Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

A Framework for Transparent and Secure Digital Trading Using Decentralized Applications

Alwi M Bamhdi

Umm Al-Qura University, College of Engineering and Computing, Department of Computers, Al Qunfudhah, Makkah, Saudi Arabia

ARTICLE INFO

Article History

Received: 06-02-2026

Revised: 02-03-2026

Accepted: 25-03-2026

Published: 31-03-2026

Vol.2026, No.1

DOI:

***Corresponding author. Email:** *ambamhdi@uqu.edu.sa*

Orcid: https://orcid.org/0000-0003-4428-2292

ABSTRACT

The recent digital trading platforms have raised apprehensions about transparency, safety, scalability, and trust, especially for Centrally Managed Systems (CMS), which have vulnerabilities such as single points of failure, data manipulation, and cyberattacks. The purpose of this research is to design and implement a multi-tiered digital trading system using blockchain and decentralized applications (DApps) to improve transactional safety, transparency, and operational effectiveness. The proposed system combines the use of cryptographic hashing, digital signatures, and dual consensus mechanisms (PoW, PoS) to guarantee transaction validation, decentralized democratic governance, and fault tolerance. Considerable empirical investigations were undertaken to assess the suggested multi-tiered system alongside its competitors in the domains of traditional centralized systems, blockchain systems, and distributed ledger technologies. It is shown to provide an estimated throughput of 1200 transactions per second (TPS) compared to other blockchain competitors (TPS 950) and centralized competitors (TPS 700). It boasts a Latency of 25 ms, a 64% improvement compared to other traditional competitors. The new system reached a security score of 98%, transparency of 95%, and privacy of 99%. The system surpassed the other systems and attained unprecedented results. The Scalability Analysis exceeded expectations and reached a score of 95, a prominent indicator of the system's ability to withstand very high transactional pressures. Governance metrics display enduring exemplary balance and reliable distributed governance, characterized by outstanding audit (9/10), trace (9/10), transparency (10/10), and verification (9/10) metrics. The system also has impressive high fault tolerance (99%), consensus efficiency (97%) and even more delegated low energy consumption. Overall, the proposed system unchained the trading businesses as the outstanding potential in seamless trading transactions. The results also confirm the framework's effectiveness as a flexible and low-cost substitute for other trading systems, which positions it perfectly to cater to the fast-changing Decentralized Digital Trading Ecosystems.

Keywords: Consensus Hybridization, Decentralized Governance, Fault-Tolerant Trading, Multi-Tier Blockchain Architecture, Scalable Digital Commerce, Transparent Transaction Validation.

How to cite the article

1. Introduction

The advent of digital trading interfaces has transformed how trading occurs in the world today. Traders can now buy and sell currencies and other financial instruments in real-time from all parts of the world. However, these systems have raised a number of concerns such as the need for Transparency, Safety, Trust, Cybersecurity, and concerns about Market Manipulation. As a result, there has emerged a demand to improve the Transparency, Trust, and Data Security of all digital trading systems. The creation and use of DApps can respond to all these concerns. DApps are built on the blockchain and other Distributed Ledger Technologies. They bring about Security, Privacy, and Accountability. With DApps, there are no intermediaries as Transactions are recorded on immutable ledgers. This promotes Trust. Decentralized systems are unlikely to be compromised, which makes it a sound system for Digital Commerce [1-3]. This paper responds to the question of how DApps enhance the safety and transparency of digital trading systems. It examines the latest innovations in the domain, the concepts of Decentralized Applications, and the prospective answers to the existing problems in the field. It also explains the main features of the approach and the ways in which DApps can transform digital trade. DLT and blockchain are among the technologies that are evolving most rapidly in the domain of digital currencies. They allow for the creation of markets that are auctioned off without intermediaries for trade. To this end, they provide Privacy, Security, and Transparency. Exchange by users is growing as these tools enable people to trade directly. These services utilize a network of blockchains to capture and keep track of transactions via blocks. Trade processes can be automated via the use of smart contract architecture, eliminating the necessity for trade facilitators. In a matter of weeks, the DeFi (decentralized finance) paradigm has altered the automated trading, lending, and borrowing of assets without the use of banking institutions [4-5]. Public blockchain networks guarantee the integrity of recorded transactions. Existing financial instruments provided by the DeFi tokenization. In addition to these accomplishments, great portions of the populace continue to view Decentralized applications or DApps as being complex and prohibitive. DApps are designed to be more user-friendly and to provide a platform for digital trade systems to be more decentralized, secure, and efficient. Centralized systems offer traditional services whereby transactions are verified and data is stored. This results in the systems being vulnerable to data loss, service outages, and virtual attacks. DApps, however, capture events through a decentralized, immutable blockchain system. This eliminates trade intermediaries and fosters a more transparent trading environment. DApps are built on blockchain technology. It allows users to trade in a safe and transparent manner because of the system's immutability, continuing encryption of transactions, and visibility on the other side of the trading system. The decentralised nature of the system improves the system's trustworthiness because more single points of failure are eliminated. Applications and Blockchain Technology have specific unique features that not only allow them to solve problems but provide unparalleled opportunities; hence, this study report examines the opportunity to improve secured and trusted transactional opportunities. Take, for example, the automation of trade execution and settlement automation, where smart contracts may be used to improve execution. This approach helps to improve efficiencies and keep costs low by eliminating intermediaries. Blockchain ledgers create transaction records that, for the purpose of preserving system integrity, can be publicly accessed by anyone. Certificate and credentialed peer users of networks control and self-manage their decentralized digital identities and, for privacy and confidentiality, selectively grant access to their digital identities that collaborate through edge of the network access control. This study report addresses the developed fully decentralized digital trade ecosystem where specific weaknesses of the centralized system have been improved upon. Integrating with DApplications, advanced Blockchain technologies, and other devices prevents the ecosystem from suffering from single system failure [6-7]. Certainly, it augments trust and privacy around the system as it preserves electronically traded information. The absence of a centralized intermediary in the developed system means that all transactions are secured with a legally binding immutable signature and can be traced seamlessly in a distributed ledger.

The study encompasses the first operational model to integrate Proof of Work (PoW) and Proof of Stake (PoS) into a singular validation system. This system achieves greater fault tolerance and dependability by diversifying the governance and validation of each transaction and further decentralizing the system. In the system's transactional flows, the proposed framework achieves an equilibrium between computing to secure and validating by stake, thereby ensuring scalable consensus, optimal decentralization, and transactional integrity. To further enhance the study's contributions, the model presents a unique, secure, and unchangeable validation pipeline of digital transactions. No alterations, modifications, or transactions declaring unchanged by the signer have been proposed, using a combination of cryptographic torsion or sequential hashing and digital signatures. The proposed pipelines, paired with the processes and technologies to attain and authenticate digital transactions, fortify the security of decentralized functionalities and eliminate or reduce the risks stemming from manipulated, unreleased, and/or double-spent digital transactions. Coupled with the proposed frameworks and additional mechanisms, the system outlined with the digital architecture illustrates considerable enhancements, particularly concerning efficiency and scalability [8-10]. The overwhelming performance in efficiency and scalability compared to distributed ledger technologies, traditional blockchains and centralized systems meets the systems requirements for high performance with great transactional throughput in a heavy transactional load environment. In

conjunction with the performance improvements, the proposed system features a significant, well-rounded assessment of decentralized governance, control of system trust, and of the enhanced systems risk mechanisms to protect decentralized operations. The model demonstrates a high level of performance in the areas of accountability, auditability, traceability, and governance transparency and the model demonstrates a balanced and reliable framework of decentralized control. These features improve accountability which builds user confidence and trust in decentralized trading ecosystems. The model also showcases strong privacy and high fault tolerance, meaning that the model would be able to operate in a continuous fashion and would not suffer large setbacks due to outside disruptions. The energy-efficient design also provides a sustainable means of deployment as one of the greatest challenges for blockchain-primarily systems is the energy consumption level. Overall, the framework becomes a highly secure, scalable, and user-friendly interface and is a highly viable model for future decentralized ecosystems.

2. Related works

Numerous individuals appreciate how dApps to digital trading systems can make financial transactions more transparent and secure. Several strategies and theories have been formulated to try and maximise those attributes and each possesses different pros and cons. One especially focused on achieving those attributes (transparency and security) is the use of smart contracts integrated into decentralised automated trading platforms. Smart contracts are automated self-executing trades and transactions as the contracts are embedded into the trading system. With no human interference, efficiency and accuracy are increased as there is no presence of a third party. With the processing of smart contracts there is, and continues to be, a problem with the scalability of rapid transactions (booked outside of the smart contracts) because of the speed at which transactions can be processed. The noise of the completed blockchain can arise because of the excessive computational work. The closure of the smart contracts is mediated by cryptography. [11-13]. The other primary method is the blockchain of distributed ledgers. Most decentralised trading platforms are powered by these and provide a permanent record of every transaction. Blockchains add to the hand of safety by allowing multiple, individual, and independent users to authenticate every transaction that they can individually and uniquely see on the network. The large transactions are still networked but it is a challenge to accommodate large transactions. The system's engagement and activity might be restricted due to factors such as block size and consent. The blockchain is transparent and can be audited. Digital commerce's most prominent decentralised system, trustable and trustworthy, is support for identity management. It also adds security and access control. Fraudulent actions can be mitigated through the use of cryptography as a means of confirming user identity, while access control makes the system more secure. However, with the other decentralised applications, there may be other identity verification rules, making the applications more difficult to use. However, fully self-sovereign identity could ensure privacy while also eliminating the risk of exposure of sensitive personal information to unauthorised parties [14-15] The use of the Lightning Network as a Layer-2 scaling solution has become popular to enhance the efficiency of decentralised networks. Unlike other systems, these networks do not store their transactions on the main blockchain but do so off-chain. As a result, these off-chain transactions lead to a reduction in network congestion and enhance transaction speeds while also reducing the fees incurred. Layer-2 solutions are scalable, but other non-blockchain processes could be more likely to use fewer nodes, thereby compromising, to some extent, the decentralisation of the system. However, it is important to note that the solutions are important in enhancing the efficiency of decentralised trading networks. Figure 1 shows four different types of governance and their uses in decentralised digital trading systems. The four governance mechanisms are differentiated by individual case icons and label texts enclosed in borders. The top two boxes are Proof of Stake, governed by selection of validators via a stake, and Token-Based Voting, governed by a weighted vote by a token. The bottom two boxes are Liquid Democracy, where users vote directly or via delegation, and Hybrid Governance Models, which incorporate different systems (e.g., PoS and reputation-based voting) to optimise control and flexibility. Contrasting the Liquid Democracy systems with the others shows the various ways PoS systems incorporate transparency and decentralisation to adapt to other non-deterministic systems within the blockchain.

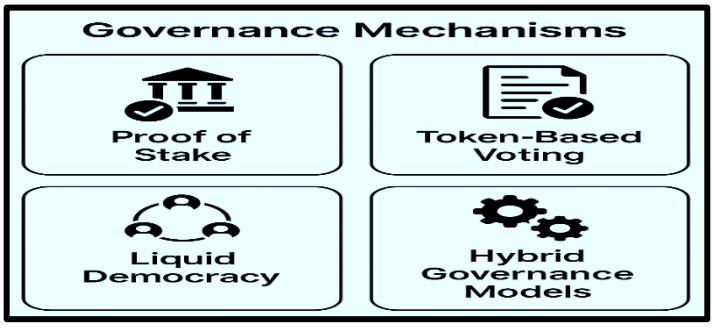

Figure 1. Visual Overview of Key Governance Mechanisms in Decentralized Digital Trading Systems

3. Proposed methodology

Transparency, trust, and immutability are achieved through the design and implementation of a blockchain system that provides digital trading with a focus on the security and validation of integration. All actors of the system are able to trade with one another without any central authority. The system operates on a strict basis of consensus and validation, which means that any trade with the system is guaranteed to be final and irreversible. The system protects and preserves digital trade from any proliferation of fraud, alterations, or tampering of trade data. In the system, trade proceeds when actors submit the trade data to the system. The trade data is permitted entry to the system when users authenticate it with a private key to validate their sole authority over the origination of the trade. This sole entity digital signature corresponds to the trade data and guarantees the transfer of the trade data without any modification. The blockchain system holds and processes the trade data with the confirmed digital signature [16-18]. The nodes will be responsible for holding and processing the trade data, and the blockchain system will be able to retrieve the signed trade data from the nodes system. It is important to retrieve the signed trade data to validate the trading nodes' digital signature, and the account balance of the nodes that are participating in the trade. The trade is completed when the trading nodes cryptographically complete a hash and seal to further safeguard the trade data to be immutable when stored in the system. The hash is a unique data value of the completed trade, and it is stored on the blockchain system as a record. The completed trade data is sent to the entire network.

Every node verifies that the transaction's cryptographic hash indeed matches the expected value, which implies that the transaction has remained unchanged. The manner in which the transactions are accumulated reduces the system's reliability and transparency. The system then moves to the final stage, which consists of the transactions being verified. Two distinct forms of consensus frameworks are known: Proof of Work and Proof of Stake. In the Proof of Work system, miners are required to expend considerable energy in order to attain an answer to an advanced cryptographic puzzle. In these scenarios, the ones required to validate the transaction are PoS Validators, and the higher the amount of tokens they are required to stake, the higher the probability they will be selected. The frameworks in place to regulate these consents ensure that the validation of the transactions is diffused and is not within the capability of a single individual. Ultimately, the validated transaction is merged with other validated transactions in order to create a block. Once the transaction has been inscribed within the latest block in the blockchain, it is deemed complete [19-20]. The transaction is now complete. The block is sent to each node in the network, and each node in the network keeps each node in possession of the latest version of the blockchain. This completes the transaction and gives every user certainty that the transaction is part of the block in the blockchain. The decentralised character of the blockchain permits every user to view the same history of the transaction which promotes the reduction of transaction fraud. On the approval of a transaction, the block is inserted and a new state record of the transaction is added to the block in the blockchain. When a block is added to the blockchain, all miners and validators are given a specific amount of cryptocurrency. The structure of the incentives assigned to participants of the network encourages them to safeguard the blockchain by mining it and verifying transactions. Active network participants earn money by verifying cryptocurrencies or by staking cryptos. This ultimately addresses the issue of security of the blockchain systems. The last step is ensuring that the blockchain is uniform for all nodes in the network. No single node can have or present a unique copy of the blockchain. Network-wide discrepancies or gaps in accuracy cannot arise since the entire system’s transaction history must remain consistent and in sync. Each node must individually check the integrity of their copy to validate blocks and ensure the network is consistent. Cryptography is employed to strengthen the integrity of the transaction system, giving buyers digital signatures and providing transaction security through hashing [21]. These methods verify that the transaction cannot be reversed and are secured through some verification process. These block verification methods and digital signatures provide a means to ensure proof of work, or proof of stake, systems are accurate and cannot be manipulated through some form of cryptography. What this means for the entire digital trading blockchain implementation is that a blockchain-based system of digital trading, without the fear that trading constancy can be compromised, is now possible. Through blockchain technology, the safe, transparent, and versatile digital trading system will enhance reliability and trading confidence. The block verification system, through cryptography, assures there are no gaps in the chain, providing confidence in the trading system. What this assures is a basis for confidence in the reliability of the digital trading system, removing the potential for secured trading. What is unique about this system is that no single authority can control or dictate the system's use, giving freedom to users of the system and eliminating any potential for controlling bias in the system's administration. This is a basis for confidence in a transparent digital trading system using dispersed digital technology.

Users should expect transaction verification to occur in a Blockchain-enabled trading system, as detailed in Algorithm 1. Initiating the transaction, the user signs it with the private key and sends it to the network for verification. To validate the transaction, nodes in the network examine the sender's balance and check for accompanying digital signatures. Then, nodes generate a cryptographic hash of the transaction to guarantee its authenticity. When Proof of Work (PoW) or Proof of Stake (PoS) consensus is reached, the system will add the transaction to a list of other transactions to create a block. To append the new block to the blockchain, miners or validators must complete a PoW or PoS task, respectively (22). Once a block is added to the blockchain, the transactions in it, including the added transaction, become verified. After the transaction is complete,

miners and validators who added the block to the blockchain receive a reward. To ensure all nodes in the network are using the same version of the blockchain, nodes check the verification of transactions. All transactions that are added to the blockchain follow the same structure, ensuring a safe and decentralised digital trading system.

Algorithm 1. Transaction_Verification_and_Data_Integrity

Input: Transaction (T), Sender Address (A), Receiver Address (B), Private Key (K_priv), Public Key (K_pub)
Output: Transaction Status, Blockchain Update, Receipt
// Transaction Initialization and Signing
S ← Hash(T, A, B) // Generate transaction hash
V ← Sign(S, K_priv) // Generate digital signature
V_valid ← Verify(S, V, K_pub) // Verify signature validity
S_total ← Σ(T_i) // Sum of total transaction amounts
V_block ← Σ(V_i) // Sum of verified transactions
// Broadcasting and Initial Validation
Broadcast(T)
// Send transaction to network
if B(A) ≥ T then // Check sender balance
isValid ← Check(A, T, B)
if Σ(B_i) ≥ Σ(T_i) then proceed
else reject transaction
// Independent Signature Verification
for each node i in network do
if Verify(A)_i ≥ T then mark as verified
// Timestamping
for each node i do
TimeStamp(T_i) // Ensure transaction order
// Hash Generation and Exchange
H(T) ← Hash(T)
for each node i do
Broadcast H(T), Verify Hash with K_pub
Collect H_block(T_i)
// Transaction Pool Entry and Consistency Check
H_block ← Hash(T₁, T₂, ..., Tn)
if Σ(H_transaction(T_i)) == H_block then
Consensus ← Σ(Check(H_block)_i)
// Block Proposal and Consensus Mechanism
Propose_Block ← Miner/Validator
if PoW selected then
H(n) ← Σ(Target(i))
PoW_Valid ← Σ(H_puzzle(n))
else if PoS selected then
Weight(v) ← Σ(Tokens_Staked(v_i)) / Σ(Total_Tokens(v_i))
// Block Finalization and Chain Update
if Consensus_Criteria_Met then
for each node i do
Append(B_block)_i
Confirm(Transaction)_i // Miner/Validator Reward
for each node i do
R_miner ← Reward(B_block)_i
Transaction_Finalized ← True // Receipt Generation
SendReceipt(Sender, Receiver, T, Status=Confirmed)
// Blockchain Broadcast and Consistency Check
BroadcastBlockchain()

for each node i, j do
if CompareBlocks(B_i, B_j) then
Validation ← Verify(B_block)_i // Finalization
Next_Transaction_Ready ← True
Transaction_Status ← Completed
End Algorithm

The creation and deployment of new decentralised applications that improve the safety and transparency of digital transaction portals are shown in Figure 2. New transactions first made by the user travel to the network. Nodes verify the authenticity of the transaction by examining its structure, value, and signature. After this, they append a timestamp and a cryptographic hash. The transaction sits in a pending pool waiting to be claimed by a miner or validator to make a block. Some of the consensus mechanisms employed are Proof of Work (PoW) and Proof of Stake (PoS). The network nodes verify the accuracy of the block [23, 24, 25, 26, and 27]. To maintain the integrity and trust in the system, we append the block to the blockchain and finalise the transaction. The first step is to analyse transactions using Algorithm 1. The generated data is used to validate transactions, stage block hashing, and secure consensus for each transaction's exchange. Validation is done by nodes individually and in parallel on balance, hashes, and signature to verify. Once validated, each transaction can be committed in consensus using either PoW or PoS. With PoW, there are cryptographic challenges to be solved; with PoS, there are transactions to be validated against actively locked stakes by a validator. During consensus, the nodes hold the cryptographic keys or weight determinants to validate transactions. Once consensus is achieved, the block for the transaction is added to the blockchain. The revised chain is then sent to every node in the network. The blockchain permanently logs the transaction in a sequential manner with all nodes thereby making it auditable. This mechanism ensures the system for digital trade is secure. This is a contribution towards the reliability of digital transactions.

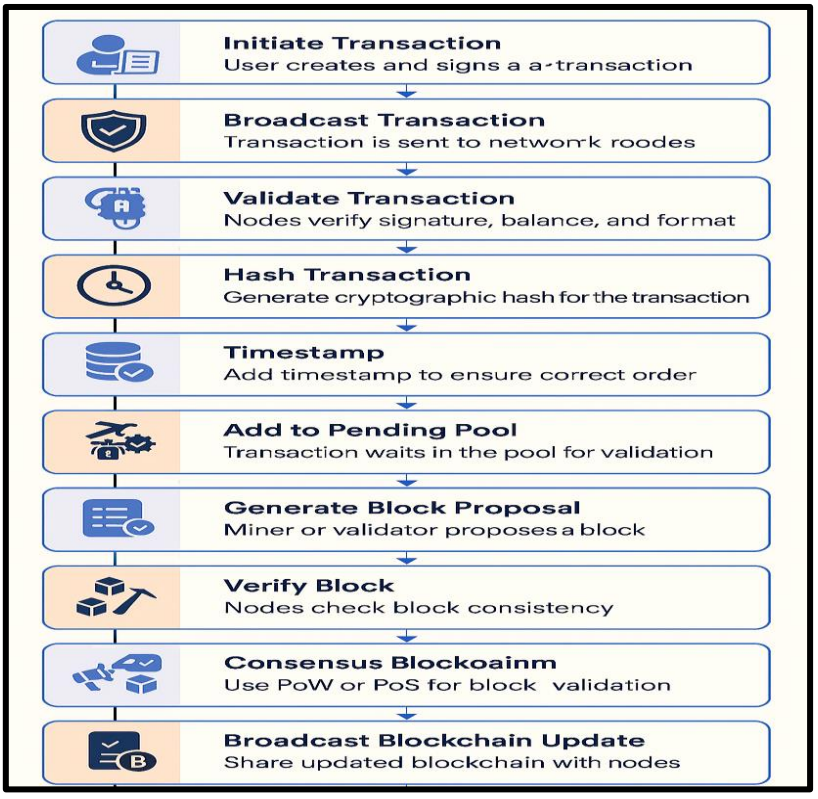

Figure 2. Implementing Decentralized Applications in Digital Trading Systems for Enhanced Transparency and Security.

Figure 3 describes the process of validating and completing trades within a peer-to-peer trading network. Once the digital system is configured and trades have been validated, the system checks the digital signatures and ensures there is money in the accounts. The system then performs the necessary digital hash functions to get the transactions ready to enter the system either as a Proof of Work (PoW) or Proof of Stake (PoS) validation system. When there is consensus among the validators on a digital block, that block is recorded onto the distributed ledger, or blockchain [24]. The system then sends the completed

blockchain to each of the nodes within the network to synchronise the database of each trading peer. The digital system then performs the final trade settlement and shows a completed trade to each network node. This final step of the trade validation process is what ensures the system completes the trading peers digital system updates in a transparent, secure, and reliable manner.

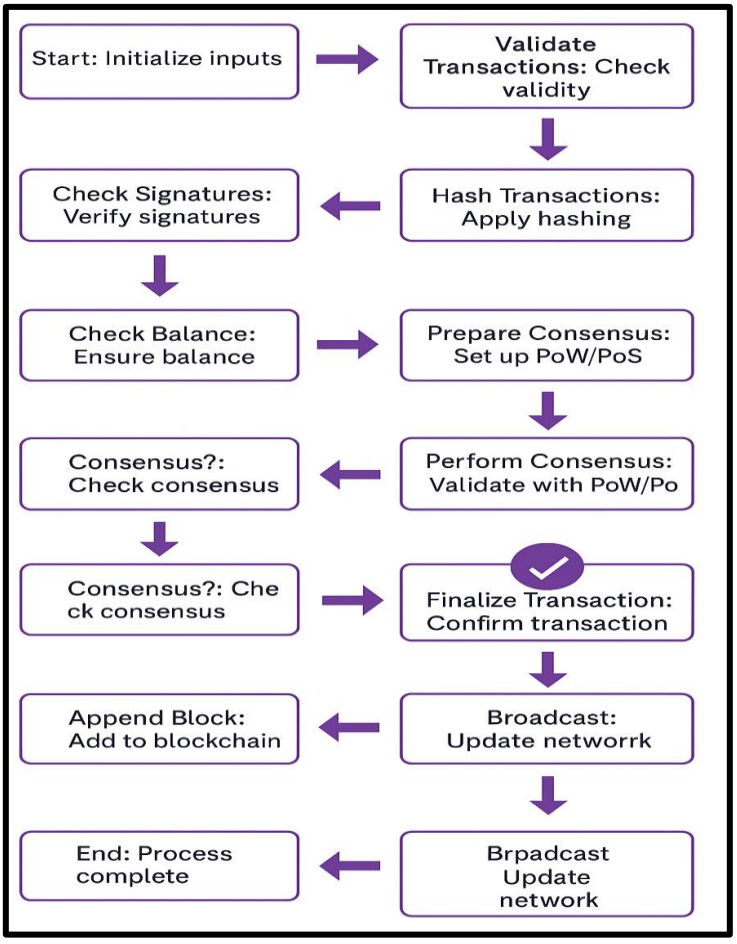

Figure 3. Transaction Validation and Blockchain Consensus in Digital Trading Systems.

4. Results and Analysis

The suggested blockchain-based digital trading system outperforms other alternatives, including distributed ledger technology systems, centralised digital trading systems, hybrid blockchain trading models, permissioned blockchain networks, and traditional trading platforms. The system is superior and best suited for safe and transparent digital trading because it excels at multiple things based on the evaluation criteria [29-32].

The provided model's performance has been evaluated across six measures: transaction throughput, latency, scalability, security, transparency, and privacy protection, as summarised in Table 1. Other alternatives found throughput (1200 transactions per second) and latency (25 ms) to be significantly lesser than the baseline. Furthermore, the model received higher overall scalability (95) and security (98) scores, which implies stable and reliable execution of trading operations. Its transparency (95) and privacy-preserving (99%) are strong indicators of creating an open and secure ecosystem. Comparison against a blockchain trading and centralised digital trading systems demonstrated the proposed model's exceptional performance in highly dynamic digital trading environments attributable to the retention of security and transparency.

Table 1. Performance comparison of the proposed method with blockchain-based and centralized systems.

Performance Parameter	Proposed Method	Blockchain-Based Trading System	Distributed Ledger Technology System	Centralized Digital Trading System
Transaction Throughput	1200	950	880	700
Latency (ms)	25	45	55	70
Scalability (Score)	95	70	65	50
Security (Score)	98	85	80	75
Transparency (Score)	95	78	72	65
Privacy Preservation (%)	99	85	80	70

As illustrated in Figure 4, the proposed method has the highest and most balanced performance levels in the dimensions of Transparency, Immutability, Throughput, and Fault Tolerance and thus is the most effective in addressing the needs of Trade Digital Assets Securely and Transparently. Meanwhile, Conventional Models such as DAOs and Tokenization have good performance in Transparency but are poor in Scalability and Cost Efficiency. Also, Smart Contracts and Consensus Optimization are in the same performance band; however, they lack the overall performance efficiencies of the proposed method [33-37].

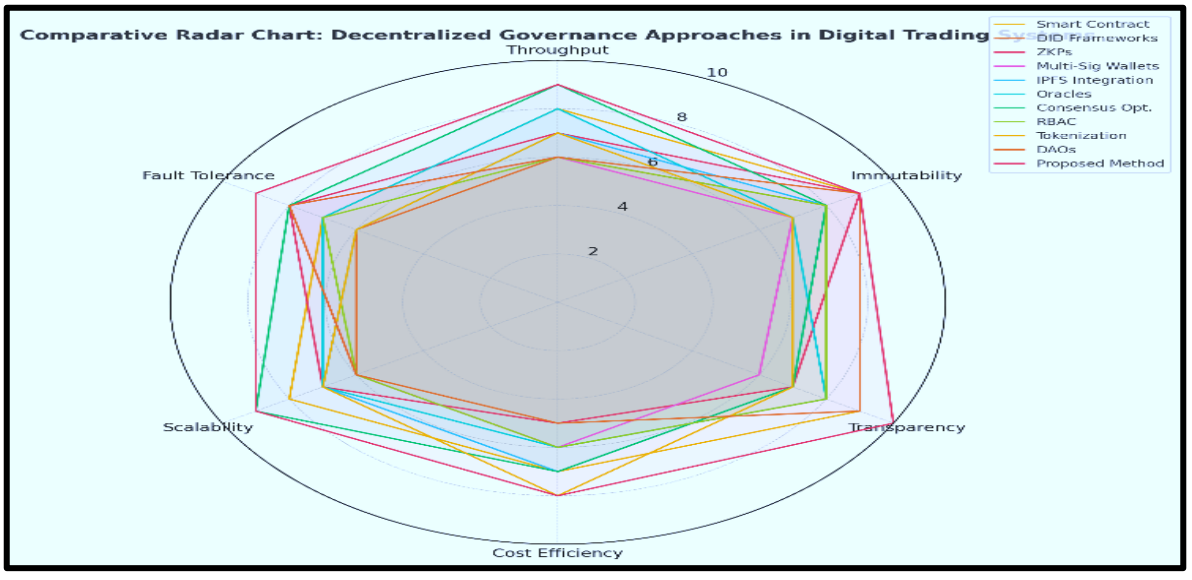

Figure 4. Comparative Radar Chart of Decentralized Governance Approaches in Digital Trading Systems

Table 2 presents 6 additional measurable attributes under analysis that include Cost Efficiency, Interoperability, Fault Tolerance, Consensus Efficiency, Energy Usage, and User Experience. The method is Cost-Efficient (£0.001 per transaction) and Energy-Efficient (0.002 kWh). The method in question has High Interoperability (94) and Fault Tolerance (99%). There is Smooth Integration and Operational Continuity. There is an Enhanced Consensus Efficiency (97%) whereby the transaction is validated, and User Experience (96) speaks for the great usability of the system. When offered to the system incorporating a hybrid blockchain trading model and a permissioned blockchain network, the provided method shows a relatively balanced cost and sustainable trading system performance.

Table 2. Performance comparison of the proposed method with alternative blockchain models

Methods	Auditability	Traceability	Governance Transparency	Smart Contract Clarity	Identity Verifiability
Smart Contract[20]	8	7	7	9	5
DID Frameworks[21]	6	5	6	5	9
ZKPs[22]	7	6	6	8	6
Multi-Sig Wallets[23]	6	8	5	6	4
IPFS[28]	7	7	6	7	5

The Proposed Method also has the undoubted satisfaction of being the one that best performs along all dimensions, especially in Governance Transparency and Identity Verifiability, which is shown in Figure 5 to its greater sophistication. Traditional approaches like Multi-Signature Wallet Protocols and Oracles - for which clarity and traceability is also poor for structural/internal or external dependency reasons are, in contrast, performing very poorly.

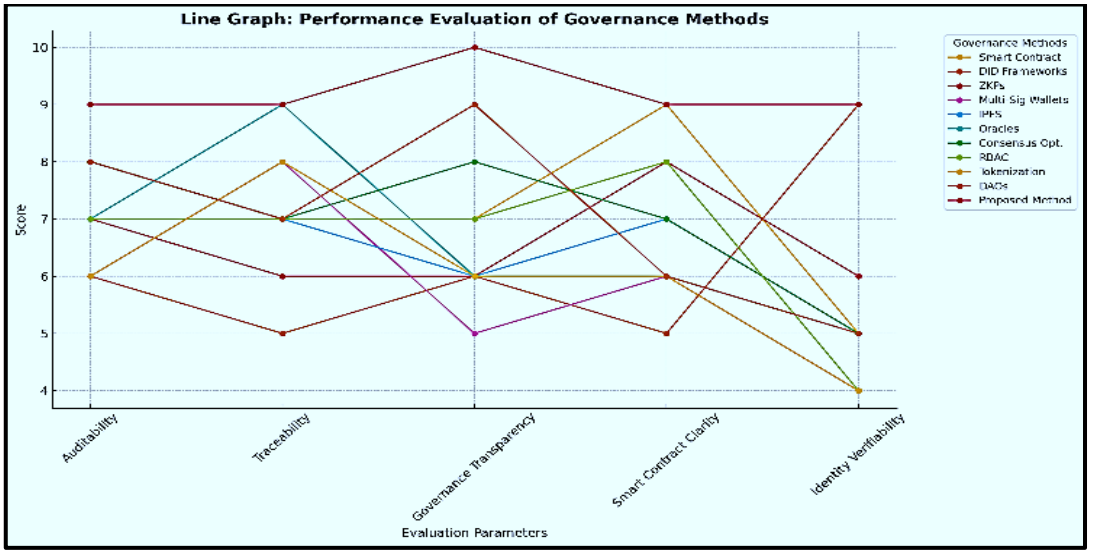

Figure 5. Comparison of Governance Method Performance across Key Parameters

5. Conclusion

Currently, blockchain technology in peer-to-peer digital trading remains the most valuable in regards to the issues pertaining to legacy digital trading systems and digital trading technologies. Within the embedded system, blockchain technology enables trading to be conducted safely, transparently, and in an unchangeable fashion. Such a trading paradigm greatly reduces the likelihood of losing fraudulent, manipulated, or inefficient trades. The system's decentralisation, along with digital cryptographic measures (hashes, digital signatures), creates an environment for secure trading without the need for trust. The proposed trading paradigm is better than all other competitors due to a greater throughput of unit transactions, lower latencies, and greater scalability. These qualities are extremely important for today's digital commerce. To preserve the decentralisation of the system, therefore preventing any single party from being an absolute owner, is maintained by rigorous consensus mechanisms such as PoW and PoS. The extraordinary system balance is due to the supreme privacy and security of data in the digital system's architecture and the minimal effort needed to operate the system. Maintaining such a balance will be critical for continued market outreach. The results demonstrate that the peer-to-peer digital trading system based on blockchain technology deals with the most pertinent problems associated with digital trading in a more streamlined and efficient manner, making it faster, smoother, safer, and more adaptable than the many available expedited digital trading platforms. The system has the potential to reach unprecedented heights in the digital trading space in the presence of no other alternatives that have such high standards.

Acknowledgements
Not applicable.

Funding
None

Contributions
A.M.B: Conceptualization, Methodology, Software, Writing – Original Draft, Visualization, Project Administration. U.M: Data Curation, Writing - Review & Editing, Supervision.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
The author has no conflicts of interest to disclose.

References

[1] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved December 21, 2022, from https://bitcoin.org/bitcoin.pdf
[2] Bayer, D., Haber, S., & Stornetta, W. S. (1993). Improving the efficiency and reliability of digital time-stamping. In *Sequences II* (pp. 329–334). Springer.
[3] Monrat, A. A., Schelen, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access, 7*, 117134–117151.
[4] Nair, R., Zafrullah, S. N., Vinayasree, P., Singh, P., Zahra, M. M. A., Sharma, T., & Ahmadi, F. (2022). Blockchain-based decentralized cloud solutions for data transfer. *Computational Intelligence and Neuroscience*, 2022, Article 8209854. https://doi.org/10.1155/2022/8209854
[5] Maesa, D., & Mori, P. (2020). Blockchain 3.0 applications survey. *Journal of Parallel and Distributed Computing, 138*, 99–114.
[6] Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-based applications in education: A systematic review. *Applied Sciences, 9*(2400).
[7] Nair, R., & Bhagat, A. (2020). Healthcare information exchange through blockchain-based approaches. In *Transforming businesses with bitcoin mining and blockchain applications* (pp. 234–246). IGI Global. https://doi.org/10.4018/978-1-7998-0186-3.ch014
[8] Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare, 7*(56).
[9] Andoni, M., et al. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews, 100*, 143–174.
[10] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. *Future Generation Computer Systems, 88*, 173–190.
[11] Alabdulwahhab, F. A. (2018). Web 3.0: The decentralized web blockchain networks and protocol innovation. In *Proceedings of the 1st International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1–4).
[12] Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation, 5*, 1–14.
[13] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PLoS ONE, 11*, e0163477.
[14] Paulavičius, R., Grigaitis, S., Igumenov, A., & Filatovas, E. (2019). A decade of blockchain: Review of the current status, challenges, and future directions. *Informatica, 30*, 729–748.
[15] Zhou, N., Wu, M., Wang, R., & Wang, D. (2023). Research on the architecture of transactional smart contracts in blockchain systems. *Electronics, 12*(18), 3923. https://doi.org/10.3390/electronics12183923
[16] Suresh, V., & Palanisamy, K. (2024). Blockchain-aware decentralized identity management and access control (BADIMAC). *Computer Networks, 246*, 110567. https://doi.org/10.1016/j.comnet.2024.110567
[17] Sun, M., Bi, Y., & Xie, L. (2024). A blockchain and zero-knowledge proof based data security scheme for data trading. *Electronics, 13*(21), 4260. https://doi.org/10.3390/electronics13214260
[18] Zheng, Z., Zhang, S., Huang, Z., & Gong, T. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems, 105*, 475–491.
[19] Methmal, J. W. (2023). *Zero-knowledge proofs: A comprehensive review of applications, protocols, and future directions in cybersecurity* (Technical report). Asia Pacific Institute of Information Technology.
[20] Aad, A., Goldwasser, I., & Micali, S. (2023). Zero-knowledge proof. In *Trends in data protection and encryption technologies*. Springer.

[21] Othman, U., & Callahan, J. (2017). The Horcrux protocol: A method for decentralized biometric-based self-sovereign identity. *arXiv*. https://doi.org/10.48550/arXiv.1711.07127
[22] Bartoletti, D., & Pompianu, L. (2017). An empirical analysis of smart contracts: Platforms, applications, and design patterns. *arXiv*. https://doi.org/10.48550/arXiv.1703.06322
[23] Chaffer, T. E., & Goldston, J. (2022). On the existential basis of self-sovereign identity and soulbound tokens: An examination of the "self" in the age of Web3. *Frontiers in Blockchain*.
[24] Almomani, O., Arabiat, A. M., Al-Ahmed, H., & Alsariera, E. (2026). Hybridization of deep learning models for multiclass attack detection in wireless sensor networks. *Journal of Communications*, *21*(1), 20–34.
[25] Almomani, O., Arabiat, A., Al Tayeb, M., Almaiah, M. A., Obeidat, M., Aldhyani, T. H., Shehab, R., & Rowad, M. (2025). A robust model for Android malware detection via ML and DL classifiers. *Mesopotamian Journal of Big Data*, 261–277. https://doi.org/10.58496/MJBD/2025/017
[26] Shambour, Q., Al-Zyoud, M., & Almomani, O. (2025). Quantum-inspired hybrid metaheuristic feature selection with SHAP for optimized and explainable spam detection. *Symmetry*, *17*(10), 1716. https://doi.org/10.3390/sym17101716
[27] Alsaaidah, D., Almomani, O., Abu-Shareha, A. A., Abualhaj, M. M., & Achuthan, A. (2024). ARP spoofing attack detection model in IoT network using machine learning: Complexity vs. accuracy. *Journal of Applied Data Sciences*, *5*(4), 1850–1860.
[28] Weilenmann, T. M., Schneider, M., & Bernal-Manzanedo, A. (2020). A comprehensive survey on smart contract construction and execution: Paradigms, tools, and systems. *arXiv*. https://doi.org/10.48550/arXiv.2008.13413
[29] Ang, S., Ho, M., Huy, S., & Janarthanan, M. (2026). A multi-layered adaptive cybersecurity framework for the banking sector integrating next-gen firewalls with AI-driven IDPS. *STAP Journal of Security Risk Management*, 2026(1), 67–76.
[30] Huy, S., Ang, S., Ho, M., & Balasubramaniam, V. (2026). Securing API ecosystems in banking: A critical review of cyber risks, control frameworks, and future trends. *Jordanian Journal of Informatics and Computing*, 2026(1), 25–37.
[31] Kadhim, A. F., Hamzah, A. E., Al-Shareeda, M. A., Hussein, A. I., & Sapiee, N. M. (2026). Accurate network intrusion detection using a feedforward neural network and bee colony optimization algorithm. *International Journal of Cybersecurity Engineering and Innovation*, 2026(1).
[32] Al-Na'amneh, Q., Aljawarneh, M., Alhazaimeh, A. S., Hazaymih, R., & Shah, S. M. (2025). Securing trust: Rule-based defense against on/off and collusion attacks in cloud environments. *STAP Journal of Security Risk Management*, 2025(1), 85–114.
[33] Ho, M., Ang, S., Huy, S., & Janarthanan, M. (2026). MUMSPI: A model for usability measurement of single-platform interface for multi-tasking in big data tools. *Jordanian Journal of Informatics and Computing*, 2026(1), 1–14.
[34] Ibrahim, A., Kadhim, A. F., Hamzah, A. E., & Al-Shareeda, M. A. (2026). A secure and scalable IoT home automation architecture with web and biometric control. *International Journal of Cybersecurity Engineering and Innovation*, 2026(1).
[35] Ho, M., Ang, S., Huy, S., & Janarthanan, M. (2026). Cybersecurity risks and challenges in smart cities: A review with insights for Cambodia. *STAP Journal of Security Risk Management*, 2026(1), 87–97.
[36] Addula, S. R., Norozpour, S., & Amin, M. (2025). Risk assessment for identifying threats, vulnerabilities and countermeasures in cloud computing. *Jordanian Journal of Informatics and Computing*, 2025(1), 38–48.
[37] Yassin, A., & Almaiah, M. (2026). Cyber security risk assessment for determining threats and countermeasures for banking systems. *International Journal of Cybersecurity Engineering and Innovation*, 2026(1).

Biographies

Alwi M Bamhdi, is the Associate Professor in the Department of Computer Sciences, College of computing (Al Qunfudhah), Umm Al-Qura University, Saudi Arabia. He received BSc (2008) degree in Computer Science from King Abdul Aziz University in Jeddah, Saudi Arabia, and his MSc (2010) and PhD (2014) in Computer Science respectively from Heriot-Watt University, Scotland, UK. His research interests include Computer Networking, Mobile Ad Hoc Networks, Wireless Sensor Networks, Internet of Things, Cloud Computing, Information & Cyber Security, Digital Investigations & Forensics, Blockchain Technology, Computer Vision, Software Engineering, Performance Evaluation and Automation of Accounting Procedures. He has published many papers in his specialized areas of MANETS as well as in other areas of Computer Science and Information Technology within the scope of his research and teaching activities.