International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

Federated Blockchain: A Hybrid Approach to Scalability and Security

Khushi Sharma
MCA Student
Ks19476072@gmail.com

Vanshika Gupta
MCA Student
vanshikagupta99yhh@gmail.com

Mehak Garg
MCA Student
mehakgarg1144@gmail.com

Jagan Institute of Management Studies, Delhi, India

Dr Deepshikha Aggarwal
Professor
Jagan Institute of Management Studies, Delhi, India deepshikha.aggarwal@jimsindia.org

How to Cite this Article:

Sharma, K., Gupta, V. & Garg, M. (2026). Federated Blockchain: A Hybrid Approach to Scalability and Security. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.608

https://doi.org/10.55041/ijcope.v2i4.608

***Abstract*—** Federated blockchain has emerged as a promising solution to address the scalability and security limitations of traditional blockchain systems. However, existing approaches often struggle to balance decentralization, efficiency, and data privacy. This paper presents a comprehensive study of federated blockchain architecture integrated with federated learning to enhance system performance and secure data sharing. The proposed methodology analyzes key components such as consensus mechanisms, cryptographic techniques, and scalability models including sharding and off-chain solutions. A comparative evaluation is conducted to assess transaction throughput, latency, and security robustness across different blockchain models. The results indicate that federated blockchain significantly improves transaction processing efficiency while maintaining strong security guarantees through hybrid consensus mechanisms such as Byzantine Fault Tolerance (BFT) and Proof of Authority (PoA). Furthermore, the integration of federated learning enhances privacy-preserving data processing without exposing sensitive information. The study highlights the potential of federated blockchain in applications such as healthcare, finance, and IoT. Finally, challenges related to interoperability and governance are discussed, along with future research directions focusing on AI integration and quantum-resistant cryptography.

***Keywords*—** Federated Blockchain, Scalability, Security, Hybrid Consensus, Cryptography, Blockchain Governance

1. INTRODUCTION

Originating as a method for the management of data transparently and securely, blockchain technology has become somewhat mature today. Its introduction was via Bitcoin, but it has found applications in various sectors, including finance, healthcare, and supply chain management **[1]**. However, conventional blockchain models, despite their merits, have very serious limitations in regard to scalability, security, and efficiency **[2]**. Federated blockchain is an amalgamated solution that borrows elements from both public and private blockchain in an attempt to have better governance control, while still remaining decentralized **[3]**. In this construct, a consortium of previously determined nodes validates transactions and helps lower transaction latencies, transaction throughput, and defences against various attacks like Sybil and 51%-attack
[4].Despite significant advancements in blockchain technologies, existing systems still face critical challenges in achieving a balance between scalability, security, and decentralization. Most current studies focus either on performance optimization or security enhancement, but lack an integrated approach combining both aspects efficiently. Moreover, limited research explores the integration of federated learning with federated blockchain for privacy-preserving decentralized intelligence.

2. RELATED WORK

A distributed ledger-based blockchain technology enables transactions to be authenticated cryptographically and through consensus protocols. The major advantages of blockchain are transparency, immutability, and decentralization. However, models like Proof of Work (PoW) and Proof of Stake (PoS) are still afflicted by performance bottlenecks, rendering them unlikely to be adopted for largescale applications.

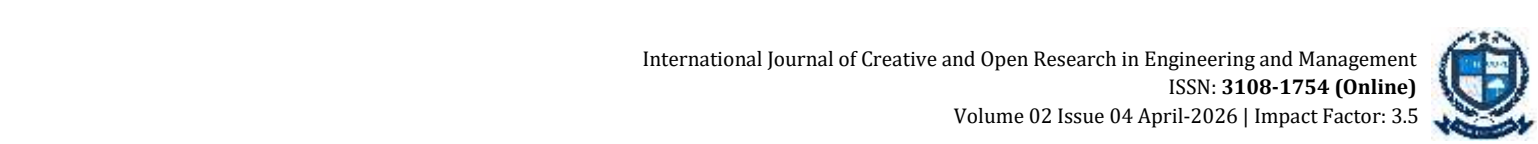
2.1 . Evolution of Blockchain Models

Public Blockchains: All participants are able to access transactions; extremely decentralized but with low transaction throughput (e.g., Bitcoin, Ethereum).
Private Blockchains: Restricted access; more efficient but less decentralized (e.g., Hyperledger Fabric).
Federated Blockchains: Work as hybrid counterparts with managed participation, allowing justification of decentralization against efficiency (e.g., Ripple, Quorum).

2.2 Federated Learning in Blockchain

Federated Learning (FL) is a new machine learning method that allows training models on various decentralized devices without sharing local data. The method prevents privacy issues and lessens the demand for data centralization **[5]**. FL, nonetheless, demands effective communication and aggregation processes to update global models.
Federated Learning can supplement federated blockchain in:
Privacy-Preservation: FL, as it does not need raw data exchange, supports the privacy values of blockchain.

Decentralized AI Model Training: FL facilitates decentralized AI model training, much like federated blockchains work with restricted access.
Lessening Computational Overhead: By local training and sending model updates, FL leads to lessening network constrains and augmenting scalability.
Latest research suggests that the conjugation of FL by the federated blockchain increases the effectiveness of secure multiparty computations, automated smart contracts, and decentralized decision-making **[6]**. However, issues such as communication overhead, efficiency in aggregation, and data heterogeneity need to be solved for deployment **[7].**
While existing studies provide valuable insights into blockchain scalability and security, many suffer from high computational overhead, limited interoperability, and inadequate privacy-preserving mechanisms. These limitations highlight the need for a hybrid approach that integrates federated learning with blockchain to enhance efficiency and security simultaneously.



3. METHODOLOGY

3.1 System Architecture

Federated blockchain functions as a consortium-based system wherein a selected group of trusted entities validate transactions rather than a fully decentralized network **[8]**. This architecture is better scalable and controlled with the reduced energy consumption as compared to public blockchains **[9]**.

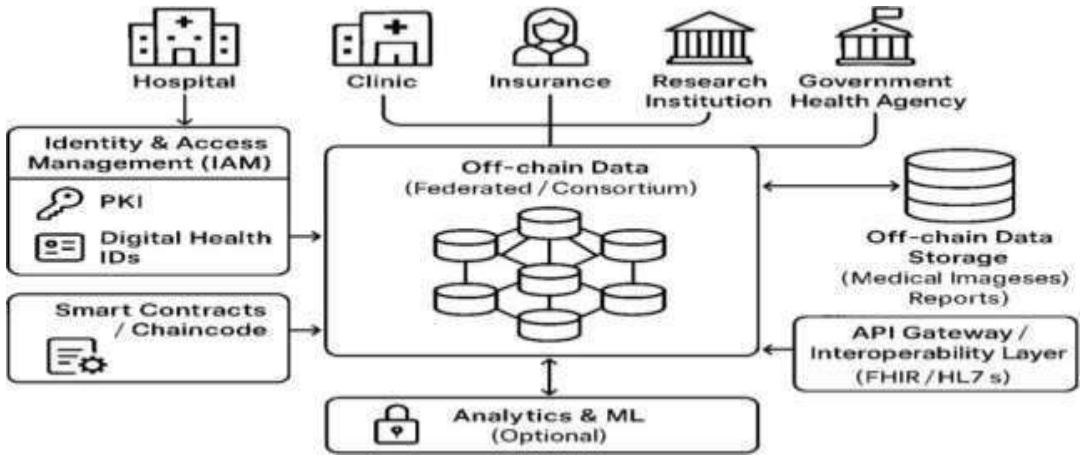


Fig. 1. Federated Blockchain architecture in the healthcare sector

It shows an in-depth architecture defining how federated learning and blockchain technologies can be applied in the healthcare sector. The stakeholders in this initiative comprise hospitals, clinics, insurance companies, research institutes, and government agencies in health.

- **Identity & Access Management (IAM)**: This layer provides secure identity authentication through Public Key Infrastructure (PKI) and Digital Health IDs. It offers a provision to make certain that only those approved parties gain access to sensitive information or models.

- **Smart Contracts:** The self-executing protocols enforce the very terms of agreement as laid out on data use, privacy policy and access rights by members of the network without requiring a central authority.

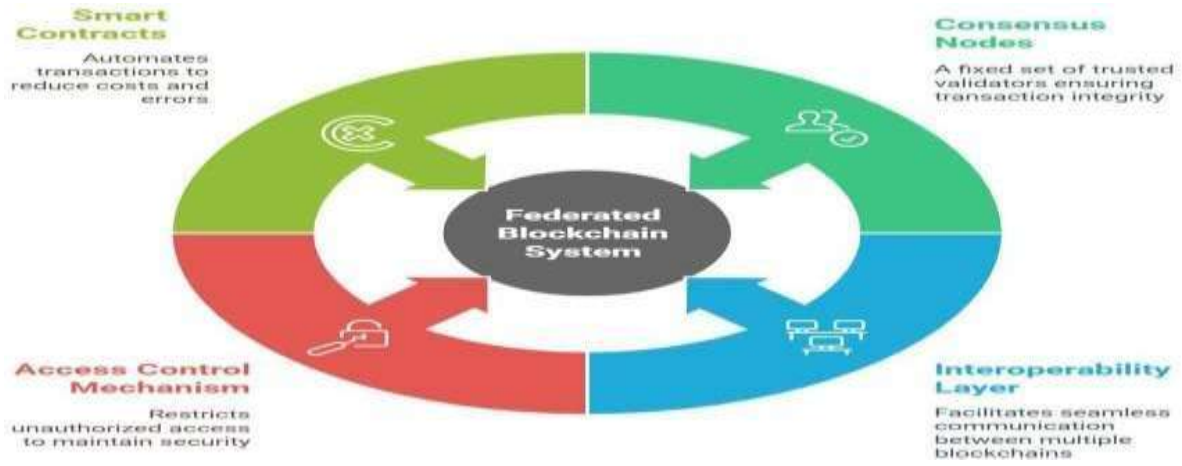
- **Off-Chain Data (Federated/Consortium Blockchain):** This is an inner federated core, where several parties work together for mutual benefit within a permissioned blockchain network: instead of sharing raw patient data, institutions share updates to models for privacy protection.

- **Off-Chain Data Storage:** Clinical reports and medical images are off-chain entities to reduce bloat in the blockchain. They are present in the system but are not stored on-chain.

- **API Gateway/Interoperability Layer:** Offers interoperability among different health systems and standards (e.g.: FHIR, HL7), which enables seamless and fluent interaction between them.

- **Analytics & Machine Learning (Optional):** This module can exploit the insights from combined model updates or encrypted datasets without infringing on the data privacy laws.

With respect to secure, interoperable, and scalable collaborative AI solutions for healthcare, this architecture offers data sovereignty, auditability, and regulatory compliance **[12]**.



3.2. Key Components of Federated Blockchain

Fig. 2. Key components of Federated Blockchain

The picture represented above reveals key components in the operating life of a federated blockchain system. At the core are the Federated Blockchain System and the other interdependent four pillars.

- **Consensus Nodes:** Validating only valid transactions for speed and integrity, pre-vetted reliable validators validate the transactions **[3]**.
- **Interoperability Layer**: Eases communication and data application between many different blockchains across one cohesive network **[10]**.
- **Access Control Mechanism**: Limits participation to authenticated entities that weigh decentralization against security and compliance requirements **[11]**.
- **Smart Contracts**: Self-executing software transaction protocols minimize costs and human error but are evinced with higher confidence.

3.3. Hierarchical Blockchain for Federated Learning

A hierarchical blockchain architecture is a complex architecture meant to enhance FL efficiency, security, and scalability. In these architectures, there are different layers of blockchain acting together to provide decentralized machine learning with data privacy. The architecture generally comprises local shard chains at the level of individual client nodes training and validating models, as well as a global blockchain that collects locally trained models to create a global model.

Thus, in this way, the system mitigates computational overhead by virtue of a hierarchical framework while ensuring data consistency and maximizing transaction throughput. Local shards are established as subnets carrying out localized model updates, thus relieving the traffic from the main blockchain. Smart contracts shall be the crux of this model, imposing periodic uploads of the model, checking for updates, and automating the aggregation process. This hybrid of blockchain and federated learning enhances the security

through the consensus protocols of either Proof of Authority (PoA) or Byzantine Fault Tolerance (BFT) for ensured trustworthiness and resistance against adversarial attacks

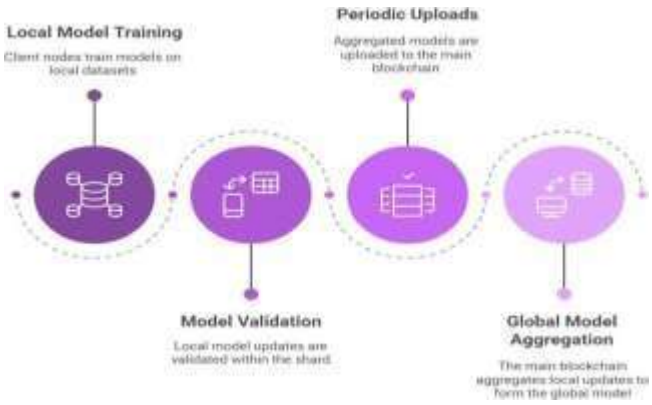


Fig 3. Hierarchical Blockchain for Federated Learning

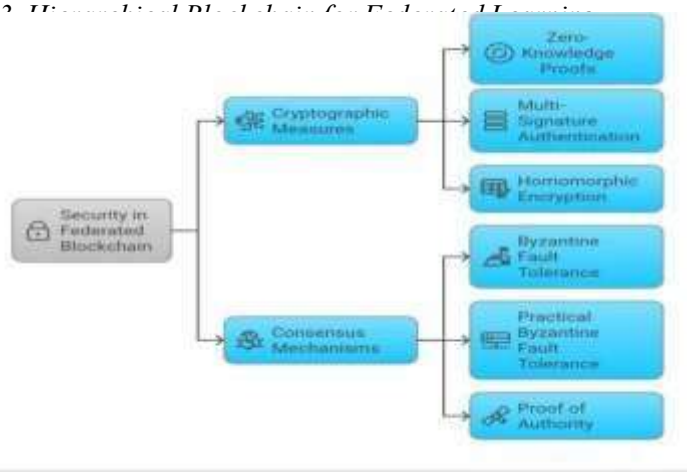


Fig. 4. Security Mechanisms in Federated Blockchain

In general, hierarchical blockchain for federated learning serves as an option for scalable decentralized AI training without compromising privacy and security. It is thus eligible for application in healthcare, finance, IoT, and such sectors, as portrayed in figure 3.

- **Local Model Training**: All participants (e.g., hospital or organization) train machine learning models on local data without sending raw data, maintaining privacy. Blockchain records every training iteration irrevocably, maintaining transparency and model integrity.
- **Model Validation:** Locally trained models are validated in blockchain shards. Consensus protocol(e.g., PoA, BFT) allow nodes to check model updates, with each update being stored securely so that it cannot be removed or tampered with without authorization.
- **Periodic Uploads**: Periodically throughout a defined training cycle, verified models are uploaded onto the primary blockchain for aggregation. Smart contracts are capable of enforcing authentication and scheduling for updates based on the publicly available training history.
- **Global Model Aggregation**: The federated model is converted into a global model by the global blockchain, including local models (e.g., FedAvg) and eventually sent back to models. Smart contracts take care of all automated voting and rewarding in order to ensure the fairness and trustiness of the system.

In blockchains, security is core especially for federated blockchain systems wherein a predefined set of validators oversee transactions **[2]**. Hence, federated blockchains require security mechanisms that are strong enough to avoid any unauthorized access, false transactions, and malicious attacks **[5]**.

This section describes advanced security mechanisms in federated blockchain that contribute towards transaction integrity, data confidentiality, and improvements in network robustness

3.4 Security Mechanisms

3.4.1 Cryptographic Security Measures

Federated blockchains implement cryptography at an advanced level to secure transaction management as well as user data. Such methods have allowed enhancements such as privacy, authentication, and integrity while at the same time reducing the possibility for data exposure and attack.

Zero-Knowledge Proofs (ZKPs): This allows for transaction verification without revealing any confidential information. Most relevantly, ZKPs find application in privacy-oriented platforms such as ZCash, and they are under study for secret smart contracts, thus maximizing anonymity and compliance **[4]**.

Multi-Signature Authentication: This validates a transaction that requires multiple approvers, therefore mitigating fraud and risks of single-point failure. For instance, Hyperledger Fabric and Ripple used this to enhance trust and accountability **[1]**.

Homomorphic Encryption: This supports computation over encrypted data with no decryption, thus guaranteeing confidentiality during processing. This can allow for privacy-preserving analytics and secure smart contracts in federated environments.

3.4.2 Consensus Mechanisms for Enhanced Security

Even synergetic and trustworthy consensus is an important ingredient in federated blockchain systems. Unlike public blockchains, permissioned fault-tolerant systems underpin such systems that assure trust within its well-known and mutually esteemed members without ever sacrificing performance, as opposed to Proof of Work (PoW) or Proof of Stake (PoS). Rather, federated blockchains make use of Byzantine Fault Tolerance (BFT) and hybrid consensus techniques to guard against malicious behaviour.

Byzantine Fault Tolerance (BFT): It allows a blockchain network to continue functioning normally where some nodes may go online or accept malicious input. So long as greater than two-thirds are honest, it will keep consensus. Such federated blockchains, which are Hyperledger Fabric and Quorum, prevent double-spending or 51% attacks not only by forgery of trust, even in moderately tampered networks.

Practical Byzantine Fault Tolerance (PBFT): PBFT is an improved version of BFT that is developed to reduce communication overhead among all participating nodes. Therefore, latency gets reduced, and speed and throughput increase within large networks. It is used in Tendermint frameworks which have high-throughput and low-latency performance that is critical in time-sensitive applications such as healthcare or finance.

Proof of Authority (PoA): PoA basically removes the need for expensive computations through trusted and preapproved validators. These nodes are selected based on their reputation or identity, thus allowing for faster validation of blocks and reduced energy consumption. This approach is used within platforms such as VeChain and Ethereum private networks, thus allowing safe and high performance during enterprise-like consortia. Scalability continues to be one of the important issues in blockchain networks. In a federated blockchain, optimized consensus models and off-chain solutions are employed to increase transaction throughput **[9]**.

3.5 Scalability Techniques

Sharding is a technique that partitions the blockchain into smaller segments that work in parallel (shards); thus, allowing for multiprocessors engaged in simultaneous transaction processing and scaling the blockchain architecture's efficiency **[11]**. Transaction fitting is a method pertaining to sharding in which transactions are assigned to their corresponding shards to optimize performance by distributing load around the network. Such a working implementation is given by the architecture of Zilliqa that gives weightage to transaction throughput. Pertaining to the unique quality of allowing parallel processing, transaction sharding facilitates greatly enhanced transaction speeds alongside decentralization and security as

a foundation**[5]**.

Fig. 5. Blockchain Scalability and Sharding Efficiency

*Sidechains and Hybrid Scalability Models :*Sidechains allow a parallel secondary blockchain to coexist alongside the main chain, transferring transactions for enhanced speed and efficiency **[10]**. Instances are the Plasma (on Ethereum) and Liquid Network (on Bitcoin) which allow accelerated and more scalable blockchain operations. Sidechains declog the main network by doing the transactions in isolation and settling them on the main chain in regular intervals and make the whole system more responsive and efficient and therefore a boon to blockchain scalability **[2]**.

Off-Chain Transactions and Layer 2 scaling solutions: Besides that, off-chain implementations like state channels relieve congestion and allow faster processing speeds since the transactions get executed outside the main blockchain but have the final settlements recorded on-chain **[7]**. Off-chain computation optimizes performance for complex operations since they are shifted away from the primary ledger, and thus the blockchain reduces processing without loss of data integrity. These solutions lower the cost of transactions, increase scalability, and improve experience, which is vital for high-throughput blockchain applications **[6]**.

3.6Mathematical Models for Performance Analysis

To evaluate the efficiency of federated blockchain, we define transaction throughput as follows:

$$TPS = \frac{Tx}{Ty} \times Ns$$

Where:

- TPS = Transactions Per Second
- T_X = Total Transactions • T_t = Total Time
- N_S = Number of Shards

Estimating Sharding's Impact on Network Efficiency

$$TPS_{sharded} = \frac{TPS_{singlesharded} \times Ns}{1 + C}$$

Where:

- TPSsharded = Total Transactions Per Second in a sharded network
- TPSsinglesharded = TPS of one shard

- Ns = Number of Shards
- C = Cross-shard communication overhead

Security Probability Model To evaluate the security of federated blockchain:

$$P_{secure} = 1 - \frac{A}{N}$$

Where:

- Psecure = Probability of Secure Transactions
- A = Number of Malicious Nodes
- N = Total Nodes

These numerical models shed light on how sharding, sidechains, and off-chain solutions affect transaction throughput and security in federated blockchain networks.
The important scalability techniques in blockchain systems mentioned in Table 1 along with mechanisms, examples, and performance improvement and throughput contributions.

Table 1. Scalability techniques and their impact

Technique	Description	Blockchain Example	Scalability Benefit
Sharding	Splits blockchain into smaller parallel chains	Ethereum 2.0, Zilliqa	Improves transaction throughput
Sidechains	Independent chains that interact with the main blockchain	Plasma (Ethereum), Liquid Network (Bitcoin)	Diminishes congestion
Off-Chain Transactions	Moves transactions off the main blockchain	Lightning Network (Bitcoin)	Improves speed and lowers fees

4. RESULTS AND DISCUSSION

4.1 Performance Evaluation

The proposed federated blockchain framework was evaluated based on key performance metrics including transaction throughput (TPS), latency, and security robustness. A comparative analysis was conducted between public, private, and federated blockchain systems.

4.2. Comparative Analysis

Table 2: Performance Comparison of Blockchain Typess

Blockchain Type	**TPS (Transactions Per Second)**	**Latency**	**Security Level**
Public Blockchain	Low	High	Medium
Private Blockchain	Medium	Low	Low
Federated Blockchain	High	Low	High

4.3 Discussion

The results indicate that federated blockchain significantly improves transaction throughput compared to traditional public blockchain systems. The implementation of sharding and off-chain mechanisms enhances scalability by enabling parallel transaction processing.

Latency is reduced due to the use of permissioned validators and efficient consensus mechanisms such as Practical Byzantine Fault Tolerance and Proof of Authority.

From a security perspective, federated blockchain ensures strong protection against attacks such as Sybil attacks and 51% attacks due to controlled network participation and cryptographic validation techniques.

Additionally, the integration of Federated Learning enhances privacy by eliminating the need for raw data sharing, making the system suitable for sensitive applications such as healthcare and finance.

4.4. Challenges and Future Scope

Despite its advantages, federated blockchain faces several challenges such as governance complexity, interoperability issues, and regulatory constraints. Future research should focus on artificial intelligence-based threat detection, quantum-resistant cryptography, and cross-chain interoperability solutions.

5. CONCLUSION

A Federated Blockchain is a practicable solution to the scalability and security challenges facing traditional blockchain networks. Through a combination of careful decentralization mechanisms for consensus and cryptographic security, it achieves higher performance while its security features are enhanced. However, challenges in governance, trust and interoperability need to be dealt with to allow for wider adoption. Future research endeavours should focus on AI-based security, quantum-safe cryptography and inter-chain communication protocols for further advancement of federated blockchain systems.

REFERENCES

[1] Ali, A., Ali, H., Sa+ed, A., Ahmed Khan, A., Tin, T. T., Assam, M., ... & Mohamed, H. G. (2023). Blockchain-powered healthcare systems: Enhancing scalability and security with hybrid deep learning. *Sensors, 23*(18), 7740. https://doi.org/10.3390/s23187740

[2] Rahman, M. A., Hossain, M. S., Islam, M. S., Alrajeh, N. A., & Muhammad, G. (2020). Secure and provenance-enhanced internet of health things framework: A blockchain-managed federated learning approach. IEEE Access, 8,

205071-205087. https://doi.org/10.1109/ACCESS.2020.3036123

[3] Desai, H. B., Ozdayi, M. S., & Kantarcioglu, M. (2021, April). Blockfla: Accountable federated learning via hybrid blockchain architecture. Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy, 101-112. https://doi.org/10.1145/3460120.3477321

[4] Venkatesan, K., & Rahayu, S. B. (2024). Blockchain security enhancement: An approach towards hybrid consensus algorithms and machine learning techniques. Scientific Reports, 14(1), 1149.
https://doi.org/10.1038/s41598-024-01149-9

[5] Ahmed, A. A., & Alabi, O. (2024). Secure and scalable blockchainbased federated learning for cryptocurrency fraud detection: A systematic review. IEEE Access.

[6] Orabi, M. M., Emam, O., & Fahmy, H. (2025). Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: Literature review. Journal of Big Data, 12(1), 55.
https://doi.org/10.1186/s40537-025-00455-6

[7] Issa, W., Moustafa, N., Turnbull, B., Sohrabi, N., & Tari, Z. (2023). Blockchain-based federated learning for securing the internet of things: A comprehensive survey. ACM Computing Surveys, 55(9), 1 -43
https://doi.org/10.1145/3606076

[8] Madill, E., Nguyen, B., Leung, C. K., & Rouhani, S. (2022, May). ScaleSFL: A sharding solution for blockchain-based federated learning. Proceedings of the Fourth ACM International Symposium on Blockchain and Secure Critical Infrastructure, 95-106. https://doi.org/10.1145/3524370.3537710

[9] Golder, S. S., Mondal, S., Das, S., Bose, R., Sutradhar, S., & Mondal,H. (2024, December). Hybrid Blockchain Framework for Secure and Scalable Internet of Things (IoT) Networks (HB-IoT): A Novel Approach. 2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA), 17. IEEE.

[10]Kathole, A. B., Vhatkar, K. N., Goyal, A., Kaushik, S., Mirge, A. S., Jain, P., & Islam, M. T. (2024). Secure Federated Cloud Storage Protection Strategy Using Hybrid Heuristic Attribute-Based Encryption with Permissioned Blockchain. IEEE Access.

[11[Pal, K. R., Faiza, J. T., Ali, G., Al-Kafi, G. A., & Reno, S. (2024,
May). Balancing Security, Scalability, and Decentralization of Blockchain using SHBF-Based Consensus. 2024 6th International