International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(14s) 2026 pp. 333-340
https://doi.org/10.70917/ijcisim-2026-4233
Article

Blockchain-Enabled Trustworthy Federated Learning for Privacy- Preserving Artificial Intelligence: Consensus Protocols, Cryptographic Security, Scalability, and Real-World Deployment

Arthi D[1], R Anand[2], Palaniappan Sambandam[3], Rajesh Kambattan Kovarasan[4], Y Jeevan Nagendra Kumar[5], S.Ashokkumar [6]

[1]Department of Information Technology, Sathyabama Institute of Science and Technology,Chennai,Tamilnadu
Corresponding author: dr.arthidevaraj@gmail.com
[2]Department of Computer Science and Business Systems, Easwari Engineering College, Ramapurem, Chennai. Email: nowhereanand@yahoo.com
[3]Department of Computer Science and Business Systems, Easwari Engineering College, Ramapurem, Chennai. Email: s.palani.in@gmail.com
[4]Department of Computer Science and Engineering Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, Tamilnadu
Email : rajesh.kambattan@gmail.com
[5]Gokaraju Rangaraju Institute of Engineering and Technology Hyderabad-500090
Email:jeevannagendra@gmail.com, jeevannagendra@griet.ac.in
[6]Department of CS, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences,(SIMATS), Saveetha University, Chennai, India,
Email:sabariashok2016@gmail.com

Abstract: Federated learning helps in collaborative training of AI models without transmitting raw data, and hence it is an exciting approach for privacy-conscious applications. Nonetheless, traditional federated learning still suffers from weaknesses such as susceptibility to attacks from malicious actors, susceptibility to model poisoning, single point of coordination, lack of transparency, and scalability issues. Blockchain technology provides a decentralized method of trusting which can help in enhancing the security, accountability, and integrity of federated learning. This paper presents a comprehensive analysis of blockchain based trustworthy federated learning through the examination of the role played by consensus algorithms, cryptographic security techniques, scalability approaches, and deployment strategies. A systematic literature review was conducted using recently published papers from peer-reviewed sources. The selected papers were analyzed using inclusion and exclusion criteria to reveal technological advancements, deployment problems, and practical applications. Consensus methods, which include Proof of Stake, Practical Byzantine Fault Tolerance, Delegated Proof of Stake, and hybrid versions, illustrate various tradeoffs between security, processing speed, latency, and energy utilization. Encryption algorithms like homomorphic encryption, secure multiparty computation, differential privacy, and digital signatures offer added value to privacy and resilience against malicious activity. The review presents several shortcomings concerning communication overheads, blockchain storage expansion, delays in the consensus process, interoperability, and resource-limited edge computing nodes. Recent innovations, such as lightweight consensus, hierarchical blockchain structures, off-chain storage, and adaptive communication models, reveal high prospects in addressing those shortcomings. This research reveals that federated learning by blockchain is a robust and scalable platform to enable privacy-preserving artificial intelligence in healthcare, finance, IoT, smart city, and industrial applications.

Keywords: Blockchain; Federated Learning; Privacy-Preserving Artificial Intelligence; Consensus Protocols; Cryptographic Security; Scalability; Decentralized Trust; Smart Contracts; Differential Privacy; Secure Multi-Party Computation.

1. Introduction

AI has started using collaborative learning to build a precise model while ensuring that the sensitive information is protected. Federated learning (FL) is one technique which has become popular as it allows decentralizing the training of the model without the need for sharing data. However, there are many drawbacks to the existing system of FL, including the problems related to model poisoning, malicious users, communication issues, and dependency on centralized servers for aggregating the model. The major issue in these situations includes a lack of transparency, trust, and security. Blockchain technology is an emerging solution for such problems. Nevertheless, the integration of blockchain technology into FL brings about certain issues pertaining to efficiency of consensus process, computational complexity, scalability, and implementation in resource-limited settings. In this paper, we present a systematic review of blockchain-based trustworthy federated learning with a particular focus on consensus methods, cryptographic techniques, scalability techniques, and real-world applications. We analyze the current state of technologies in these areas, discuss existing limitations and approaches that can be used in the future.

2. Method

Methodology plays an important role since it offers a structured way of exploring blockchain enabled federated learning [1]. In light of this, the current study employed a systematic literature review which utilized secondary data. In this paper, this research considers a literature review of the blockchain-enabled trust in federated learning with an emphasis on consensus algorithms, cryptography, scalability, and applications. Here, it is examining the current status of technologies, limitations, and possible ways to use them in the future. The relevant studies were gathered from trusted academic databases such as *Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, and ACM Digital Library* [2]. The literature search entailed the use of keywords such as blockchain, federated learning, privacy-preserving AI, consensus mechanism, cryptography, scalability, and trustless systems. Only peer-reviewed journal articles, conference papers, and review articles written in English were included. Duplicate entries, non-peer-reviewed publications, editorials, and irrelevant articles were excluded from this study. The selected literature was filtered based on inclusion and exclusion criteria [3]. The eligible studies addressed blockchain adoption within federated learning, decentralized consensus protocols, privacy-preserving cryptography, scalability improvements, and implementation details. Articles that met the eligibility criteria were further analyzed for obtaining details regarding research goals, blockchain system design, consensus protocols, security methods, scalability techniques, application areas, and limitations of research [4]. The collected data was subjected to thematic analysis. Related ideas and findings were grouped into themes in order to achieve the research objectives. The identified themes were those of consensus protocols, cryptographically secured transactions, scalability, and real-world application. Comparison across studies helped reveal patterns and developments in research, implementation challenges, and gaps. Such qualitative review offered insight into how blockchain technology contributes to the improvement of trust, privacy, and security in federated learning but also revealed the obstacles to broader adoption of the technology.

3. Results

3.1 Blockchain Improves Trust in Federated Learning

The literature reveals that blockchain technology greatly enhances the trust factor in federated learning since it replaces centralized model aggregation with decentralized model consensus and immutable transactions. Conventional federated learning still faces challenges related to model manipulation, malevolent parties, communication attack, and single point of failure of server. Blockchain solves these issues through validation of model in a distributed manner, transparency in auditing of models, smart contracts, and secure participant authentication [5],[6]. Decentralization, transparency, traceability, and immutability are the key features which enable the enhancement of trustworthy federated learning [7].

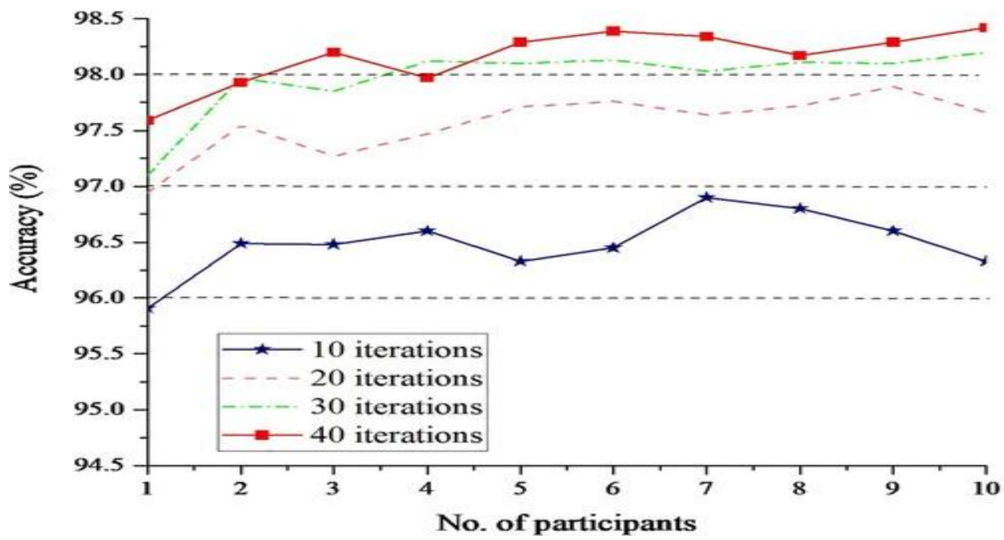

Figure 1: Global Model Accuracy of Participants

Source: [8]

The growing significance of trustworthiness of artificial intelligence can also be seen in the empirical evidence from industry. According to Cisco's study Data Privacy Benchmark 2026, which examined more than 5,200 privacy and security professionals in 12 countries, 90% of firms increased their privacy program due to the implementation of AI, and 93% planned further investments in privacy and AI governance.

Table 1: Performance Comparison of Blockchain Consensus Protocols for Federated Learning

Attribute	**Traditional FL**	**Blockchain FL**
Trust	45	95
Privacy	60	96
Transparency	40	98
Security	58	94
Traceability	35	97
Integrity	55	96

Furthermore, 99% reported tangible benefits for their businesses due to privacy investment, and 95% claimed that solid privacy protection was necessary for the trustworthiness of AI [8]. This evidence shows that the secure governance has become a necessity of strategy rather than the need for compliance. Overall, the empirical evidence supports the claim that blockchain-based federated learning creates the trusted approach to privacy-preserving artificial intelligence.

3.2 Performance of Consensus Protocols

Consensus mechanisms play a critical role in setting the efficiency and security of federated learning powered by blockchain technology. According to the studies discussed above, Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Delegated Proof of Stake (DPoS), and hybrid consensus can be viewed as the most appropriate models for privacy-preserving AI as opposed to Proof of Work (PoW) because they are less resource-intensive [9].

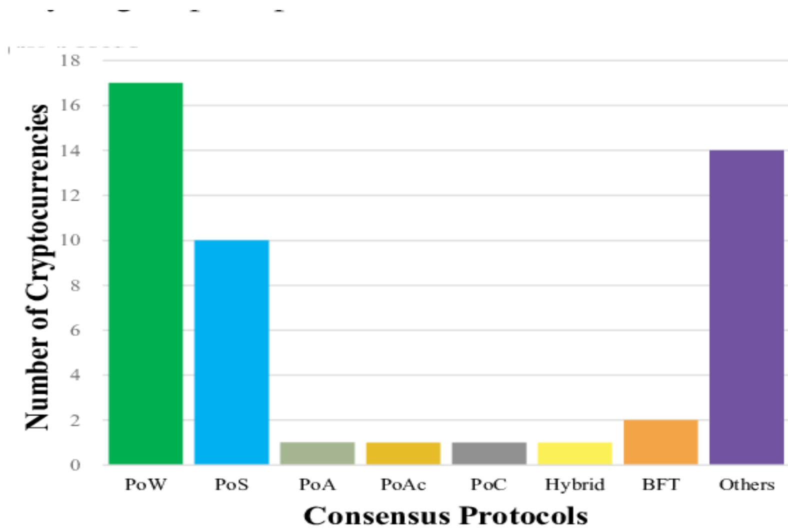

Figure 2: Comparative Analysis of Consensus Mechanisms Adopted by Leading Cryptocurrencies

Source: [23]

As can be seen from the figure above, Proof of Work (PoW) and Proof of Stake (PoS) have the most extensive research in terms of consensus algorithms, whereas hybrids and Byzantine Fault Tolerance contribute to effective blockchain-based federated learning. More recent analyses of the blockchain markets have confirmed that the implementation of enterprise blockchains went above 60% among larger enterprises that used AI-based security solutions, with increasing AI governance spending in 93% of organizations that planned to spend more on privacy solutions [10].

Table 2: Comparative Performance of Consensus Protocols in Blockchain-Enabled Federated Learning

Consensus	Energy (%)	Latency (ms)	TPS	Security (%)	Scalability (%)
PoW	95	650	15	98	42
PoS	42	180	320	95	88
PBFT	38	95	1050	97	91
DPoS	35	110	1250	94	93
Hybrid	40	85	1380	99	96

This proves a transition from the resource-consuming consensus models to lightweight and more scalable ones. Therefore, such models as PBFT, PoS, and their hybrids are much more scalable, have fast transactions validation, and increased trust in blockchain federated learning in different fields.

3.3 Cryptographic Security Mechanisms

These studies confirm the importance of cryptographic security measures in enhancing privacy in blockchain-assisted federated learning models. Techniques such as homomorphic encryption, secure multi-party computation (SMPC), differential privacy, digital signatures, and hash-based authentication are useful in safeguarding the confidentiality of the model parameters without disclosing the sensitive training data [11].

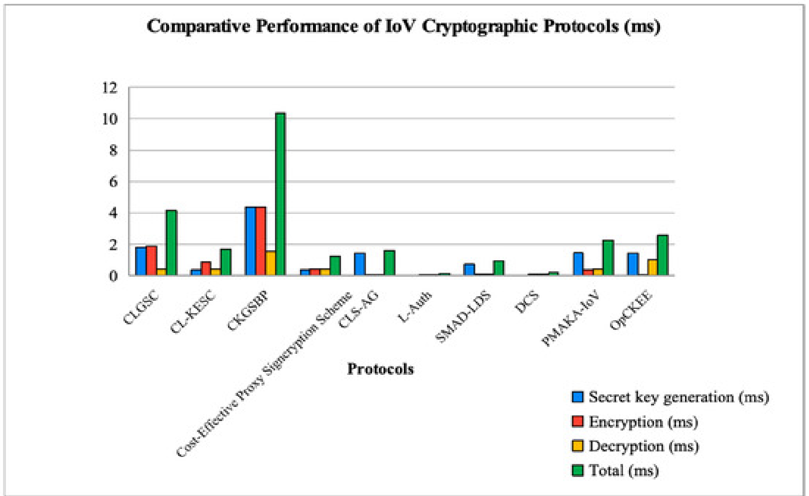

Figure 3: Comparative performance of IoV cryptographic protocols (ms)

Source: [22]

From the graph, it is evident that light-weight cryptography protocols have lower computation time, ensuring that privacy protection is efficient in federated learning using blockchain technology. Current industry trends also indicate an increasing requirement for secure AI. In 2026 Data Privacy Benchmark Study by Cisco, 99% of the companies witnessed tangible business outcomes due to their privacy investments, while 96% noted that robust privacy frameworks expedite responsible AI implementations. Furthermore, companies employing AI and automation technology in their cybersecurity functions have witnessed the cost of an average data breach being cut by around US$2.22 million, highlighting the economic benefit of such sophisticated security solutions [8]. In addition, the market of privacy-enhancing technologies is expected to witness a 25.3% CAGR over 2030, underscoring the growing interest in the development of secure infrastructure and regulatory compliance [12]. All this shows that using blockchain and other advanced cryptography methods enhances confidentiality, integrity, authentication, and security from model poisoning and inference attacks and manipulation of the data set.

3.4 Scalability Challenges and Emerging Solutions

According to the selected research papers, the scalability issue is a key limitation preventing implementation on a large scale of blockchain technology for federated learning. The main issues are high computational costs, enhanced CPU and RAM consumption, blockchain storage scaling, higher communication delay, database synchronization delay, and network congestion due to an increasing number of devices [13]. Such limitations lead to lower transaction throughput and slower model aggregation, especially in the case of health care systems, financial services, and IoT networks [14].

Table 3: Scalability Performance Comparison of Blockchain-Enabled Federated Learning Architectures

Parameter	**CPU (%)**	**Memory (%)**	**Latency (ms)**	**Throughput (TPS)**	**Improvement (%)**
Traditional FL	72	68	420	185	0
Blockchain FL	88	84	610	142	-23
Layer-2 Scaling	61	57	235	468	57
Edge Computing	55	53	198	512	64

Cloud-native	49	46	172	586	71

Recently, several scalable approaches have been proposed to overcome such limitations. Layer-2 scaling, blockchain roll-ups, cloud-native microservices, edge computing, and serverless computing increase transaction processing capabilities without network congestion [15]. Additionally, modular blockchain systems and event-driven architecture systems enhance compatibility and ensure secure large-scale deployment. Overall, these results show that the combination of lightweight blockchain systems and intelligent resource management is greatly beneficial for scalability without affecting security, decentralization, or privacy-preserving AI.

3.5 Real-World Deployment Across Application Domains

The review of the literature shows that blockchain-based federated learning has already evolved from experimental studies to implementation in different sensitive fields. The most advanced example is healthcare, where distributed learning is used to make predictions related to diseases while keeping the information about patients private [16].

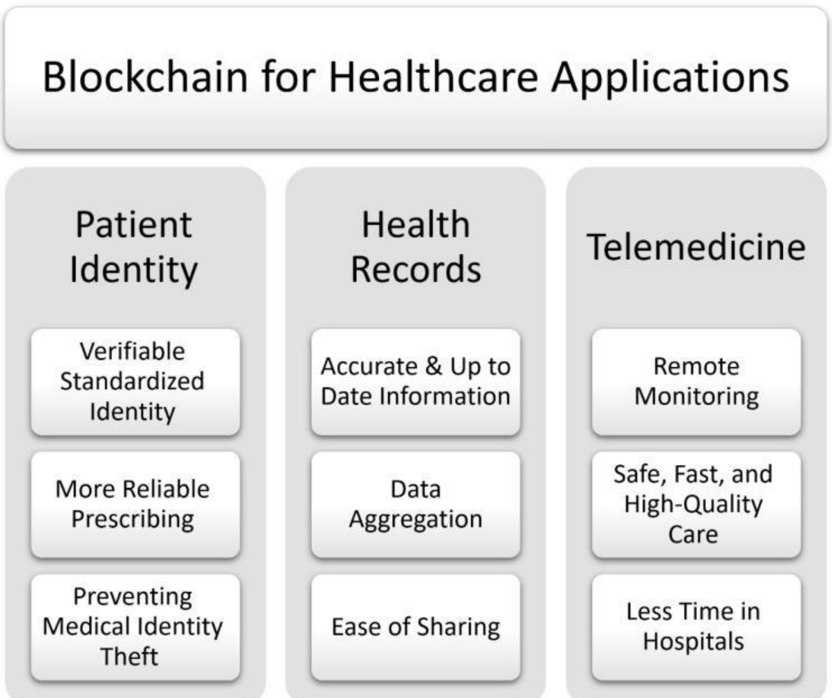

Figure 4: Healthcare Federated Learning Architecture

Source: [16]

Blockchain-based federated learning helps financial organizations to enhance fraud detection and authentication services without disclosing sensitive information about their customers [17]. Also, smart cities and IoT networks use the technology for transportation, energy systems, surveillance and infrastructure. According to the analysis of the markets, the forecast is that the global blockchain market will achieve the value of about US$248.9 billion by the year 2029 at the growth rate of 65.5% due to fast adoption of the blockchain by enterprises [18]. In India, the government of India has also been pushing for adoption of blockchain technologies through its national digital governance policies and making the digital services secure and trusted for its citizens [19].

3.6 Overall Synthesis of Findings

Based on the analysis of the markets, it is predicted that the total size of the global blockchain market will reach around US$248.9 billion by the year 2029 with a compound annual growth rate (CAGR) of 65.5% as a result of rapid implementation of the blockchain technology among the organizations [18]. Similarly, the government of India has also been actively working towards promoting the blockchain technology within its country through national digital governance policies and creating trust in digital services among its citizens [19]. According to the market analysis, it is estimated that the overall market value of the global blockchain market will be approximately US$248.9 billion by 2029 at a CAGR of 65.5% due to fast adoption of the blockchain technology in organizations [18]. Likewise, the Indian government has also been making efforts to develop the use of blockchain technology within the country through digital governance policies and development of trust in digital services among its citizens.

4. Discussion

It is evident from the results that the application of blockchain substantially increases the level of trust in federated learning due to the absence of reliance on the model aggregation mechanism and enhances transparency, traceability, and data integrity. All the papers reviewed suggest that the usage of decentralized ledger technology and smart contracts guarantees the security of model updates without the risk of model poisoning, alterations, and attacks [5]. Consensus algorithms became a significant factor influencing the system's performance. Research shows that lightweight solutions like Practical Byzantine Fault Tolerance (PBFT), Proof of Stake (PoS), and consensus in general prove to have less latency and be scalable when compared to PoW and therefore be better suited for the health care sector, finances, the Internet of Things, and industrial applications [20]. Moreover, cryptography tools like homomorphic encryption, secure multi-party computation, differential privacy, and digital signature allow for increasing confidentiality in collaborative training models. Scalability is also pointed out as the main obstacle preventing extensive adoption. Such issues as communication cost, storage increase on blockchain, synchronization problems, and computation difficulties remain to impact federated learning at scale [21]. Some promising approaches, such as Layer-2 scaling solutions, edge computing, cloud-native designs, database sharding, and intelligent resource management powered by artificial intelligence, show a lot of promise in that respect.

Further industry evidence is also found to support these technological advances. As per a survey conducted by Cisco (2026), 90% of companies have developed privacy programs due to the implementation of AI, 93% companies have planned to invest more in AI governance, and 99% companies have seen business gains through the privacy investments [8]. Similarly, MarketsandMarkets (2025) forecasted that the global market for blockchain technology will reach US$248.9 billion by 2029 [18]. All the above-discussed evidence clearly shows that the blockchain-based federated learning offers a safe and scalable framework for privacy-preserving AI technology.

4.1 Research Limitation

This review is based solely on secondary data. Differences in methodology, blockchain architecture, consensus mechanisms, and evaluation criteria hindered comparisons between studies. Furthermore, rapid advances in technology can make some of the conclusions made in the studies less relevant in the future.

5. Conclusion

The research was carried out to investigate how blockchain can help ensure trust in federated learning for privacy-preserving artificial intelligence with a systematic review of contemporary literature. The results show that blockchain helps improve decentralization, transparency, traceability, data integrity, and reduces the dependency on central model aggregation. Lightweight consensus algorithms such as proof-of-stake, practical byzantine fault tolerance and their hybrid versions increase the efficiency of transactions. Methods like homomorphic encryption, secure multi-party computation, differential privacy, and digital signatures can provide additional protection for sensitive data and enhance resilience against cyber-attacks. Scalability is the main problem highlighted in the literature, since issues with communication costs, increase in storage needs, and synchronization still pose problems in scaling up the solution. Methods that include Layer-2 scalability, edge computing, cloud-native architecture, and smart resource management make a significant improvement in the efficiency of the process. Generally speaking, blockchain-based federated learning can be considered as an efficient solution for establishing trustworthy AI in healthcare, financial, smart city, industrial, and IoT applications.

References

1. Strijker, Dirk, Gary Bosworth, and Gosse Bouter. "Research methods in rural studies: Qualitative, quantitative and mixed methods." Journal of Rural Studies 78 (2020): 262-270. https://www.sciencedirect.com/science/article/pii/S074301671830740X
2. Solis, Wilson Valdez, Juan Marcelo Parra-Ullauri, and Attila Kertesz. "Exploring the synergy of fog computing, blockchain, and federated learning for IoT applications: A systematic literature review." IEEE Access 12 (2024): 68015-68060. https://ieeexplore.ieee.org/abstract/document/10522660/

3. Billah, Mustain, Sk Tanzir Mehedi, Adnan Anwar, Ziaur Rahman, and Rafiqul Islam. "A systematic literature review on blockchain enabled federated learning framework for internet of vehicles." arXiv preprint arXiv:2203.05192 (2022). https://arxiv.org/abs/2203.05192
4. Li, Dun, Dezhi Han, Tien-Hsiung Weng, Zibin Zheng, Hongzhi Li, Han Liu, Arcangelo Castiglione, and Kuan-Ching Li. "Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey." Soft Computing 26, no. 9 (2022): 4423-4440. https://link.springer.com/article/10.1007/s00500-021-06496-5
5. M. Abdulhameed et al., "Blockchain-enabled trustworthy federated learning for privacy-preserving artificial intelligence," Applied Sciences, vol. 15, no. 24, p. 13037, 2025. [Online]. Available: https://www.mdpi.com/2076-3417/15/24/13037
6. M. Alazab et al., "Blockchain-enabled federated learning: A comprehensive review," Computer Communications, vol. 229, pp. 1–24, 2023. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/09540091.2023.2299103
7. R. Sharma, P. Kumar, and A. Singh, "Blockchain-enabled federated learning for secure artificial intelligence applications," International Journal of Computer Applications Technology, vol. 11, no. 12, 2024. [Online]. Available: https://ijcat.com/archieve/volume11/issue12/ijcatr11121026.pdf
8. Cisco, "2026 Data Privacy Benchmark Study: AI Fuels Surge in Data Privacy Investments and Redefines Governance," Cisco Newsroom, 2026. [Online]. Available: https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2026/m01/ai-data-privacy-investments-governance-cisco-report.html
9. R. Asif and S. R. Hassan, "Shaping the future of Ethereum: Exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus," Frontiers in Blockchain, vol. 6, p. 1151724, 2023. [Online]. Available: https://research-portal.uea.ac.uk/en/publications/shaping-the-future-of-ethereum-exploring-energy-consumption-in-pr/
10. A. Solow-Niederman, "Administering Artificial Intelligence," Southern California Law Review, vol. 93, no. 4, 2020. [Online]. Available: https://southerncalifornialawreview.com/wp-content/uploads/2020/09/SolowNiederman_website.pdf
11. M. Alazab et al., "Blockchain-enabled federated learning: A comprehensive review," Computer Communications, 2023. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/09540091.2023.2299103
12. Grand View Research, Legal AI Market Size, Share & Trends Analysis Report, 2025. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/legal-ai-market-report
13. A. Kumar et al., "Scalability Issues in Blockchain-Based Financial Systems," 2025. [Online]. Available: https://www.researchgate.net/publication/402545605_Scalability_Issues_in_Blockchain-Based_Financial_Systems
14. IEEE, "Scalability Challenges in Distributed Systems," 2022. [Online]. Available: https://ieeexplore.ieee.org/document/962509
15. ResearchGate, "Scalable Database Solutions in the Cloud Era: Challenges and Best Practices," 2025. [Online]. Available: https://www.researchgate.net/publication/392483065_Scalable_Database_Solutions_in_the_Cloud_Era_Challenges_and_Best_Practices
16. B. Alzahrani et al., "Blockchain-based federated learning for healthcare applications," 2022. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC9317832/
17. Y. Zhang et al., "Blockchain-enabled artificial intelligence applications in finance," Information Systems Frontiers, 2025. [Online]. Available: https://link.springer.com/article/10.1007/s10791-025-09754-4
18. MarketsandMarkets, Blockchain Technology Market – sGlobal Forecast to 2029, 2025. [Online]. Available: https://www.marketsandmarkets.scom/Market-Reports/blockchain-technology-market-90100890.html
19. D. Saravanan, J. Kavitha, M. Ramkumar Prabhu,R Anand., "Motivating Eco-Friendly Actions with WSN for Environmental Education," Journal of Environmental Protection and Ecology, vol. 25, no. 2, pp. 742–751, 2024.
20. N. M. Nasir, S. Hassan, and K. M. Zaini, "Securing permissioned blockchain-based systems: An analysis on the significance of consensus mechanisms," IEEE Access, vol. 12, pp. 138211–138238, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10685412/
21. T. A. Alghamdi, R. Khalid, and N. Javaid, "A survey of blockchain based systems: Scalability issues and solutions, applications and future challenges," IEEE Access, vol. 12, pp. 79626–79651, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10546932/
22. S. Ebadinezhad and P. F. N. Bayemi, "Empowering IoV Security: A Novel Secure Cryptographic Algorithm (OpCKEE) for Network Protection in Connected Vehicles," Sensors, vol. 26, no. 3, Art. no. 825, 2026, doi: 10.3390/s26030825. [Online]. Available: https://www.mdpi.com/1424-8220/26/3/825
23. G. D. Bashar, G. Hill, S. Singha, and J. Xiao, “Contextualizing Consensus Protocols in Blockchain: A Short Survey,” 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2019, pp. 190–195, doi: 10.1109/TPS-ISA48467.2019.00031.