ISSN-3139-6593 (Online)

Journal of Interdisciplinary Science &Technology

Integration of Artificial Intelligence and Blockchain: A Systematic Review of Applications, Architectures, Security, and Open Challenges

Ekansh Tayade[1], Pranav Pagare[2], Darshan Aher[3], Smit Chaudhari[4]

[1,2,3] Computer Engineering, Sandip Institute of Technology and Research Center Nashik (SITRC), Maharashtra, India;

[4] Dharmsinh Desai University, Nadiad, Gujarat (DDU), India

ekanshshweta06@gmail.com, pranavnpagare@gmail.com, aherdarshan2803@gmail.com, smitchaudhari2601@gmail.com

Corresponding author- *Ekansh Tayade*

DOI: ***10.5281/zenodo.22903650***

Abstract: The integration of artificial intelligence (AI) and blockchain combines adaptive computation with decentralized trust, cryptographic integrity, programmable transactions, and auditable data exchange. This systematic review synthesizes research on integration architectures, applications, reciprocal benefits, security, privacy, scalability, interoperability, and open challenges. Four recurring integration patterns are examined: AI enhancing blockchain operations, blockchain supporting AI systems, bidirectional AI–blockchain architectures, and decentralized or federated intelligent systems. Applications are considered across healthcare, finance, supply chains, Internet of Things, cybersecurity, energy, smart cities, and education. The review finds that AI can strengthen anomaly detection, fraud analytics, smart-contract analysis, prediction, and network optimization, while blockchain can strengthen data provenance, identity, model traceability, access control, and collaborative learning. However, combined architectures introduce additional trust boundaries involving models, oracles, smart contracts, data pipelines, and cross-system interfaces. Latency, storage growth, interoperability, privacy leakage, model manipulation, poisoning, and governance remain important barriers. The review therefore argues for selective integration: intensive AI computation and sensitive data should generally remain off-chain or in controlled edge/cloud environments, while blockchain should anchor identities, commitments, permissions, provenance, and auditable events. Future research should prioritize verifiable AI outputs, privacy-preserving decentralized learning, trustworthy oracles, cross-chain interoperability, standardized benchmarks, and governance-aware architectures.

Keywords: Artificial Intelligence; Blockchain; Machine Learning; Smart Contracts; Decentralized AI; Federated Learning; Privacy; Security; Data Provenance; Distributed Ledger Technology

I INTRODUCTION

Artificial intelligence and blockchain solve different but complementary problems. AI learns patterns from data and supports prediction, classification, optimization, and decision-making. Blockchain provides a distributed ledger in which records are cryptographically linked and collectively validated. NIST describes blockchain as a tamper-evident and tamper-resistant distributed ledger maintained through distributed copies and validation rules [1].

AI systems depend on data, models, and computational infrastructure, while blockchain systems generate transactional and network data that can be analyzed by AI. Blockchain can record selected data events, model versions, identities, permissions, and commitments; AI can provide anomaly detection, fraud analytics, predictive monitoring, optimization, and intelligent automation. Recent literature shows increasing attention to integrated ecosystems. A 2025 systematic review of blockchain, AI, and cloud integration analyzed 108 peer-reviewed studies from 2012–2025 and identified interoperability, latency, security trade-offs, and resource allocation as recurring challenges [2]. A 2025 systematic review of blockchain-enabled AI systems examined architectural patterns, governance, applications, and recurring privacy, scalability, interoperability, and regulatory issues [3]. A 2024 review focused on AI-enhanced blockchain and examined machine learning, deep learning, natural-language processing, and reinforcement learning for security, consensus, smart contracts, privacy, scalability, and interoperability [4].

This review takes a broader cross-domain perspective, examining how AI improves blockchain, how blockchain improves AI, how the technologies are architected together, and which security and governance problems emerge at their interface.

II REVIEW METHODOLOGY

The review uses a structured thematic synthesis. Search concepts covered artificial intelligence, machine learning, deep learning, reinforcement learning, natural language processing, blockchain, distributed ledger technology, smart contracts, decentralized AI, federated learning, privacy, security, interoperability, and trustworthy AI. Priority was given to peer-reviewed systematic reviews, surveys, application studies, foundational works, and authoritative standards. Recent literature from 2024–2026 was emphasized.

The evidence base is heterogeneous. Existing reviews use different databases, time windows, inclusion criteria, and research questions. Therefore, publication counts from different studies are not combined into a single statistical corpus. Singh et al. report 108 studies in a blockchain–AI–cloud review [2], while the 2025 decentralized-AI review began with 2,702 records and screened them to a final included set [3]. A 2025 financial-sector SLR examined 134 peer-reviewed publications using PRISMA [5]. These figures describe the source studies rather than a new pooled dataset (Figure 1, 2, 3).

RQ	Question
RQ1	What architectures are used to integrate AI and blockchain?
RQ2	Which application domains use the integration?
RQ3	How does AI improve blockchain systems?
RQ4	How does blockchain improve AI systems?
RQ5	What security, privacy, scalability, and interoperability challenges emerge?
RQ6	What research directions could improve trustworthy deployment?

Table 1. Research questions guiding the review

III FOUNDATIONS OF AI–BLOCKCHAIN INTEGRATION

A. Artificial Intelligence Layer

AI provides learning and inference capabilities. Machine-learning models can classify transactions, detect anomalies, predict demand, estimate risk, optimize resources, and support decisions. In integrated systems, intensive training and inference are commonly performed off-chain or at edge/cloud nodes, while selected evidence or outputs can be anchored on a ledger.

B. Blockchain Layer

Blockchain provides shared state, transaction ordering, consensus, cryptographic identity mechanisms, and smart-contract execution. Its strongest role appears where multiple parties must coordinate while reducing dependence on a single system of record. Blockchain does not itself establish the truth of external information or the correctness of an AI model.

C. Complementarity Principle

The combined architecture can be viewed as a trust–intelligence loop: blockchain records or verifies selected events, AI analyzes data and produces predictions, and approved results can inform smart-contract actions. A blockchain can preserve an incorrect AI output just as reliably as a correct one if upstream data, models, or oracles are compromised.

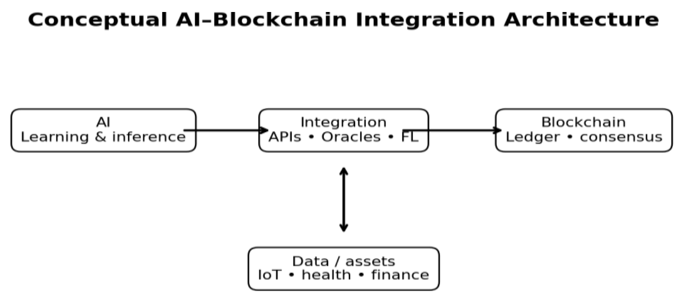

Figure 1. Conceptual architecture for AI–blockchain integration.

IV TAXONOMY OF INTEGRATION ARCHITECTURES

Pattern	Typical Role	Examples
AI → Blockchain	AI enhances ledger operations	Fraud, anomaly detection, network analytic
Blockchain → AI	Ledger supports AI trust	Provenance, identity, model/version record
Bidirectional	Both systems exchange state	Intelligent contracts, automated governance
Decentralized / federate	ledger coordinates distributed	Federated learning, incentives, verification

Table 2. Taxonomy of AI–blockchain integration patterns.

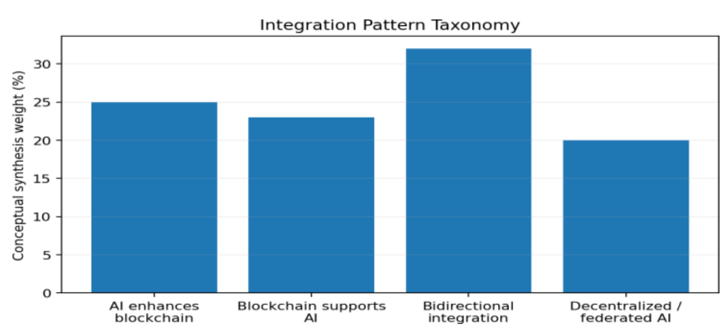

Figure 2. Conceptual integration-pattern weights used for synthesis; these are not bibliometric prevalence estimates.

V AI FOR BLOCKCHAIN

AI can analyze blockchain-generated data and improve selected blockchain functions. The literature emphasizes anomaly detection, fraud detection, smart-contract analysis, consensus or network optimization, and privacy/security monitoring [4,6]. AI is particularly useful where patterns are difficult to express through deterministic rules.

A. Fraud and Anomaly Detection

Transaction histories provide structured behavioral information. Models can combine transaction frequency, timing, graph relationships, addresses, contract interactions, and historical behavior to identify suspicious activity. These systems should be evaluated with domain-specific false-positive and false-negative measures.

B. Smart-Contract Security

AI can assist vulnerability classification, code analysis, test generation, and behavioral monitoring. Because deployed smart contracts may be difficult to modify, pre-deployment analysis and controlled release gates are especially important [7].

C. Consensus and Network Optimization

Learning methods can support workload prediction, resource allocation, node behavior analysis, and adaptive network management. Consensus is security critical, so learned components should not replace deterministic safety assumptions without rigorous validation.

VI BLOCKCHAIN FOR AI

Blockchain can strengthen AI systems through provenance, identity, access control, model-version traceability, and auditable records. This is particularly relevant when multiple organizations collaborate but cannot or should not transfer all raw data to a central repository.

A. Data Provenance and Integrity

A ledger can record hashes, timestamps, dataset versions, ownership claims, consent states, and access events. Large or sensitive datasets generally remain off-chain, while cryptographic commitments or metadata are anchored to the ledger.

B. Federated and Decentralized Learning

Federated learning keeps training data at participating nodes and exchanges model updates rather than raw records. Blockchain can coordinate participant identity, update registration, incentive mechanisms, and audit trails. However, blockchain does not by itself prevent poisoned model updates or privacy leakage [8,9].

C. Model Accountability

A ledger can record model versions, training events, approvals, evaluation results, deployment transitions, and access events. NIST AI RMF provides a complementary framework for managing AI risks through governance, measurement, and management [10].

VII APPLICATION DOMAINS

Domain	AI contribution	Blockchain contribution	Recurring challenge
Healthcare	Diagnosis, prediction, analytics	Consent, provenance, secure exchange	Privacy, interoperability, regulation
Finance	Fraud, risk scoring, forecasting	Integrity, identity, auditability	Latency, compliance, explainability
Supply chain	Demand/quality prediction, anomaly	provenance	Oracle reliability, interoperability
IoT	Anomaly detection, predictive main	enhance identity and event integrity	Resource limits, throughput
Cybersecurity	Threat and behavior analytics	Tamper-evident records and identity	Adversarial ML, key management
Energy	Forecasting and optimization	Peer-to-peer coordination	Scalability, real-time requirements
Smart cities	Traffic/resource analytics	Identity and decentralized coordination	Governance and ownership
Education	Personalization and analytics	Credentials and provenance	Privacy and adoption

Table 3. Application-domain synthesis.

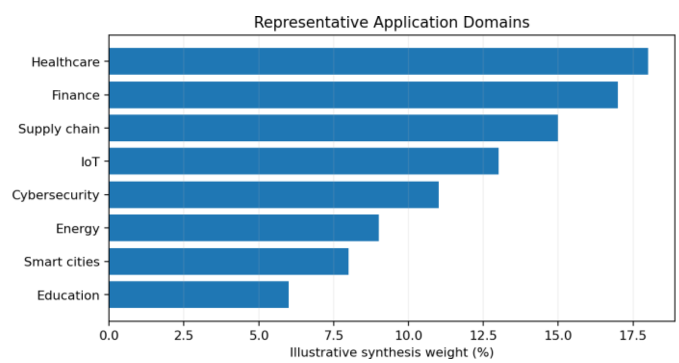

Figure 3. Representative application domains; values are illustrative synthesis weights, not publication counts.

VIII SECURITY AND PRIVACY

AI–blockchain integration creates a composite attack surface spanning data, models, consensus, smart contracts, interfaces, oracles, identities, and application logic. A 2025 security review analyzed more than 100 peer-reviewed studies and highlighted AI applications for consensus, anomaly detection, smart-contract vulnerability identification, and privacy, while also identifying ethical, regulatory, and standardization challenges [6].

Threat	Affected layer	Potential impact	Mitigation direction
Data poisoning	Training pipeline	Biased/malicious model	Provenance, robust aggregation, validation
Model manipulation	Model/update layer	Incorrect decisions	Signed artifacts, evaluation gates, monitoring
Smart-contract flaws	On-chain logic	Unauthorized execution	Testing, formal analysis, audits
Oracle attacks	Off-chain interface	Incorrect on-chain state	Multiple sources, attestation, anomaly check
Privacy leakage	Data/model updates	Sensitive exposure	Access control, secure aggregation, privacy
Identity/Sybil abuse	Participation layer	Manipulated voting/learning	Strong identity and permissions

***Table 4. Security and privacy threat taxonomy*.**

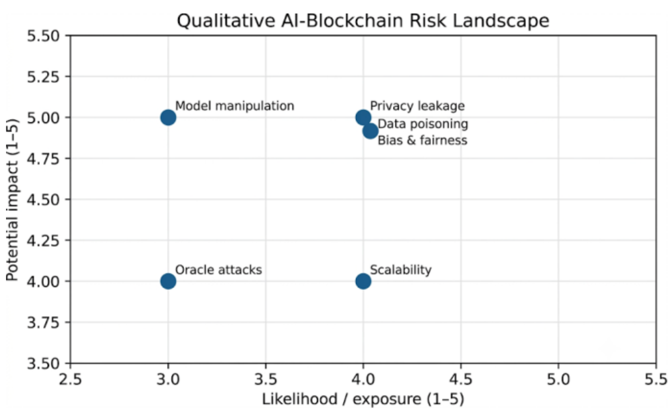

***Figure 4. Qualitative risk landscape; scores organize recurring concerns and are not incident probabilities*.**

IX PRIVACY-PRESERVING INTEGRATION

Privacy is simultaneously a motivation and a constraint. Blockchain transparency can conflict with confidentiality because ledger records may persist. Privacy-preserving designs therefore avoid placing raw sensitive data directly on-chain. Existing work identifies authorization, access control, data protection, network security, and scalability as major dimensions of privacy-preserving AI–blockchain integration [11].

Useful patterns include encrypted off-chain storage, hashes or commitments on-chain, permissioned ledgers, federated learning, secure aggregation, selective disclosure, and privacy-preserving computation.

X PERFORMANCE, SCALABILITY, AND INTEROPERABILITY

Dimension	AI requirement	Blockchain constraint	Architectural response
Latency	Fast inference	Consensus/confirmation delay	Off-chain or edge inference
Storage	Large datasets/models	Ledger growth	Hashes/metadata on-chain
Compute	GPU/accelerator workloads	Node resource limits	Cloud/edge AI
Interoperability	Multiple frameworks	Cross-chain differences	Standard APIs/schemas
Energy	Training/inference cost	Consensus overhead	Efficient models/consensus

Table 5. Performance and interoperability considerations.

AI and blockchain have different resource profiles. Model training may require accelerators and large datasets, while blockchain consensus requires distributed communication and validation. Consequently, layered on-chain/off-chain designs are often more practical than storing all AI computation or artifacts on-chain. Recent reviews similarly identify scalability, latency, computational overhead, and interoperability as persistent barriers [2,3,12].

XI COMPARATIVE SYNTHESIS

Direction	Primary value	Representative applications	Main challenge
AI+ blockchain	Adaptive detection/optimization	Fraud, anomaly, network analytics	Model reliability
Blockchain for AI	Provenance/accountability	Data sharing, model lifecycle	Privacy/ledger overhead
AI + smart contracts	Decision-to-action automation	Finance, supply chains, IoT	Oracle/contract risks
Blockchain + federated AI	Decentralized collaboration	Healthcare, IoT	Poisoning/governance

Table 6. Comparative synthesis of major integration directions.

XII OPEN RESEARCH CHALLENGES

A. Verifiable AI outputs. Blockchain can prove that a record or commitment was preserved, but it cannot by itself prove that a prediction is correct. Future systems need stronger mechanisms for model provenance, reproducible inference, attestations, and independent verification.

B. Trustworthy oracles. Smart contracts often depend on information outside the ledger. The oracle becomes a critical trust boundary. Multi-source validation, provenance, anomaly detection, and dispute mechanisms are promising directions.

C. Cross-chain interoperability. AI services, data stores, permissioned ledgers, public chains, and edge systems often use incompatible interfaces. Standardized identity, model metadata, provenance, and event schemas could reduce integration cost.

D. Privacy versus auditability. Permanent ledgers can conflict with data minimization and confidentiality. Selective disclosure, zero-knowledge methods, confidential computing, and lifecycle-aware governance deserve further investigation.

E. Robust decentralized learning. Distributed learning can be attacked through malicious updates or participant manipulation. Blockchain can coordinate participants but does not automatically establish that updates are trustworthy.

F. Standardized evaluation. Current studies use different datasets, chains, models, and metrics. A common benchmark should jointly report AI quality, robustness, transaction latency, throughput, storage growth, privacy leakage, resource use, and cost.

XIII EVALUATION FRAMEWORK FOR FUTURE STUDIES

Dimension	Example metrics	Purpose
AI quality	Accuracy, F1, AUROC, calibration	Decision quality
Blockchain performance	TPS, confirmation latency, storage growth	Ledger feasibility
Security	Attack success rate, vulnerability coverage	Resilience
Privacy	Leakage/disclosure exposure	Confidentiality
Interoperability	Integration time, portability	Compatibility
Governance	Audit completeness, approval coverage	Accountability
Economics	Compute, storage, transaction cost	Sustainability

Table 7. Multidimensional evaluation framework.

XIV FUTURE RESEARCH DIRECTIONS

Direction	Expected contribution
Verifiable AI + blockchain	Independent checking of model versions and selected outputs
Privacy-preserving decentralized AI	Collaborative learning without centralizing sensitive data
AI-driven smart-contract security	Automated vulnerability detection and monitoring
Trustworthy oracle networks	More reliable external information
Cross-chain AI services	Portable models, identity, provenance, and events
Edge AI + blockchain	Resource-aware decentralized intelligence
Standardized benchmarks	Comparable quality, security, performance, and cost
Governance-aware architectures	Explicit accountability, permissions, and dispute handling

Table 8. Strategic Research Directions and Expected Contributions in AI–Blockchain Integration

XV DISCUSSION

The literature supports a reciprocal interpretation of AI–blockchain integration. AI contributes adaptive intelligence to blockchain systems, while blockchain contributes decentralized coordination, provenance, and auditability to AI systems. The strongest applications are those in which a concrete trust problem and a concrete intelligence problem are addressed together.

The combination should not be treated as beneficial by default. Blockchain introduces consensus, storage, latency, and governance overhead; AI introduces model uncertainty, data dependence, adversarial vulnerabilities, and explainability concerns. When combined, these limitations interact and create additional interface risks. Recent reviews consistently identify interoperability, scalability, privacy, latency, and security as persistent challenges [2–6].

A practical design principle emerging from the review is selective integration. Not every AI computation needs decentralization, and not every AI artifact needs to be placed on a blockchain. Intensive computation and sensitive data can remain off-chain, while blockchain can anchor identity, permissions, commitments, provenance, and auditable events.

XVI CONCLUSION

This systematic review examined the integration of artificial intelligence and blockchain across architectures, applications, security, privacy, performance, and future research. Four major patterns were identified: AI-enhanced blockchain, blockchain-supported AI, bidirectional integration, and decentralized/federated AI. The literature demonstrates potential value across healthcare, finance, supply chains, IoT, cybersecurity, energy, smart cities, and education.

At the same time, the integration introduces important technical and governance barriers, including smart-contract vulnerabilities, oracle dependence, model manipulation, data poisoning, privacy leakage, scalability, latency, and interoperability. Future progress requires evaluation frameworks that assess AI quality and blockchain performance together. Verifiable AI, privacy-preserving decentralized learning, trustworthy oracles, interoperable protocols, and governance-aware architectures are promising directions.

XVII REFERENCE

[1] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," NISTIR 8202, NIST, 2018. DOI: 10.6028/NIST.IR.8202. https://doi.org/10.6028/NIST.IR.8202.

[2] J. Singh, S. Bharany, S. Rani, A. U. Rehman, B. M. Taye, R. Pant, and U. Kaur, "A Systematic Review of Blockchain, AI, and Cloud Integration for Secure Digital Ecosystems," International Journal of Networked and Distributed Computing, vol. 13, art. 28, 2025. DOI: 10.1007/s44227-025-00072-1. https://doi.org/10.1007/s44227-025-00072-1.

[3] Al Jasem, Mohamad S., Trevor De Clark, and Ajay K. Shrestha. "Toward Decentralized Intelligence: A Systematic Literature Review of Blockchain-Enabled AI Systems." *Information 16*, no. 9 (2025): 765. https://doi.org/10.3390/info16090765.
.

[4] Ressi, Dalila, Riccardo Romanello, Carla Piazza, and Sabina Rossi. "AI-enhanced Blockchain Technology: A Review of Advancements and Opportunities." *Journal of Network and Computer Applications 225*, (2024): 103858. https://doi.org/10.1016/j.jnca.2024.103858.

[5] Khan, Habib U., Muhammad Z. Malik, Shah Nazir, and Farhad Ali. "Artificial Intelligence Driven Insights on Blockchain Risks: A Systematic Review in the Financial Sector." *Concurrency and Computation: Practice and Experience 37*, no. 27-28 (2025): e70459. Accessed September 19, 2026. https://doi.org/10.1002/cpe.70459.

[6] Zebari, Gheyath M., and Nasser A. Musalhi. "A Comprehensive Review of Integrating AI and Blockchain Security: Innovations, Challenges, and Future Directions." *Security and Privacy 8*, no. 5 (2025): e70094. Accessed September 19, 2026. https://doi.org/10.1002/spy2.70094.

[7] "Security Architectural Approaches and Risk Assessment Methods for Blockchain Systems: A Review and Future Directions," Distributed Ledger Technologies: Research and Practice, vol. 5, no. 1, art. 7, 2025. DOI: 10.1145/3721140. https://www.uspto.gov/web/offices/pac/mpep/s2162.html.

[8] McMahan B, Moore E, Ramage D, Hampson S, Arcas BA. Communication-efficient learning of deep networks from decentralized data. In: Singh A, Zhu J, editors. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics; 2017 Apr 20–22; Fort Lauderdale, FL. PMLR; 2017. p. 1273–82. (Proceedings of Machine Learning Research; vol. 54). Available from: https://proceedings.mlr.press/v54/mcmahan17a.html.

[9] Kairouz P, McMahan HB. Advances and open problems in federated learning. *Found Trends Mach Learn*. 2021 Jun;14(1–2):1–210. https://doi.org/10.1561/2200000083

[10] E. Tabassi, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," NIST AI 100-1, 2023. https://doi.org/10.6028/NIST.AI.100

[11] Yuan, Fujiang, Zihao Zuo, Yang Jiang, Wenzhou Shu, Zhen Tian, Chenxi Ye, Junye Yang et al. "AI-Driven Optimization of Blockchain Scalability, Security, and Privacy Protection." *Algorithms 18*, no. 5 (2025): 263. Accessed September 19, 2026. https://doi.org/10.3390/a18050263.

[12] Kaushik D, Gulia P, Gill NS, Yahya M, Shukla PK, Shreyas J. Synergizing blockchain and AI to fortify IoT security: a comprehensive review. *Artif Intell Rev*. 2026;59(2):41. https://doi.org/10.1007/s10462-025-11434-0.

[13] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review. 2008:21260. Available from: https://ssrn.com/abstract=3440802.

[14] Buterin V. Ethereum: A next-generation smart contract and decentralized application platform [Internet]. Ethereum.org; 2014. Available from: https://ethereum.org/en/whitepaper/

[15] Crosby M, Nachiappan, Pattanayak P, Verma S, Kalyanaraman V. Blockchain technology: beyond Bitcoin [Internet]. Appl Innov Rev. 2016 Jun ;(2):6–19. Available from:https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf.

[16] Swan M. Blockchain: blueprint for a new economy [Internet]. Sebastopol (CA): O'Reilly Media; 2015. 152 p. Available from: https://www.oreilly.com/library/view/blockchain-blueprint-for/9781491920480/.

[17] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. IEEE Access. 2016; 4:2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339.

[18] Dorri A, Kanhere SS, Jurdak R. Blockchain in internet of things: challenges and solutions. arXiv [Preprint]. 2016 arXiv:1608.05187 [cs.CR]. Available from: https://arxiv.org/abs/1608.05187.

[19] Leka E, Selimi B, Lamani L. Systematic literature review of blockchain applications: smart contracts. In: 2019 International Conference on Information Technologies (InfoTech); 2019 Sep 19–20; Varna, Bulgaria. Piscataway (NJ): IEEE; 2019. p. 1–3. https://doi.org/10.1109/InfoTech.2019.8860872.

[20] Alharby M, van Moorsel A. Blockchain-based smart contracts: a systematic mapping study. In: Nagamalai D, et al., editors. Computer Science & Information Technology (CS & IT). AIR, CSIT, IPPR, IPDCA - 2017; 2017. p. 125–140. https://doi.org/10.5121/csit.2017.71011.

[21] Szabo N. Formalizing and Securing Relationships on Public Networks. FM [Internet]. 1997 Sep. 1;2(9). Available from: https://firstmonday.org/ojs/index.php/fm/article/view/548.

[22] Kim KG. Deep learning [book review on the Internet]. Health Inform Res. 2016 Oct;22(4):351–354. Available from: https://doi.org/10.4258/hir.2016.22.4.351.

[23] Bishop CM. Pattern recognition and machine learning [Internet]. New York (NY): Springer; 2006. 738 p. Available from: https://link.springer.com/book/9780387310732.

[24] Zhou ZH, Liu S. Machine learning. Beijing / Singapore: Tsinghua University Press and Springer Nature; 2021. https://doi.org/10.1007/978-981-15-1967-3.

[25] Vaswani A, Shazeer N, Parmar N, Uszkoreit J, Jones L, Gomez AN, et al. Attention is all you need. In: Guyon I, Luxburg UV, Bengio S, Wallach H, Fergus R, Vishwanathan S, Garnett R, editors. Advances in Neural Information Processing Systems 30 (NIPS 2017); 2017 Dec 4–9; Long Beach, CA. Red Hook (NY): Curran Associates, Inc.; 2017. p. 5998–6008.

[26] Brown TB, Mann B, Ryder N, Subbiah M, Kaplan J, Dhariwal P, et al. Language models are few-shot learners. arXiv [Preprint]. 2020 arXiv:2005.14165 [cs.CL]. Available from: https://arxiv.org/abs/2005.14165.

[27] Yang Q, Liu Y, Chen T, Tong Y. Federated machine learning: concept and applications. arXiv [Preprint]. 2019 arXiv:1902.04885 [cs.AI]. Available from: https://arxiv.org/abs/1902.04885.

[28] Lyu L, Yu H, Yang Q. Threats to federated learning: a survey. arXiv [Preprint]. 2020 arXiv:2003.02133 [cs.CR]. Available from: https://arxiv.org/abs/2003.02133.

[29] Abadi M, McMahan HB, Chu A, Mironov I, Zhang L, Goodfellow I, et al. Deep learning with differential privacy. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16); 2016 Oct 24–28; Vienna, Austria. New York (NY): Association for Computing Machinery; 2016. p. 308–318. https://doi.org/10.1145/2976749.2978318.

[30] B. Biggio and F. Roli, "Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning," Pattern Recognition, vol. 84, pp. 317–331, 2018.

[31] Carlini N, Chien S, Nasr M, Song S, Terzis A, Tramèr F. Membership inference attacks from first principles. In: 2022 IEEE Symposium on Security and Privacy (SP); 2022 May 22–26; San Francisco, CA, USA. Piscataway (NJ): IEEE; 2022. p. 1897–1914. https://doi.org/10.1109/SP46214.2022.9833649.

[32] Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress); 2017 Jun 25–30; Honolulu, HI, USA. Piscataway (NJ): IEEE; 2017. p. 557–564. https://doi.org/10.1109/BigDataCongress.2017.85.

[33] Conti M, Sandeep Kumar E, Lal C, Ruj S. A survey on security and privacy issues of Bitcoin. IEEE Commun Surv Tutor. 2018;20(4):3416–3452. https://doi.org/10.1109/COMST.2018.2842460.

[34] Belotti M, Božić N, Pujolle G, Secci S. A vademecum on blockchain technologies: when, which, and how. IEEE Commun Surv Tutor. 2019;21(4):3796–3838. https://doi.org/10.1109/COMST.2019.2928178.

[35] Kshetri N. 1 Blockchain's roles in meeting key supply chain management objectives. Int J Inf Manage. 2018; 39:80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005.

[36] Nayyar P, Garg P. Impact of blockchain on retail supply chain. In: Ali I, Chatterjee P, Shaikh AA, Gupta N, AlArjani A, editors. Computational modelling in Industry 4.0. Singapore: Springer; 2022. p. 197–210. https://doi.org/10.1007/978-981-16-7723-6_12.

[37] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD); 2016 Aug 22–24; Vienna, Austria. Piscataway (NJ): IEEE; 2016. p. 25–30. https://doi.org/10.1109/OBD.2016.11.

[38] Khan MA, Salah K. IoT security: review, blockchain solutions, and open challenges. Future Gener Comput Syst. 2018;82:395–411. https://doi.org/10.1016/j.future.2017.11.022.

[39] Dorri A, Kanhere SS, Jurdak R. Towards an optimized blockchain for IoT. In: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (IoTDI '17); 2017 Apr 18–21; Pittsburgh, PA, USA. New York (NY): Association for Computing Machinery; 2017. p. 173–178. https://doi.org/10.1145/3054977.3055003.

[40] Bathula A, Gupta SK, Merugu S, Saba L, Khanna NN, Laird JR, et al. Blockchain, artificial intelligence, and healthcare: the tripod of future—a narrative review. Artif Intell Rev. 2024;57(9):238. https://doi.org/10.1007/s10462-024-10873-5.

[41] Mallick SR, Sobhanayak S, Lenka RK. Blockchain-enhanced IoT ecosystem for healthcare: Transformative potentials, applications, challenges, solutions, and future perspectives. Comput Ind Eng. 2024;197:110538. https://doi.org/10.1016/j.cie.2024.110538.

[42] Dubey R, Jain AK, Sharma R. A review on blockchain-

enabled federated learning: security, privacy, scalability and incentive challenges. In: 2026 9th International Conference on Circuit, Power & Computing Technologies (ICCPCT); 2026; Kollam, India. Piscataway (NJ): IEEE; 2026. p. 640–644. https://doi.org/10.1109/ICCPCT70290.2026.11654916.

[43] Shinde S, Manjramkar H, Gaidhani V, Wagh V, Joshi A. Code Sentinel: AI-driven smart contract attack simulation for vulnerability detection. ACSET [Internet]. 2026 Sep 15;2(3):125–131. Available from: https://conferenceseries.adroidjournals.com/index.php/ACSET/article/view/117.

[44] Skubis I. AI governance: ethics of trustworthy AI in healthcare. In: 2025 International Joint Conference on Neural Networks (IJCNN); 2025; Rome, Italy. Piscataway (NJ): IEEE; 2025. p. 1–8. https://doi.org/10.1109/IJCNN64981.2025.11229217.

[45] Rezaei A, Davidson SL, Wong B. Providing cross-chain interoperability through decentralized message routing and delivery. In: 2026 IEEE 46th International Conference on Distributed Computing Systems (ICDCS); 2026; Seoul, Korea, Republic of. Piscataway (NJ): IEEE; 2026. p. 1–11. https://doi.org/10.1109/2575-8411.2026.00053.