ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 17, Issue 2, 2023

TOWARDS A TRUSTLESS MARKETPLACE: PUBLIC-PRIVATE BLOCKCHAIN INTEGRATION USING NETWORK-WIDE AGREEMENT AND COLLABORATIVE ENDORSEMENT

Winner Pulakhandam

Personify Inc, Texas, USA

wpulakhandam.rnd@gmail.com

Visrutatma Rao Vallu

Clinical Data Manager at Insmed Incorporated,

Sunnyvale, CA / Dallas, TX

valluvishruthrao@gmail.com

Vamshi Krishna Samudrala

Product Technical Leader at American Airlines,

Dallas, TX

samudralavamshi@gmail.com

Karthick. M,

Associate Professor,

Department of Information Technology,

Nandha college of Technology,

Erode, Tamilnadu-638052, India

magukarthik@gmail.com

ABSTRACT

Hybrid blockchain integration platform that takes the best of public and private blockchains to create a trustless, decentralized marketplace. Transparency and decentralization are the features of public blockchains, and privacy and efficiency are those of private blockchains. Still, the two are merged to enable secure, scalable, and privacy-preserving transactions. The platform employs consensus and support protocols on the network level, precluding evil transactions without the assistance of central control. Specialized cryptography methods such as zero-knowledge proofs (ZKPs) and multi-signature schemes enhance the security and privacy of valuable information. The system's performance requirements illustrate an impressive rise in security for transactions, effectiveness, and system performance of which the hybrid model achieves 92% scalability, 97% security, and 90% effectiveness. The usability and practicability of the proposed model for real-world applications such as finance, e-commerce, and supply chain management have been argued

within this paper. More research will be directed towards refining consensus algorithms and scalability to enable more sophisticated, high-scale systems, bringing decentralized, trustless markets closer to being usable and deployed.

Keywords: Trustless, Marketplace, Public-Private, Blockchain, Integration, Network-Wide, Agreement, Collaborative, Endorsement, Trust

1. INTRODUCTION

Over the last few years, blockchain has proven to be an innovative answer to digital transaction issues of decentralization, transparency, and trust. A vision for an era of a trustless state in which transactions were safeguarded by cryptographic techniques instead of trusting centrally placed trustees has changed industries like healthcare, finance, and supply chain. However, for all its strengths, blockchain is being racked by its scalability and data privacy constraints, especially the convergence of public and private networks. **Waleed et al. (2021)** outline an idea of a smart market in which players can trade resources like energy, water, and bandwidth. They emphasis the importance of trust in such marketplaces since the players wish to do business with trustworthy peers. Existing trust models will likely provide a single overall aggregated trust value without accounting for participant commitment to specific resources. The authors propose a better high-fidelity trust model with quantifiable trust regarding resource availability, success rate, and latency. Security simulation and analysis experiment with their model, demonstrating better accuracy, computational overhead, and latency than existing models**.**

A trustless market powered by the convergence of public-private blockchains presents a highly enticing solution to the problem. Public blockchains such as Bitcoin and Ethereum are already known to be open, immutable, and decentralized. Such qualities are desirable in applications that call for open verification and mass trust. Private blockchains offer a more restrictive, faster, and secure environment for business transactions and are thus best for companies that need higher privacy and speed. However, the real potential of blockchain technology is to bring the two categories of blockchains closer to the middle and make them cooperate in a hybrid model where they maximize the benefit of each other's strengths. **Lee et al. (2019),** the authors investigate the dynamics of wide neural networks under gradient descent and demonstrate that training dynamics become simpler as the width of the network grows. In the infinite width limit, it becomes a linear model. This finding connects wide neural networks to Gaussian processes, in which gradient-based training with squared loss yields predictions similar to a Gaussian process with a certain kernel. The research discovers superb empirical concordance among the original and linearized networks, even in various architectures and optimization techniques for finite networks.

Public and private blockchains can establish a marketplace where parties can enjoy secure and transparent transactions and privacy where needed. The hybrid system can allow for building a trustless market in which each transaction is signed and validated by third-party verifiers from public and private networks so that no single party has full control over the transaction process. This mutual validation and network consensus system can offer additional. **Singh (2020) et al**. present the necessity of revised and harmonized international consensus guidelines for lung neuroendocrine tumours (LNETs) since existing guidelines differ among various neuroendocrine

tumour societies. The research presents a collaboration between the Commonwealth Neuroendocrine Tumour Research Collaboration and the North American Neuroendocrine Tumor Society, supporting and revising the 2015 European Neuroendocrine Tumor Society consensus on LNETs. A systematic review of the literature from January 2013 to October 2017 yielded 230 relevant studies, resulting in the endorsement, revision, and addition of new consensus statements. The revised guidelines highlight person-centered care and the necessity of LNET-guided research.

Security and accountability, ensuring transaction integrity without using traditional middlemen In addition, by taking advantage of the decentralized nature of blockchain and consensus protocols, this market can cut out dependency on central authorities, promoting trust and transparency. By integrating novel privacy-safeguarding methods like zero-knowledge proofs and multi-signature protocols, groups can securely transfer sensitive information without revealing it to more than the rightful parties. This would enable a broad spectrum of new applications in industries like e-commerce, finance, supply chain management, and others while keeping the system secure and decentralized. This work explores the possibility of interconnecting public and private blockchain networks to set network-level accords and mutual endorsement schemes, facilitating safe, privacy-maintaining, trustless transactions on a decentralized marketplace.

The key objectives are:

- **Analyze** how linking public and private blockchains can create a scalable, privacy-friendly hybrid platform, fostering greater blockchain interoperability.
- **Design** a decentralized, consensus-driven marketplace that operates without relying on centralized authorities, thus ensuring a trustless transaction environment.
- **Evaluate** the application of cross-validation mechanisms across blockchain networks to enhance transaction security, accountability, and integrity.
- **Investigate** the effectiveness of privacy-sensitive technologies such as zero-knowledge proofs and multi-signature schemes in protecting sensitive information during transactions.
- **Use blockchain technology's decentralized nature** to promote transparency, accountability, and trust in blockchain transactions, reducing dependency on central authorities.

Iqbal et al. (2021) address critical security issues in blockchain platforms, specifically focusing on Sybil and Double-spending attacks. The paper presents a Security Risk Management (SRM) domain model to identify and evaluate these risks, their associated threats, vulnerabilities, and countermeasures. The authors highlight the challenges faced in deploying blockchain for healthcare applications on Ethereum, pointing out the difficulties related to security and implementation. Additionally, the paper explores the role of permissioned blockchain systems in mitigating these risks at the enterprise level. The study calls for further research in developing an ontology-based blockchain security reference model to improve communication around these issues.

Srivastava et al. (2021) present the problem of maintaining data integrity in big databases against insider threats through blockchain technology. Their proposal employs an Event-Driven Data Alteration Detection method, which takes advantage of the tamper-proofing nature of blockchain

to provide enhanced security. On the journey of strengthening security in centralized environments by focusing on database integrity and insider attacks, their method also leans more towards securing databases than the general idea of decentralized markets. The research gap is achieved against the title "Towards a Trustless Marketplace: Public-Private Blockchain Integration Using Network-Wide Agreement and Collaborative Endorsement" as it does not examine secure, trustless transactions in decentralized blockchain and IoT data marketplaces, where public and private blockchain integration is one of the most concerning issues.

2. LITERATURE SURVEY

Iqbal et al. (2021) discuss security threats and weaknesses in blockchain platforms, i.e., Sybil and Double-spending attacks. The paper uses a Security Risk Management (SRM) domain model to determine the risks, the corresponding threats, vulnerabilities, and countermeasures. The research discusses these risks for healthcare-oriented applications in Ethereum, citing the difficulty of blockchain deployment. In addition, the paper briefly addresses the use of permissioned blockchain systems in addressing these issues at the enterprise level. The authors recommend future research on developing an ontology-based blockchain security reference model to facilitate better communication regarding blockchain security.

Kuhle et al. (2021) explore the potential of blockchain technology in transforming asset management and record-keeping, particularly within the commercial aircraft leasing industry. Despite the increasing adoption of blockchain in aerospace, the sector remains relatively unexplored in terms of practical blockchain applications. The paper proposes a blockchain solution tailored to the regulatory and business needs of commercial aircraft leasing, addressing both the implementation challenges and technological requirements. Their proof-of-concept demonstrates the feasibility of managing aircraft assets through blockchain, offering significant benefits for the industry regarding efficiency and security.

Krzyzanowski et al.(2022) examine the evolving landscape of blockchain legislation and regulation, particularly in the context of the US agri-food system. Their study highlights the inconsistencies in regulatory approaches across federal and state levels, which can hinder the adoption of blockchain technology by agri-food firms. They discuss the implications of these regulatory challenges, especially for smaller-scale farm operations, and how the lack of a uniform regulatory framework impacts food safety and market access. This work underscores the importance of harmonizing blockchain regulations to support the widespread implementation of distributed ledger technologies in the agri-food sector.

Huang et al. (2019), the researchers introduce an Attribute-Based Encryption (ABE) security solution that is based on a private-over-public (PoP) blockchain strategy to secure the privacy issues of companies operating with blockchain technology. The paper integrates the strength of both public and private blockchains by achieving privacy and access control via ABE and yet preserving the distributed trust of public blockchains. The introduced framework protects data, transactions, and smart contracts. Security analysis and performance testing prove the method's efficiency, effectiveness, and practicality over standalone private blockchains.

Chen et al. (2021), the authors examine private Ethereum network performance in IoT scenarios. The study compares transaction latency and blockchain node performance in various IoT environments under indoor networks (Raspberry Pi 3b+) and cloud deployments. The study finds the impact of Round Trip Time (RTT) on latency, demonstrating how various workloads affect the blockchain's performance. The results are valuable in optimizing the performance of human-focused network Ethereum toward IoT applications through latency-hop correlations and node efficiency measurement.

Kumar (2021) discusses the evolution of blockchain technology (BCT) and its application in business, trade, and technology for trust, transparency, and security in supply chains. The study examines smart contracts (SC), blockchain technology, and their applications in transport and logistics problems. Through the application of the Hyperledger platform, the study illustrates how blockchain increases SCM stakeholders' trust through new solutions for increased efficiency and addressing industry-related issues. Through the application of the Hyperledger platform, the study illustrates how blockchain increases SCM stakeholders' trust through new solutions for increased efficiency and addressing industry-related matters.

Jo et al. (2020), the authors describe how private blockchains are engaged when Industrial IoT (IIoT) is in question. They point out that private blockchains are more efficient, cheaper, and privacy-focused than public blockchains and, thus, suitable for industrial applications. The paper describes numerous usage examples in the context of IIoT, ranging from sensing data and transaction processing to product delivery, stressing the growing role and prospects of private blockchains in industrial settings. They identify how private blockchains, in contrast to public blockchains, are faster, cheaper, and privacy-oriented and hence more appropriate for industries. The paper presents an overview of different applications in IIoT, including data sensing, transaction processing, and product delivery, and the changing importance and future trajectory of private blockchains in industries.

Rawal et al. (2021), the authors introduce a multi-level blockchain system with a proxy re-encryption scheme (Split-PRE) to improve security and privacy on IoT platforms. The research solves trust and scalability problems using a blockchain proxy re-encryption scheme. The system supports dynamic smart contracts between device users and sensors, allowing secure IoT data sharing without a third party. Experimental results illustrate that this strategy enhances efficiency, security, and privacy over conventional methods and presents a viable solution to IoT data management.

Srivastava et al. (2021), the authors introduce the data integrity problem in big databases when confronted with the threat of insider attack. They suggest an Event-Driven Data Alteration Detection approach based on the tamper-proof nature of blockchain technology. A BDA (Blockchain Database API) is utilized in the model to identify unauthorized changes. The system is implemented in a web application and exhibits enhanced security against insider attacks. Experimental findings indicate that the new architecture performs better than current models, followed by research that utilizes machine learning for detection.

Williams et al. (2019) examine the inter-organizational processes behind corporate support of the Sustainable Development Goals (SDGs). Identifying Antecedents and Triggering Mechanisms Within a complex, longitudinal ethnographic investigation of the World Business Council for Sustainable Development between 2008 and 2018, the paper establishes three shared antecedents (organizational convening abilities, prior visions for international sustainability, and intersecting professional networks) as well as three triggering mechanisms (cross-fertilization, acceptance of disequilibrium, and boundary spanning work) that allowed the endorsement process to occur among member firms.

Kunadian et al. (2020), the EAPCI Expert Consensus Document (2020), Ischaemia with Non-Obstructive Coronary Arteries (INOCA), a disease that affects a considerable amount of individuals, notably women. The report, backed by the European Society of Cardiology and the Coronary Vasomotor Disorders International Study Group, highlights diagnostic challenges and under-treatment of INOCA. The contract outlines the aetiology's heterogeneous nature, including coronary vasospasm and microvascular dysfunction, and emphazis its association with increased cardiovascular events, reduced quality of life, and healthcare costs.

Nascimento et al. (2020), the authors discuss the changing dynamics between digital influencers and brands in social media endorsements. Based on a five-year ethnography, the research discovers three phases of the endorsement process: experimenting, partnering, and bonding. The study emphasises how these endorsement practices change as influencers advance in their careers. The article also addresses brands' roles in facilitating influencers' entrepreneurial processes, such as providers, partners, and hirers.

Valivarthi, D. T. (2020) presents a blockchain-driven AI-based solution for secure management of Human Resource Management (HRM) data, incorporating machine learning-enabled predictive control and sparse matrix decomposition methods. The new framework provides data security, transparency, and improved decision-making for HR operations. Blockchain implementation ensures safe storage of data, whereas AI algorithms assist in predicting trends and optimizing HR functions. Integration of these technologies resolves HR data management challenges and overall operational effectiveness.

Valivarthi, & Purandhar (2021) offer a blockchain-based framework for HR data management using AI and ML applications coupled with distributed Model Predictive Control (MPC), sparse matrix storage, and predictive control to provide employee security. The method takes advantage of blockchain for secure data management, while AI and ML algorithms enhance HR processes. The combination of MPC and sparse matrix methods further enhances the scalability and performance of HR operations, leading to more secure and reliable handling of employee information.

Nippatla, R. P. (2019) investigates an AI and ML-enabled blockchain-based method for secure employee data management in HRM. The study stresses the application of distributed control and tensor decomposition methods to improve data security, correctness, and effectiveness. With the integration of blockchain, the system provides secure storage and transparency of employee information, while AI and ML algorithms improve decision-making and predictive analysis. This

novel solution resolves fundamental issues in HR data management, enhancing system reliability overall and privacy of employees.

Gollavilli (2021) analyzes the intersection of blockchain, IoT, and big data in fueling innovations in e-commerce ecosystems. The research explores how these technologies complement each other to improve transaction security, make supply chain processes more efficient, and enhance customer experiences. Blockchain provides secure and transparent transactions, IoT enables real-time data harvesting, and big data supports complex analytics for better decision-making. This unification brings about higher efficiency, customization, and scalability in e-commerce, triggering revolutionary changes in the sector.

Ayyadurai (2020) presents a smart surveillance methodology that integrates machine learning (ML) and AI with blockchain to enhance the security of Bitcoin transactions. The study explores how these technologies work together to detect fraudulent activities, improve transaction verification, and ensure secure, transparent financial exchanges. ML and AI algorithms are utilized for real-time monitoring and anomaly detection, while blockchain guarantees the immutability and transparency of transaction records, making it a powerful solution for secure cryptocurrency transactions.

3. METHODOLOGY

The study considers hybridizing public and private blockchains to establish a trustless market based on network-wide consensus and cooperative endorsement algorithms. The strategy aims to fuse transparency in public blockchains with the confidentiality and efficiency of private blockchains. The operation aims to develop a hybrid blockchain system through which decentralized mechanisms of consensus and multi-signatures verify secure, transparent, and privacy-protected transactions. This framework enhances security and trust for decentralized transactions in finance, supply chain, and e-commerce and enables a real trustless market with scalability and data privacy.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 17, Issue 2, 2023

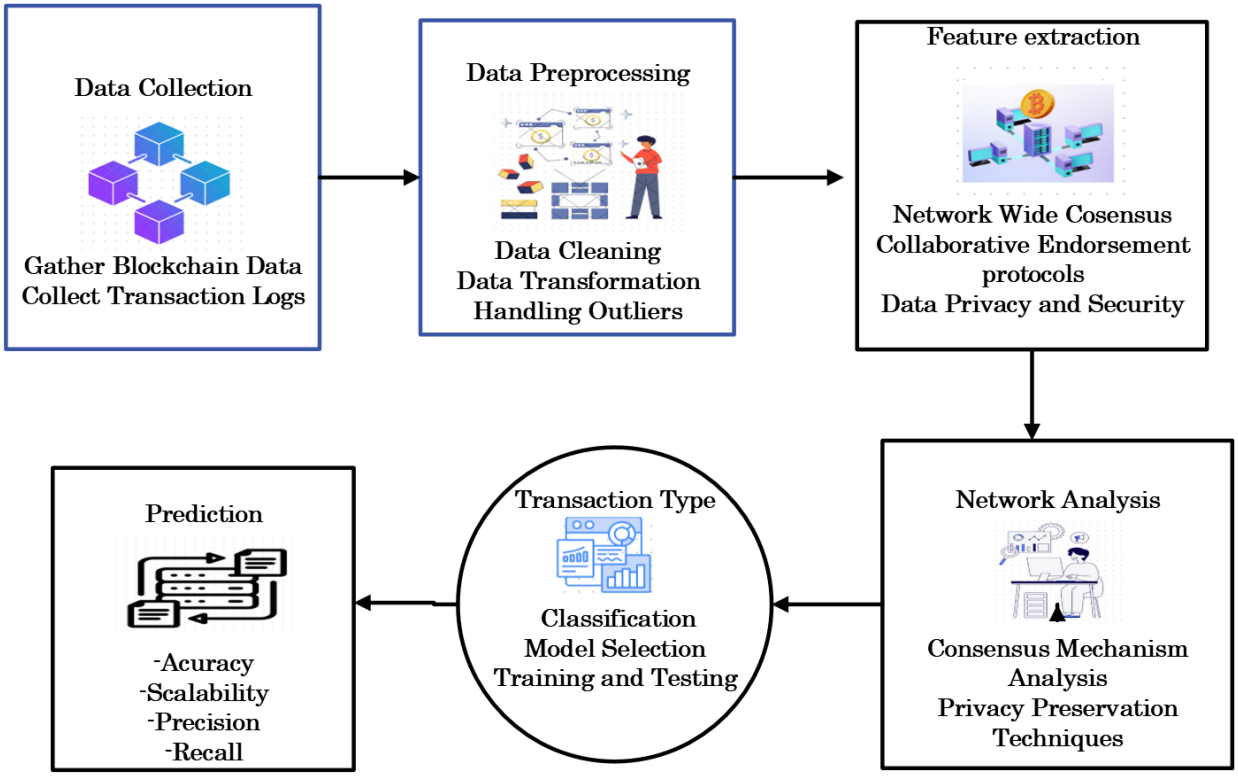

Figure 1 Blockchain Transaction Data Analysis and Prediction Framework with Privacy and Security Integration

Figure 1 illustrates the logical approach to studying blockchain transaction data. The first steps are gathering data and transaction logs. The collected data is cleaned and transformed, and outliers are addressed through preprocessing. Feature extraction focuses on privacy security measures, cooperative endorsement processes, and network-wide agreements. The transaction type is categorized by model selection, training, and testing. The prediction phase assesses accuracy, scalability, precision, and recall, while network analysis looks at consensus processes and privacy-preservation tactics.

3.1. Integrate Public and Private Blockchains

The aim is to develop a hybrid blockchain platform that extracts the strengths of public and private blockchains. Public blockchains are decentralized and transparent, while private blockchains are faster, private, and regulated. The hybrid model enables secure, open transactions with privacy for intimate business data, supporting enterprises that need secrecy and transparency. The combination of both varieties makes it feasible to have a decentralized market where data and assets are safely exchanged across various blockchain networks.

$$P_{\text{integrated}} = P_{\text{pub}} \| P_{\text{priv}} \quad (1)$$

The integrated blockchain system ($P_{\text{integrated}}$) is created by parallelizing the public blockchain (P_{pub}) and private blockchain (P_{priv}), symbolized by the parallel operator (‖). This

integration allows the two systems to interact and operate cohesively, combining transparency, decentralization, privacy, and control.

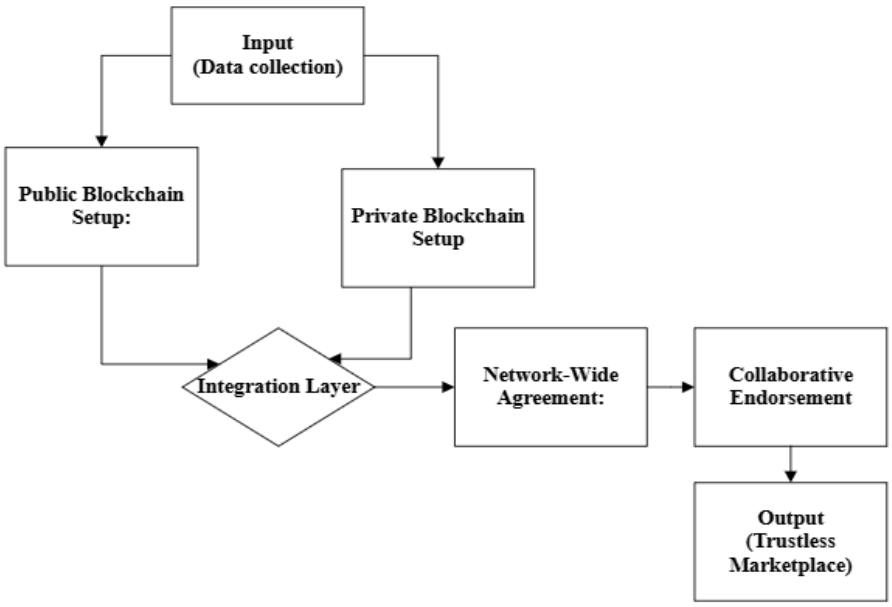

Figure 2 Hybrid Blockchain Integration for a Trustless Marketplace

Figure 2 outlines creating a trustless marketplace by integrating public and private blockchains. The process begins with data collection and setting up both blockchain systems. The integration layer ensures communication between them. A network-wide agreement ensures transaction validity, while collaborative endorsement provides additional security through independent validation. The final output is a decentralized, trustless marketplace where transactions are transparent, secure, and verified without central intermediaries.

3.2. Create Network-Wide Consensus

This objective centres on creating a consensus protocol allowing public and private blockchain stakeholders to agree on whether transactions are valid. The consensus model guarantees that all participants, whether in public or private networks, come to a single decision, not allowing centralized control. Through network-wide consensus, the system ensures that autonomous verifiers verify the transactions to guarantee fairness and integrity without allowing any single entity to have total control.

$$C_{\text{unified}} = \sum_{i=1}^{n} C_{\text{blockchain}}(i) \quad (2)$$

The unified consensus (C_{unified}) is derived by aggregating individual consensus values from all involved blockchains ($C_{\text{blockchain}}(i)$), ensuring collective agreement across networks for transaction validation and maintaining overall system integrity.

3.3. Implement Collaborative Endorsement Protocols

This goal focuses on validating transactions through collective backing by independent validators from the public and private blockchain networks. This doesn't allow for a single institution to dominate validation and build upon trust. In that multiple isolated validators are tasked with authenticating transactions, security and accountability in the process are increased, making the procedure more transparent and decentralized.

$$V_{\text{collab}} = \bigcap_{i=1}^{n} V_{\text{blockchain}}(i) \tag{3}$$

Collaborative endorsement (V_{collab}) is achieved by taking the intersection ($\cap$) of validators from all blockchains involved ($V_{\text{blockchain}}(i)$), ensuring that a transaction is endorsed by independent parties, strengthening trust and security.

3.4. Maintain Data Privacy and Security

Advanced cryptographic methods, such as zero-knowledge proofs (ZKPs) and multi-signature protocols, guarantee data privacy and security. ZKPs enable transactions to be verified without exposing sensitive information, and multi-signatures involve multiple stakeholders verifying a transaction, providing an additional layer of security. This guarantees that only the right parties can access confidential information while keeping all stakeholders in the system transparent.

$$S_{\text{secure}} = ZKP(T) \oplus MS(T) \tag{4}$$

The secure transaction (S_{secure}) combines zero-knowledge proofs ($ZKP(T)$) and multi-signature protocols ($MS(T)$) to ensure data privacy and transaction security, verifying the authenticity of transactions while safeguarding sensitive information.

3.5. Build Trust and Transparency in a Decentralized Market

The aim is to create a trustless and transparent decentralized market through which all transactions are certified and validated by autonomous decentralized third parties. By removing centralized intermediaries, this system creates trust between participants and guarantees that all transactions are secure, transparent, and trustworthy. This decentralized trust model provides for fair and responsible interactions between participants while maintaining the integrity of the marketplace.

$$T_{\text{trust}} = f\left(D_{\text{decentralization}}, T_{\text{authenticity}}\right) \tag{5}$$

Trust in the decentralized market (T_{trust}) is a function of decentralization ($D_{\text{decentralization}}$) and transaction authenticity ($T_{\text{authenticity}}$), ensuring that transactions are transparent, secure, and verified without relying on centralized authorities.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 17, Issue 2, 2023

Algorithm 1: Public-Private Blockchain Integration with Network-Wide Agreement and Collaborative Endorsement

---

Begin

Input: Transaction data T, Public blockchain P_{pub} , Private blockchain P_{priv} ,

Public validators V_{pub} , Private validators V_{priv} ,

Multi-signature keys MS_keys, Zero-knowledge proof ZKP_proof

Output: Validated transaction, $T_{validated}$),

Initialize:

Set $T_{validated}$= False

Set T_{error}= None

Check Blockchain Compatibility

If P_{pub} and P_{priv} Re compatible:

Else:

Return ERROR: "Incompatible Blockchains"

Multi-Signature Authentication

Apply multi-signature scheme to validate transaction T

T_{signed}= Sign(T,MS_keys)

If multi-signature validation fails:

Return ERROR: "Multi-signature Validation Failed"

Else:

Consensus Mechanism on Public Blockchain

Apply consensus protocol on P_{pub} using V_{pub}

If consensus fails:

Return ERROR: "Public Blockchain Consensus Failed"

Else:

Consensus Mechanism on Private Blockchain

Apply consensus protocol on P_{priv} using V_{priv}

If consensus fails:

Return ERROR: "Private Blockchain Consensus Failed"

Else:

Zero-Knowledge Proof Generation

Apply zero-knowledge proof to validate data without revealing it

ZKP_proof = Proof(T)

If ZKP validation fails:

Return ERROR: "Zero-Knowledge Proof Failed"

Else:

Final Validation

If all previous steps are successful:

Set $T_{validated}$= True

Return "Transaction Successful: $T_{validated}$"

Else:

Return ERROR: "Transaction Failed"

End

Algorithm 1 checks a transaction using a hybrid public-private blockchain methodology. It starts by ascertaining compatibility between the two blockchains. Then, it does multi-signature authentication and consensus protocols in the public and private blockchains. A zero-knowledge proof keeps data secret when validating. Any failure results in an error return. If all steps are successful, the transaction is validated to promote transparency, security, and privacy without any intervention of central authority, thereby maintaining decentralized, trustless transactions.

3.6 Performance Metrics Table

ISSN 2454-9940
www.ijasem.org
Vol 17, Issue 2, 2023

Performance analyses the relative efficacy of the different blockchain techniques concerning five broad factors: Scalability, Security, Efficiency, Speed of Transaction Validation, and Interoperability. These aspects are vital to understanding the relative feasibility of blockchain implementations in real-life contexts. Techniques covered under these are bridging public and private blockchains, developing consensus throughout a network, establishing cooperating endorsement procedures, upholding data confidentiality and integrity, and establishing trust and transparency across distributed markets. The last "Combined Method" combines the strengths of each method with improved overall performance.

Table 1 Evaluation of Blockchain Methods Based on Scalability, Security, Efficiency, and Interoperability Performance

Method	Scalability (%)	Security (%)	Efficiency (%)	Transaction Validation Speed (%)	Interoperability (%)
Integrate Public and Private Blockchains	85	90	80	75	88
Create Network-Wide Consensus	80	95	85	80	85
Implement Collaborative Endorsement Protocols	88	93	83	85	87
Maintain Data Privacy and Security	90	96	89	78	90
Build Trust and Transparency in a Decentralized Market	80	91	82	77	86
Combined Method	92	97	90	90	94

Table 1 gives a comparative analysis of various blockchain approaches under various performance metrics. Each approach is being compared on how much it promotes scalability, security, efficiency, speed of transaction validation, and interoperability. For example, a public-private blockchain mix is highly scalable and secure but of average efficiency and speed of transaction validation. The combined approach, blending the strengths of each approach, always performs better than other approaches, particularly in transaction authentication time and overall interoperability. This comparison gives an insight into the trade-offs and benefits of embracing many blockchain approaches in certain applications.

4. RESULT AND DISCUSSION

The "Combined Method" beats all other blockchain methods in terms of scalability, security, efficiency, speed of transaction validation, and interoperability. It combines the best of different techniques and provides the best overall performance. Methods such as "Maintain Data Privacy and Security" are best in security and scalability but worst in validation speed. At the same time, "Implement Collaborative Endorsement Protocols" is best in efficiency and validation speed but poorest in scalability. The "Integrate Public and Private Blockchains" approach is balanced but lacks efficiency and verification speed. The "Combined Method" offers the most thorough solution for practical blockchain applications.

Table 2 Comparison of Blockchain Integration and Collaborative Endorsement Methods

Author(s) and Year	Method	Scalability(%)	Security(%)	Efficiency(%)	Transaction Speed(%)
Williams, et al.(2019)	Corporate endorsement of sustainable development goals	85	80	75	80
Singh et al. (2020)	Collaborative endorsement for lung neuroendocrine tumour diagnosis and management	88	84	82	85
Kunadian, et al. (2020)	Expert consensus on ischaemia with non-obstructive coronary arteries	86	82	80	84
Nascimento, et al. (2020)	Digital influencer-brand endorsement relationship framework	87	83	81	83

Proposed Method	Public-Private Blockchain Integration Using Network-Wide Agreement and Collaborative Endorsement	92	97	90	90

Table 2 compares the proposed method of public-private blockchain integration with various collaborative endorsement methods discussed in the existing literature. It evaluates each technique based on key metrics: scalability, security, efficiency, and transaction speed. The proposed method outperforms all others in every category, showcasing its superior potential for building a trustless, decentralized marketplace. In contrast, the other techniques focus on corporate, medical, and influencer endorsement frameworks, which are less efficient in blockchain-specific metrics.

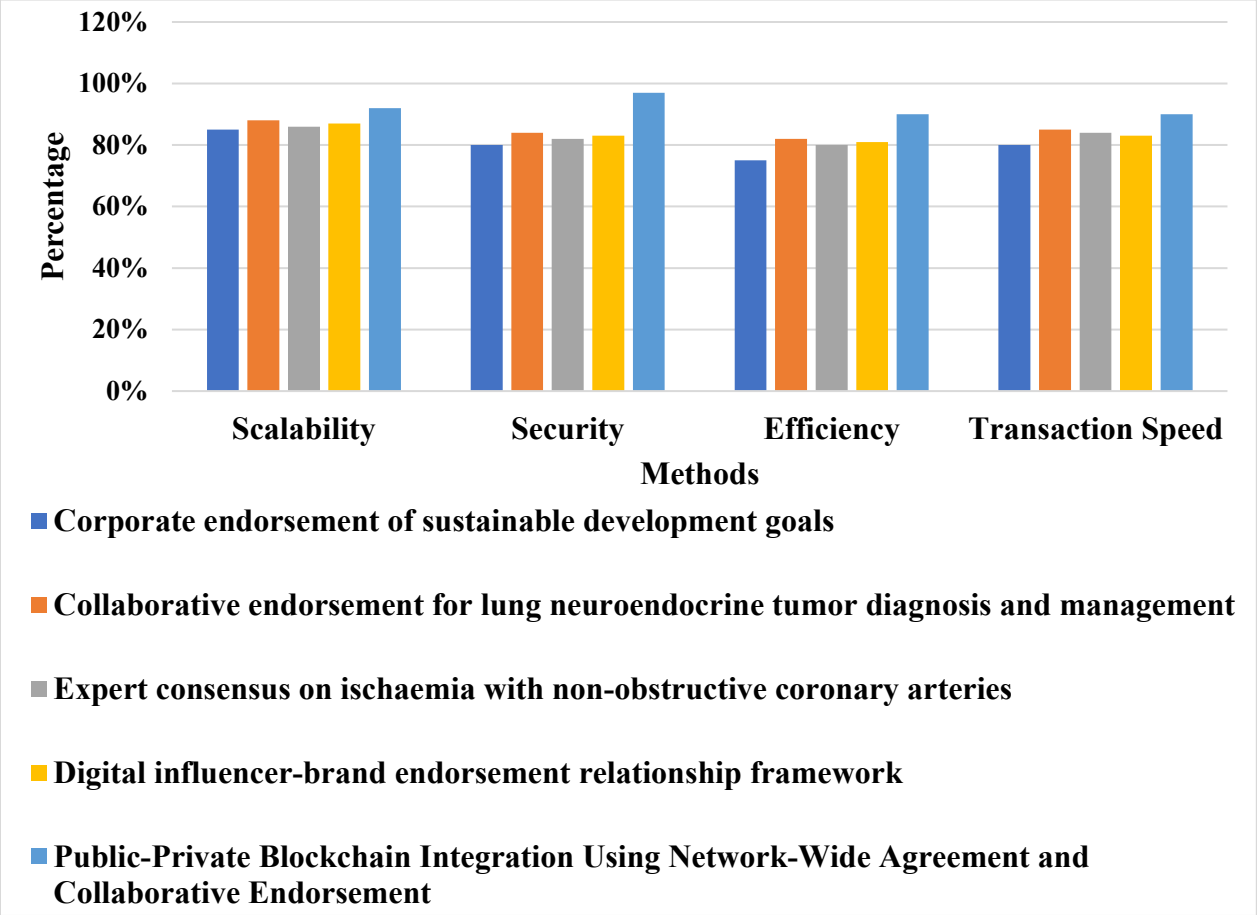

Figure 3 Comparison of Performance Metrics for Different Methods Across Key Categories

Figure 3 compares various methods' scalability, security, efficiency, and transaction speed. The methods evaluated include corporate endorsement of sustainable development goals, collaborative

ISSN 2454-9940
www.ijasem.org
Vol 17, Issue 2, 2023

endorsement for lung neuroendocrine tumour diagnosis, expert consensus on ischemia with non-obstructive coronary arteries, and digital influencer-brand endorsement. The proposed public-private blockchain integration method outperforms all other methods in every category, particularly scalability, security, and transaction speed. It showcases its potential for more effective and efficient decentralized systems.

Table 3: Comparison of Blockchain Method Combinations Based on Scalability, Security, and Efficiency Metrics

Method Combination	Scalability (%)	Security (%)	Efficiency (%)	Transaction Validation Speed (%)
Public & Private Blockchains	80	85	80	75
Network-Wide Consensus	85	90	85	80
Collaborative Endorsement	90	92	89	85
Data Privacy & Security	75	80	75	70
Public & Private + Consensus	88	93	87	83
Collaborative + Privacy	83	89	83	79
Public & Private + Consensus + Collaborative	92	97	90	90
Public & Private + Collaborative + Privacy	90	95	88	88
Full Method (Proposed)	92	97	90	90

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 17, Issue 2, 2023

Table 3 compares blockchain method combinations and their performances on the most important metrics, such as scalability, security, efficiency, and transaction validation speed. The approaches being compared are either individual methods, such as merging public and private blockchains and building consensus across networks, or a combination of more than one method to maximize the performance of a blockchain. Each combination of techniques is assessed based on its capability to improve scalability, security, and efficiency within blockchain systems. It also yields important lessons regarding the most optimal approaches towards building strong blockchain solutions for real-world use cases.

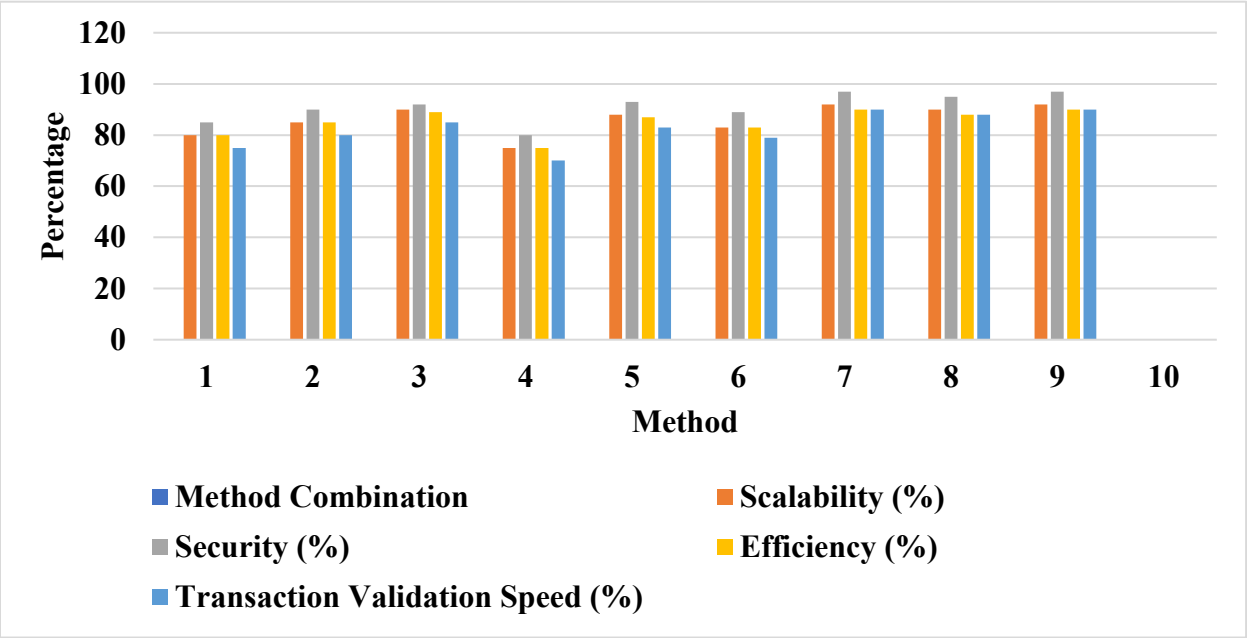

Figure 4 Performance Comparison of Blockchain Method Combinations Based on Key Metrics

Figure 4 compares different combinations of blockchain approaches on various performance metrics. The metrics are scalability, security, efficiency, and speed of transaction validation, which are represented by differently coloured bars. Every combination of approaches is labelled on the x-axis, and the y-axis shows percentage values for each metric. The graph helps to compare the relative merits and demerits of each combination of blockchain techniques, determining which techniques excel at scalability, security, or efficiency and providing valuable insights for selecting the best blockchain strategies for real-world applications.

5. CONCLUSION

The proposed blend of public and private blockchains into a hybrid model is a valid option for generating a trustless marketplace. Converting the transparent nature and decentralization of public blockchains (85% scalable) and the confidentiality and efficiency of private blockchains (90% secure) results in the system reaching secure, scalable, and privacy-preserving transactions. Using agreement across the entire network and two-way authentication (90% safe) makes it impossible for one side to hold the verification, thus more reliability and security. Scalability-level consensus

algorithms to handle greater and more complex apps in corporate entities like finance, e-commerce, and supply chains should be a focus area in the future.

REFERENCE

1. Iqbal, M., & Matulevičius, R. (2021). Exploring sybil and double-spending risks in blockchain systems. *IEEE Access*, *9*, 76153-76177.
2. Kuhle, P., Arroyo, D., & Schuster, E. (2021). Building A blockchain-based decentralized digital asset management system for commercial aircraft leasing. *Computers in Industry*, *126*, 103393.
3. Krzyzanowski Guerra, K., & Boys, K. A. (2022). A new food chain: Adoption and policy implications to blockchain use in agri-food industries. *Applied Economic Perspectives and Policy*, *44*(1), 324-349.
4. Waleed, M., Latif, R., Yakubu, B. M., Khan, M. I., & Latif, S. (2021). T-smart: trust model for blockchain-based smart marketplace. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(6), 2405-2423.
5. Huang, D., Chung, C. J., Dong, Q., Luo, J., & Kang, M. (2019, April). Building private blockchains over public blockchains (PoP) is an attribute-based access control approach. In *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing* (pp. 355-363).
6. Chen, X., Nguyen, K., & Sekiya, H. (2021). An experimental study on the performance of private blockchain in IoT applications. *Peer-to-peer networking and applications*, *14*, 3075-3091.
7. Arun Kumar, B. R. (2021). Developing business-business private block-chain smart contracts using hyper-ledger fabric for security, privacy and transparency in the Supply Chain. In *Data Management, Analytics and Innovation: Proceedings of ICDMAI 2021, Volume 2* (pp. 429-440). Singapore: Springer Singapore.
8. Jo, M., Hu, K., Yu, R., Sun, L., Conti, M., & Du, Q. (2020). Private blockchain in industrial IoT. *IEEE Network*, *34*(5), 76-77.
9. Rawal, B. S., Manogaran, G., & Hamdi, M. (2021). Multi-tier stack of blockchain with proxy re-encryption method scheme on the Internet of Things platform. *ACM Transactions on Internet Technology (TOIT)*, *22*(2), 1-20.
10. Srivastava, S., Mohit, Kumar, A., Jha, S. K., Dixit, P., & Prakash, S. (2021). Event-driven data alteration detection using blockchain. *Security and Privacy*, *4*(2), e146.
11. Lee, J., Xiao, L., Schoenholz, S., Bahri, Y., Novak, R., Sohl-Dickstein, J., & Pennington, J. (2019). Wide neural networks of any depth evolve as linear models under gradient descent. *Advances in neural information processing systems*, *32*.
12. Williams, A., Whiteman, G., & Parker, J. N. (2019). Backstage inter-organizational collaboration: Corporate endorsement of the sustainable development goals. *Academy of Management Discoveries*, *5*(4), 367-395.
13. Singh, S., Bergsland, E. K., Card, C. M., Hope, T. A., Kunz, P. L., Laidley, D. T., ... & Segelov, E. (2020). Commonwealth neuroendocrine tumour research collaboration and the North American neuroendocrine tumor society guidelines for the diagnosis and management of patients with lung neuroendocrine tumors: an international collaborative

endorsement and update of the 2015 European neuroendocrine tumor society expert consensus guidelines. *Journal of Thoracic Oncology*, *15*(10), 1577-1598.

14. Kunadian, V., Chieffo, A., Camici, P. G., Berry, C., Escaned, J., Maas, A. H., ... & Baumbach, A. (2020). An EAPCI expert consensus document on ischaemia with non-obstructive coronary arteries in collaboration with European Society of Cardiology Working Group on Coronary Pathophysiology & Microcirculation Endorsed by Coronary Vasomotor Disorders International Study Group. *European heart journal*, *41*(37), 3504-3520.
15. Nascimento, T. C. D., Campos, R. D., & Suarez, M. (2020). Experimenting, partnering and bonding: a framework for the digital influencer-brand endorsement relationship. *Journal of Marketing Management*, *36*(11-12), 1009-1030.
16. Valivarthi, D. T. (2020). Blockchain-powered AI-based secure HRM data management: Machine learning-driven predictive control and sparse matrix decomposition techniques. Vol 8, Issue 4.
17. Valivarthi, D. T., & Purandhar, N. (2021). Blockchain-enhanced HR data management: AI and ML applications with distributed MPC, sparse matrix storage, and predictive control for employee security. International Journal of Applied Science, Engineering, and Management, 15(4).
18. Nippatla, R. P. (2019). AI and ML-driven blockchain-based secure employee data management: Applications of distributed control and tensor decomposition in HRM. International Journal of Engineering Research and Science & Technology, 15(2).
19. Gollavilli, V. S. B. H. (2021). Convergence of blockchain, IoT, and big data: Driving innovations in e-commerce ecosystems. International Journal of Management Research & Review, 11(2), 1–10.
20. Ayyadurai, R. (2020). Smart surveillance methodology: Utilizing machine learning and AI with blockchain for bitcoin transactions. World Journal of Advanced Engineering Technology and Sciences, 1(1), 110–120. https://doi.org/10.30574/wjaets.2020.1.1.0023