TEE environment for random time generation. Detailed parameters for both mechanisms, such as the staking amount for PoS and the minimum execution environment requirements for PoET, can be standardized to ensure the system's consistency across implementations.

4.3. Trust Management Layer

This layer is critical to preserving the blockchain network's integrity, security, and dependability by constantly monitoring and assessing the behaviour of nodes, users, and transactions. This layer is built on ZTA, a security concept in which no internal or external entity is trusted by default. Instead of implicitly trusting nodes after initial verification, ZTA mandates continual verification and re-evaluation of all participant activities and transactions to ensure compliance with set security guidelines. This technique reduces the danger of unauthorized access or potential security breaches by implementing a dynamic and watchful trust management system. Fig. 3 illustrates a model that integrates zero trust principles and blockchain technology. Blockchain technology enables decentralization and immutability of data, while zero trust principles are used for access control and authorization where no user, device, or node is trusted by default, and trust is continuously verified and recalculated.To develop a trust management system for blockchain-enabled environments using FTRS, a critical component in computing and updating the trust scores of users and nodes.

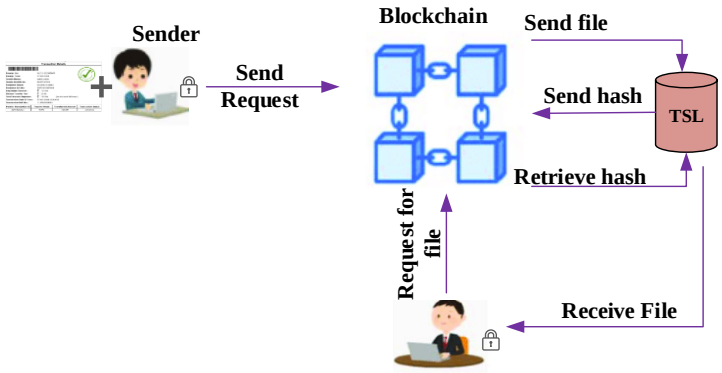

Figure 3: Integration of Zero Trust with Blockchain for Fintech

The FTRS calculates and manages these trust scores, offering a transparent and tamper-proof mechanism for monitoring network participants' trustworthiness. Then, it continuously analyses activity and flags questionable behaviour, modifying nodes' trust levels accordingly. The Trust Score Ledger (TSL), which is kept on the blockchain, provides an immutable record of trust scores and acts as the foundation for executing access control regulations based on trust level. Table 1 lists several components along with their descriptions for calculating the trust score.

Table 1: Components and Description used for Trust score calculation

Component	**Description**
FTRS	The centralized or distributed unit responsible for calculating trust scores using zero-trust principles
User/Nodes	Participants in the system that request access to resources or interact with blockchain
Data Collector	Gathers data from user activities, access logs, node behaviour and transaction history
TSL	A secure blockchain-based ledger where trust scores and access logs are recorded for transparency and traceability.
Access control gateway	Validates trust scores before granting access to blockchain resources.

The FTRS in a ZTA ensures dynamic and safe access control by constantly reviewing trust ratings for users and nodes. The process begins with initialization, which determines critical characteristics such as user behaviour, access history, and anomaly status. The features $(F_1, F_2, \ldots F_n)$ are normalized to guarantee consistency in calculations. Each attribute is allocated a weight $(w_1, w_2, \ldots w_n)$based on its relevance, ensuring the aggregate of weights equals 1 $(\sum w = 1)$. Trust score thresholds () are also specified to help with access decisions.Once initialized, the trust score T_i for each user or node i is computed using the formula,

$$T_i = w_1.F_1 + w_2.F_2 + w_3.F_3 + \cdots .w_n.F_n \qquad (5)$$

This technique dynamically combines weighted feature values to generate an overall trust score. For example, a node with regular behavioural patterns and a good access history will obtain a better trust score. In contrast, anomalies or deviations from predicted behaviour reduce the score.The trust update method ensures scores remain relevant by tracking and incorporating real-time changes. User actions such as successful logins raise the score, while failed attempts lower it. Behavioural monitoring detects departures from usual patterns and updates the score accordingly. Updates to device health, such as installing security patches, impact the trust score. Any detected anomalies, such as unauthorized access attempts or irregular activities, will result in

sanctions. Each update is stored on a blockchain-based TSL, guaranteeing immutability and transparency. The ledger records the timestamp, updated trust score, the reason for the change, and magnitude of adjustment (ΔT).Access decisions are made based on the updated trust score. If $T_i \geq \tau_{grant}$, the user or node gains access. If $T_i < \tau_{grant}$, access is refused and the node is marked for review. If a node's score falls below τ_{deny}it is considered potentially fraudulent and may be blacklisted or investigated further. Persistently low trust scores across many time frames result in block finalization, which prevents malevolent nodes from accessing the system.

$$\text{For Grant access,} \quad Access\ Decision = \begin{cases} Grant, & if\ T_i \geq \tau_{grant} \\ Deny, & T_i < \tau_{grant} \end{cases} \tag{6}$$

If T_i falls below τ_{deny}, the node is flagged as a potential insider threat or malicious actor.
This structured and dynamic approach has numerous key advantages; dynamic trust updates ensure that trust scores are updated depending on user behaviour and transactional patterns, allowing for flexible decision-making. The system prohibits implicit trust by adhering to ZTA principles, effectively decreasing insider risks. The FTRS's scalability enables it to manage thousands of users and devices simultaneously, providing seamless operation even in large-scale networks. Enhanced access control is achieved by restricting access to low-trust users or nodes, reducing the danger of illegal activity. Furthermore, a blockchain-based TSL ensures transparency and auditability by keeping a secure and immutable record of trust score revisions. Together, these traits enable the FTRS to mitigate insider threats, enhance access control and maintain robust security, which allows ZTA to function effectively in dynamic and complex environments.

5. RESULTS AND DISCUSSION

In this research, Python is utilized in the simulation experiment to analyse blockchain performance in FinTech, as it is a popular simulator for testing mobile networks and payments. Experimental analysis uses data from banking institutions and FinTech companies and computer simulations. The simulation experiment setup includes 10 servers and 200 FinTech users. FinTech users are spread across a $10km \times 10km$ radius for data processing and transmission. The user trust rates are $70\%, 80\%, and\ 90\%$, respectively. Simulation experiments can run on an average of $500\ seconds$, resulting in $200\ FinTech$transfers every second. Execute numerous simulations with different parameter values for each scenario, then average the results. FinTech users' payment arrival times reflect the Poisson distribution based on normal random variables. The essential parameters are listed in Table 2.

Table 2: Listing of Essential Parameters

Parameter	**Value/Range**
Number of Fintech users	200
Number of Servers	10
Transmission radius of Fintech user	500m
Encryption method	RSA (2048 bit)
Transaction size	250B, 500B, 1KB
Number of Fintech transactions per second	100/s
User Authentication	Public Key Infrastructure
Transaction timed out	60s
Simulation time	500s
Trusted service values	80%
Maximum number of Attacks	1000

In the FTBF trust evaluation simulation experiment, data transmission increases from 1×10^3 to 10×10^3. The verification time for FinTech data transfer is defined by the time it takes to calculate the suggested value based on blockchain trust value. Validation and request processing times scale linearly with transaction and query volume. The trust assessment mechanism allows numerous trust evaluations to be applied to the same FinTech data processing. Each trust evaluation may be specified based on the trust needs associated with that process.

5.1. Performance Parameters

- **Block Generation:** The time required to create and add a new block to the blockchainis influenced by block size, transaction processing speed and consensus mechanism efficiency.
- **Trust Rate:** The percentage of honest or trustworthy nodes actively participating in blockchain impacting system reliability, node selection and resistance to Sybil attacks.
- **Delay:** The total time taken from the transaction initiation to its final confirmation in blockchain, including network propagation, validation and block finalization.
- **Throughput:** The number of transactions successfully processed and confirmed per second, reflecting the network's ability to handle large transaction volumes efficiently.
- **Comprehensive Trust Value:**This holistic measure of a node’s trustworthiness is calculated using historical behaviour, successful validations, and ensuring secure and fair participation.

5.2. Simulation Results Analysis

The simulation results of FTBF are analyzed to assess its performance in terms of block generation, trust rate, throughput and delay. The proposed system is evaluated under varying network conditions, node participation and transaction loads. The analysis shows that FTBF significantly decreases block generation time due to its efficient hybrid consensus mechanism and simplified transaction validation process. The trust rate is constantly high, thanks to the ZTA and FTRS, which ensure that only trustworthy nodes participate in consensus. Throughput increases, suggesting greater transaction processing capability, while time is reduced due to effective processing at the Validation Layer. The comprehensive trust value emphasizes the framework's capacity to keep the network intact and fair across nodes.

Figure 4 demonstrates the relationship between block generation time and the number of FinTech users across varying trust levels (70%, 80%, and 90%). The analysis reveals that the trust levels influence the efficiency of block production in the FTBF. As trust values increase, block generation time decreases significantly. This is attributed to the faster validation and consensus process facilitated by the hybrid TESSA mechanism and enhanced trust management protocols. The graph shows a clear trend: higher trust levels reduce block generation time, particularly as the number of users increases. As trust levels rise, block creation time drops by up to 90%, highlighting the FTBF's capacity to maintain high efficiency even in large-scale FinTech environments. This improvement is further supported by the integration of DCFOM and TESSA, which improves scalability and reduces computational overhead, making the system more adaptable to the increasing size of networks. The results indicate that the FTBF, with its innovative trust-based mechanisms, is well-suited for handling the demands of large FinTech applications without compromising performance.

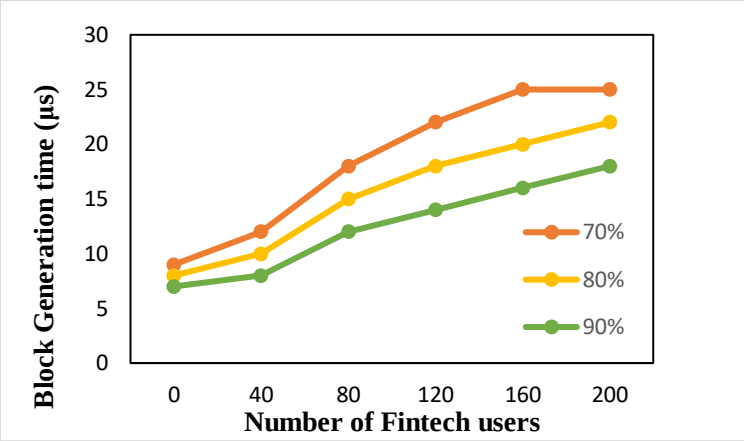

Figure 4: Block generation time analysis

Figure 5 illustrates the variation in trust rates within FinTech systems at initial trust levels of 70%, 80%, and 90% as the number of attacks increases from 0 to 1000. The adaptive behaviour of the Trust Management Layer is evident from the results, as the trust rate for each initial trust value increases despite the rise in attack frequency. This adaptation is attributed to the system's ability to adjust trust computations and dynamically reinforce resilience against malicious behaviour. The graph highlights that systems with higher initial trust levels, such as 90%, demonstrate remarkable stability under attack scenarios, maintaining a trust rate exceeding 95% even after 1000 attack incidents. This implies that the FTBF's mechanisms, including its Trust Management Layer and hybrid TESSA framework, effectively mitigate the impact of repeated attacks by quickly adapting and recalibrating trust evaluations. Furthermore, the results indicate a significant advantage for systems with higher baseline trust values, as they exhibit superior performance and reliability under stress. This stability enhances user confidence in the system's robustness, even in sustained cyberattacks. The findings emphasize the FTBF's capability to ensure trust and reliability in large-scale FinTech networks, making it a resilient solution for secure and efficient operations in dynamic and adversarial environments.

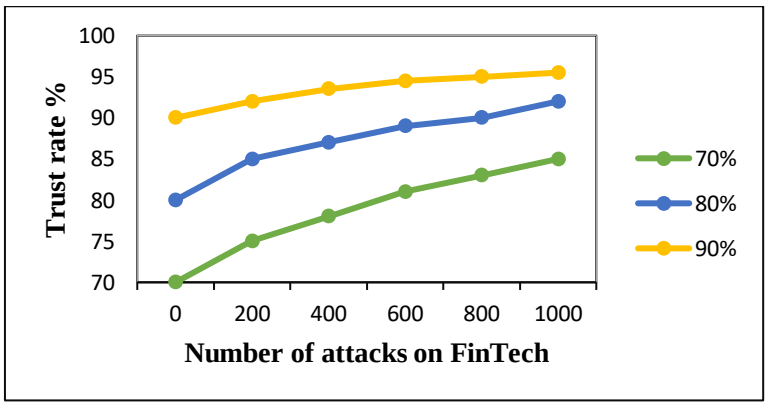

Figure 5: Trust rates under three trust values

Figure 6 illustrates the variation in blockchain computation time as transactions increase under varying conditions. The results reveal a proportional relationship between the number of transactions and the computation time, highlighting the system's scalability challenges under higher transaction loads. The computation time begins at approximately 10 seconds for 5 transactions, increases to around 20 seconds for 10 transactions, reaches 25 seconds for 15

transactions, and rises to 40 seconds for 20 transactions.This increasing trend demonstrates that while the FTBF framework can handle a growing number of transactions, the computation time scales upward linearly, reflecting the computational complexity associated with validating and recording transactions on the blockchain. This trend underscores the importance of introducing optimization mechanisms, such as parallel processing or dynamic load-balancing techniques, to enhance the efficiency of blockchain operations under high transaction volumes.The findings highlight the need for further refinement in the FTBF system to address potential bottlenecks and maintain performance consistency in real-world applications with substantial transaction demands. These results emphasize the system's scalability while pointing out opportunities for improving processing speeds to support larger-scale FinTech deployments effectively.

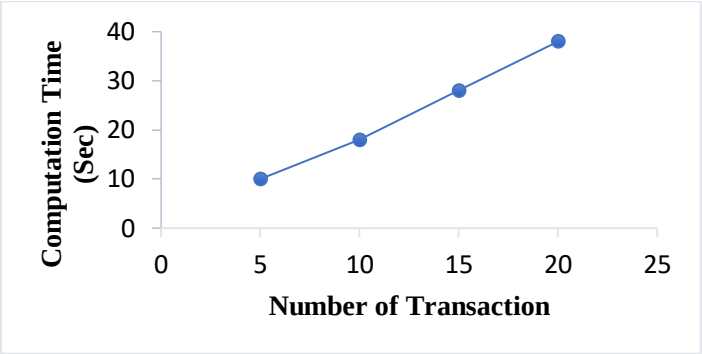

Figure 6: Computation time vs. number of transactions

5.3. Comparative Analysis

Figure 7 compares the throughput performance of four trust algorithms such asEFMCDM [37], STBC [36], BFTEM [24], and the proposed FTBF as the number of FinTechusers scales from 20 to 200. Throughput, measured in Kbps, increases across all frameworks with higher user loads, demonstrating the scalability of these systems. The results show that EFMCDM starts at approximately 250 Kbps and reaches 650 Kbps with 200 users, indicating moderate scalability. STBC performs slightly better, starting at 270 Kbps and peaking at 700 Kbps. BFTEM outperforms EFMCDM and STBC, achieving 300 Kbps initially and scaling to 750 Kbps. However, the proposed FTBF framework consistently outperforms all three, starting at 320 Kbps and achieving 850 Kbps at 200 users. This superior performance is attributed to the optimized communication protocols and advanced load-handling mechanisms within the FTBF framework, enabling it to efficiently manage the increased user traffic without significant performance degradation. The results clearly demonstrate FTBF's ability to deliver greater throughput, ensuring its suitability for high-demand environments in the FinTech domain. The findings emphasize that FTBF supports scalability and provides enhanced performance under high user loads, making it a robust and efficient solution for modern FinTech applications. These results validate the framework's design principles and ability to outperform existing trust algorithms in throughput performance.

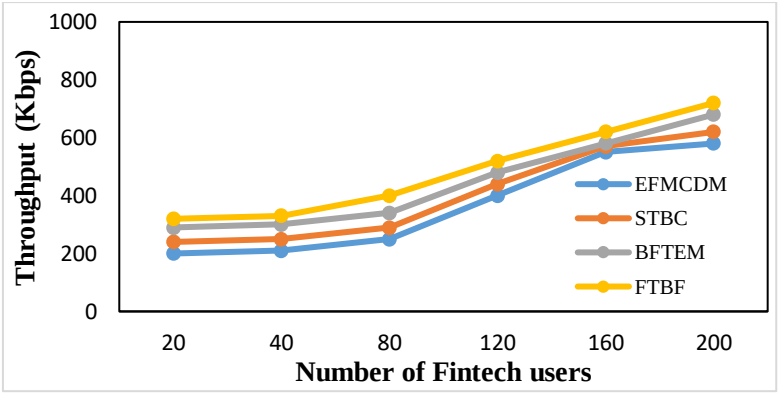

Figure 7: Comparison of throughput for different trust algorithms

Figure 8 compares delayed response times for four algorithms, EFMCDM, STBC, BFTEM, and the proposed FTBF,against varying FinTech data transmission times. The results indicate that the proposed FTBF framework demonstrates the lowest delayed response times, making it the most efficient among the compared algorithms. EFMCDM exhibits the highest delayed response times, beginning at 4.5 µs and increasing to 6.5 µs as transmission time grows. STBC follows a similar trend, with delays starting at 4.2 µs and peaking at 6.2 µs. BFTEM offers better performance, starting at 3.9 µs and reaching 5.8 µs under maximum data transmission conditions. In contrast, the proposed FTBF framework consistently outperforms the others, achieving the shortest response times, starting at 3.5 µs and increasing to just 5.5 µs as data transmission time rises. The lower delayed response times observed with the FTBF framework result from its optimized communication protocols and adaptive load-balancing mechanisms, which ensure faster and more reliable communication even under high data transmission loads. These results underscore FTBF's capability to minimize latency, making it a robust and efficient solution for real-time FinTech applications. This comparison highlights the superiority of the FTBF framework in providing faster responses and maintaining reliability in dynamic and high-demand FinTech environments, showcasing its potential to enhance user experiences and operational efficiency.

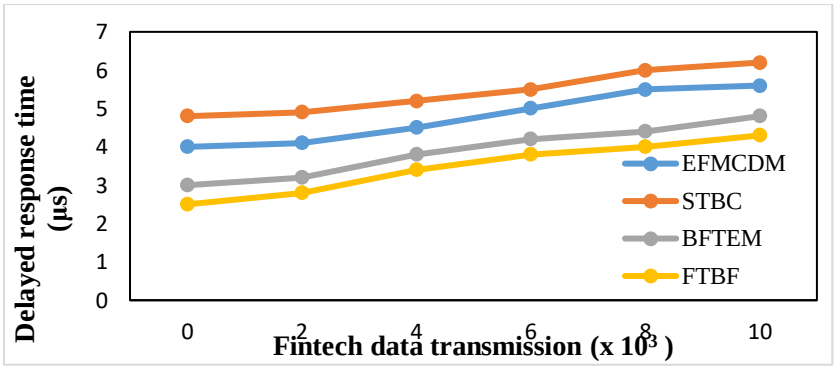

Figure 8: Comparison of delay response time

Trust value comparison during payment operations across different trust algorithms such as MDTEM [26], DREAMS [34], and TM-GT [35] highlight the effectiveness of blockchain-based ZTA. As shown in Figure 9, the trust evaluation index of the ZTA regularly outperforms the other techniques, demonstrating that it can ensure data integrity and reliability. Notably, the trust value of the sent information increases proportionally when the service provider sends more data, showing the Zero Trust approach's scalability and robustness. The proposed FTBF-based ZTA greatly enhances the trustworthiness of data transmission by utilizing blockchain

technology, ensuring secure and reliable communication even in circumstances with high data volume.

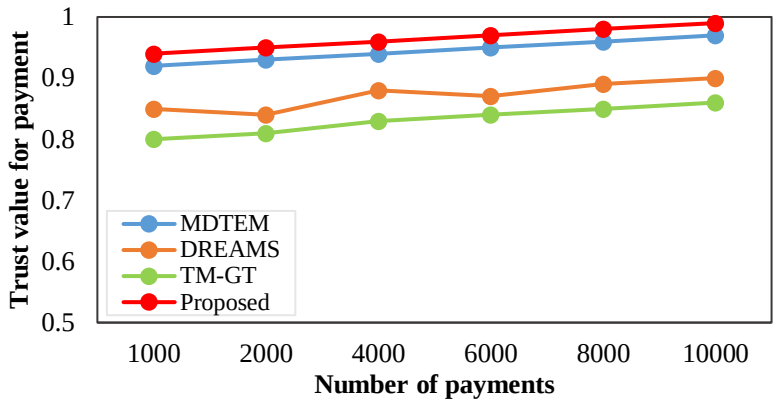

Figure 9: Trust Value for Payment Comparison

Figure 10 shows that the trust value of the ZTA transfer payments regularly outperforms existing approaches like MDTEM, DREAMS, and TM-GT. This demonstrates its superior capacity to maintain data integrity and security throughout payment processes. The results show that as the volume of information the service provider exchanges increases, the trust value continuously increases. This trend demonstrates the Zero Trust approach's strength and versatility in controlling data transfer with high accuracy and confidence. The Zero Trust framework uses blockchain technology to improve the integrity and transparency of the payment process, ensuring secure communication even in complicated and large-scale situations. In contrast, MDTEM, DREAMS, and TM-GT function moderately, but they fail to maintain constant trust when data transfer volumes increase. However, the FTBF-based ZTA, which can dynamically validate and protect transactions, makes it a more dependable choice for modern payment systems, as evidenced by the data presented in Figure 9.

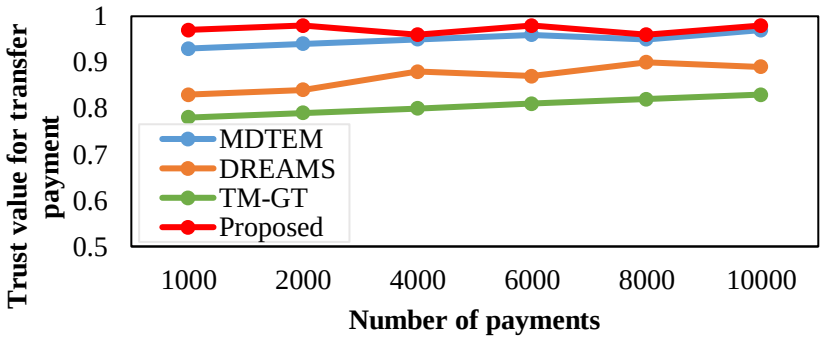

Figure 10: Trust value for transfer payment comparison

Furthermore, comparing the trust value of receiver payments across various trust algorithms proves its capacity to ensure the reliability and security of payment information received by end customers; the results show that the Zero Trust architecture's trust value steadily increases as the volume of payment-related data grows. This trend demonstrates the framework's ability to sustain high data integrity and trustworthiness levels during receiver-sided interactions. In comparison, MDTEM, DREAMS, and TM-GT have slower trust value growth, demonstrating

challenges in effectively handling large-scale, secure data transfer. The proposed FTBF-based ZTA enables a more transparent and safe payment process, especially on the receiver side, where confidence is critical. The dynamic verification processes built into blockchain improve its capacity to adapt to increased transaction volumes while ensuring constant and dependable trust levels. This positions the Zero Trust method as a more resilient and efficient alternative for modern payment systems, as seen in Figure.11

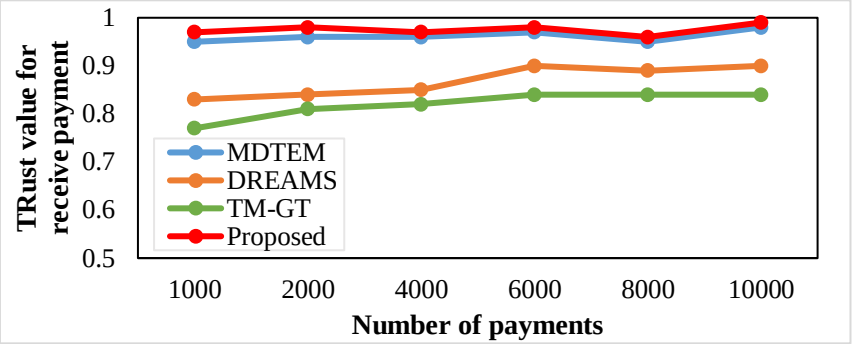

Figure 11: Trust Value for Receiver Payment Comparison

Furthermore, the proposed FTBF-based Zero Trust Architecture (ZTA) outperforms MDTEM, DREAMS, and TM-GT algorithms in achieving superior performance in data delivery success rates. The FTBF-based approach ensures reliable and secure data delivery, even with increasing network complexity and transmission loads. Unlike MDTEM, DREAMS, and TM-GT algorithms, which have moderate success rates, the FTBF-based ZTA integrates blockchain technology and trust verification mechanisms, reducing data delivery failures and improving reliability. This is due to the architecture's ability to validate and securely transmit data, ensuring higher trustworthiness and accuracy in delivery processes. The results in Figure 12 highlight the FTBF-based ZTA's effectiveness in achieving higher delivery success rates than existing trust algorithms, solidifying its suitability for secure and efficient payment and communication systems.

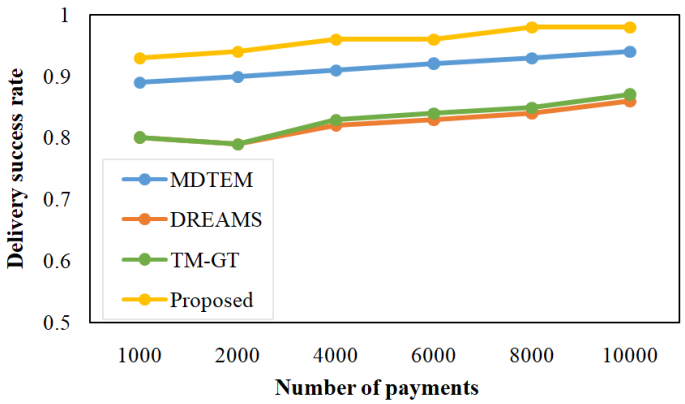

Figure 12: Delivery Success Rate Comparison

5.4. Discussion

The proposed study focuses on FTBF-based ZTAs that employ blockchain technology to improve trust, reliability, and performance in secure communication and payment systems. The study shows that the proposed blockchain-based ZTA outperforms existing trust algorithms, including

MDTEM, DREAMS, and TM-GT,regarding trust value, delivery success rate, and reaction time. The study emphasises the limits of traditional techniques, which frequently struggle with scalability, trust validation, and consistency, especially in complicated and high-traffic environments. The results show that the FTBF-based ZTA overcomes these constraints by utilizing blockchains' decentralized trust verification techniques. FTBF surpasses MDTEM, DREAMS, and TM-GT for trust value comparisons, demonstrating its capacity to improve the trust assessment index as the volume of communicated information grows. This improvement can be linked to the architecture's capacity to securely verify data and provide transparency, resulting in a higher level of trust for both service providers and recipients. The comparison results show that the FTBF-based ZTA is more effective at establishing confidence for payment transfers, making it a dependable alternative for modern financial systems. Regarding delivery success rate, the proposed technique outperforms other trust algorithms. Includingblockchain technology into the FTBF-based ZTA allows for strong validation processes, reducing data loss and boosting delivery reliability. This is especially significant in high-load transmission settings, where classic methods decrease performance. FTBF provides an efficient mechanism for safe and trustworthy communication in payment systems by increasing the delivery success rate. The FTBF-based ZTA has shown to be a very efficient and dependable solution for improving trust, delivery success, and reaction times in secure communication and payment systems. The proposed solution ensures secure, transparent, and high-performance operations by addressing the constraints of current trust algorithms, making it ideal for use in financial technology and other essential applications. The findings highlight the transformative power of blockchain-based trust architectures in tackling issues such as data security, trust management, and performance optimization.

6. CONCLUSION

The architectural design of FTBF provides a solid and comprehensive solution to the FinTech sector's security, scalability, and trust concerns. The multi-layered framework promotes modularity, efficiency, and adaptability. The Transaction Layer securely initializes and encrypts transactions to ensure data integrity. The Validation Layer ensures transaction validity by integrating the DCFOM with a hybrid TESSA consensus mechanism, resulting in energy-efficient and tamper-proof validation. Furthermore, the Trust Management Layer applies Zero Trust concepts to continuously analyse and update user and node trust scores, improving dynamic trust assessment and system resilience. Together, these layers provide a safe, transparent, and scalable approach that addresses significant blockchain limitations while improving trust management in FinTech applications.The framework supports the next generation of decentralized financial systems by fostering trust and reducing reliance on centralised authorities. Its emphasis on transparency, auditability and continuous trust updates establishes a robust and future-ready foundation for modern Fintech applications. Despite its efficiency, the proposed model faces limitations due to computational overhead from continuous trust score updates, which may impact real-time processing in high-throughput environments. An adaptive trust management framework that dynamically adjusts the frequency of trust score updates based on system load and network conditions will be introduced in terms of future scope. This approach would ensure a balance between accuracy and computational efficiency, enabling the system to maintain its performance under varying operational conditions.

DECLARATIONS

Conflict of Interest

The authors declare no conflict of interest.

Author Contribution

Al authors are equally contributed

Funding

No fund was received for this work

REFERENCES

[1] Zeidy, I. A. (2022). The role of financial technology (FinTech) in changing the financial industry and increasing efficiency in the economy. COMESA Monetary Institute. Available at https://www. comesa. int/wp-content/uploads/2022/05/The-Role-of-Financial-Technology. pdf.

[2] Ghodichor, N., Sahu, D., Borkar, G., &Sawarkar, A. (2023). Secure Routing Protocol To Mitigate Attacks By Using Blockchain Technology In Manet. arXiv preprint arXiv:2304.04254.

[3] Chen, Y., &Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights, 13, e00151.

[4] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. IEEE transactions on knowledge and data engineering, 30(7), 1366-1385.

[5] Kaur, S., Chaturvedi, S., Sharma, A., &Kar, J. (2021). A research survey on applications of consensus protocols in blockchain. Security and Communication Networks, 2021(1), 6693731.

[6] Sanyaolu, T. O., Adeleke, A. G., Azubuko, C. F., &Osundare, O. S. (2024). Harnessing blockchain technology in banking to enhance financial inclusion, security, and transaction efficiency. International Journal of Scholarly Research in Science and Technology, August, 5(01), 035-053.

[7] Mungoli, N. (2023). HybridCoin: Unifying the Advantages of Bitcoin and Ethereum in a Next-Generation Cryptocurrency. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY, 7(2), 235-250.

[8] Juan, A. A., Perez-Bernabeu, E., Li, Y., Martin, X. A., Ammouriova, M., & Barrios, B. B. (2023). Tokenized Markets Using Blockchain Technology: Exploring Recent Developments and Opportunities. Information, 14(6), 347.

[9] Jánoky, László Viktor and Levendovszky, János and Ekler, Péter, Client Performance Predictions for Private Blockchain Networks (2020). International Journal of Computer Networks & Communications (IJCNC) Vol.12, No.5, September 2020, Available at SSRN: https://ssrn.com/abstract=3732609

[10] Ahmed, A. A. A. (2024). The Rise of DeFi: Transforming Traditional Finance with Blockchain Innovation.

[11] Strebinger, A., &Treiblmaier, H. (2024). Disintermediation of consumer services through blockchain? The role of intermediary brands, value-added services, and privacy concerns. International Journal of Information Management, 78, 102806.

[12] Owolabi, O. S., Hinneh, E., Uche, P. C., Adeniken, N. T., Ohaegbulem, J. A., Attakorah, S., ... &Nwariaku, H. (2024). Blockchain-Based System for Secure and Efficient Cross-Border Remittances: A Potential Alternative to SWIFT. Journal of Software Engineering and Applications, 17(8), 664-712.

[13] Hieu, M. N. (2020). Hybrid model in the block cipher applications for high-speed communications networks. International Journal of Computer Networks & Communications (IJCNC) Vol, 12.

[14] Song, J. Y. L., & Tan, E. (2024). Beyond traditional contracts: the legal recognition and challenges of smart contracts in Malaysia and Singapore. Journal of Law, Market & Innovation, 3(3), 323-357.

[15] Deshmukh, A. A., Kandukuri, P., Vijaykumar, J., Shalini, A., Farhad, S., Muniyandy, E., & Baker El-Ebiary, Y. A. (2024). Event-based Smart Contracts for Automated Claims Processing and Payouts in Smart Insurance. International Journal of Advanced Computer Science & Applications, 15(4).

[16] Sharma, J. (2023). Blockchain Technology Adoption in Financial Services: Opportunities and Challenges. Revolutionizing Financial Services and Markets through FinTech and Blockchain, 99-117.

[17] Asif, R., & Hassan, S. R. (2023). Shaping the future of Ethereum: Exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus. Frontiers in Blockchain, 6, 1151724.

[18] Koukaras, P., Afentoulis, K. D., Gkaidatzis, P. A., Mystakidis, A., Ioannidis, D., Vagropoulos, S. I., &Tjortjis, C. (2024). Integrating Blockchain in Smart Grids for Enhanced Demand Response: Challenges, Strategies, and Future Directions. Energies, 17(5), 1007.

[19] Zhuo, X., Irresberger, F., &Bostandzic, D. (2023). Blockchain for Cross-border Payments and Financial Inclusion: The Case of Stellar Network.

[20] Rjoub, H., Adebayo, T. S., &Kirikkaleli, D. (2023). Blockchain technology-based FinTech banking sector involvement using adaptive neuro-fuzzy-based K-nearest neighbors algorithm. Financial Innovation, 9(1), 65.

[21] Gai, K., She, Y., Zhu, L., Choo, K. K. R., & Wan, Z. (2023). A blockchain-based access control scheme for zero trust cross-organizational data sharing. ACM Transactions on Internet Technology, 23(3), 1-25.

[22] Chaudhry, U. B., &Hydros, A. K. (2023). Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm. IET blockchain, 3(2), 98-115.

[23] Liu, Y., Hao, X., Ren, W., Xiong, R., Zhu, T., Choo, K. K. R., & Min, G. (2022). A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things. IEEE Transactions on Computers, 72(2), 501-512.

[24] Song, Y., Sun, C., Li, L., Wei, F., Liu, Y., & Sun, B. (2023). Research on Blockchain-Based FinTech Trust Evaluation Mechanism. IEEE Access.

[25] Wang, L., Chen, Y., Wu, T., & Hu, S. (2023). A Practice of Zero Trust Architecture in Financial Transactions. International Journal of Information and Communication Engineering, 17(12), 692-698

[26] Song, Y., Sun, C., Peng, Y., Zeng, Y., & Sun, B. (2022). Research on multidimensional trust evaluation mechanism of fintech based on blockchain. IEEE Access, 10, 57025-57036.

[27] Bahar, S. W. (2023). Advanced Security Threat Modelling for Blockchain-Based FinTech Applications. arXiv preprint arXiv:2304.06725.

[28] Delgado-Segura, S., Pérez-Solà, C., Herrera-Joancomartí, J., Navarro-Arribas, G., &Borrell, J. (2018). Cryptocurrency networks: A new P2P paradigm. Mobile Information Systems, 2018(1), 2159082.

[29] Khalilov, M. C. K., & Levi, A. (2018). A survey on anonymity and privacy in bitcoin-like digital cash systems. IEEE Communications Surveys & Tutorials, 20(3), 2543-2585.

[30] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). Ieee.

[31] Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., &Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE access, 7, 85727-85745.

[32] Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., & Shi, W. (2017). On security analysis of proof-of-elapsed-time (poet). In Stabilization, Safety, and Security of Distributed Systems: 19th International Symposium, SSS 2017, Boston, MA, USA, November 5–8, 2017, Proceedings 19 (pp. 282-297). Springer International Publishing.

[33] Pathan, S. (2024). A Thorough Review of Blockchain Consensus Algorithms. Vidhyayana-An International Multidisciplinary Peer-Reviewed E-Journal-ISSN 2454-8596, 10(1).

[34] Huang, X., Yu, R., Kang, J., & Zhang, Y. (2017). Distributed reputation management for secure and efficient vehicular edge computing and networks. IEEE Access, 5, 25408-25420.

[35] Du, R., Xu, K., & Tian, J. (2020). Optimization scheme of trust model based on graph theory for edge computing. Adv. Eng. Sci., 52(3), 150-158.

[36] Afzaal, H., Imran, M., Janjua, M. U., &Gochhayat, S. P. (2022). Formal modeling and verification of a blockchain-based crowdsourcing consensus protocol. Ieee Access, 10, 8163-8183.

[37] Lee, S. W., Hussain, S., Issa, G. F., Abbas, S., Ghazal, T. M., Sohail, T., ...& Khan, M. A. (2021). Multi-dimensional trust quantification by artificial agents through evidential fuzzy multi-criteria decision making. IEEE Access, 9, 159399-159412.