Journal of Computer and Communications, 2026, 14(8), 79-98
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Blockchain as a Platform for Artificial Intelligence (AI) Transparency

Afroja Akther, Ayesha Arobee, Abdullah Al Adnan, Omum Auyon, Farhad Akter, Antura Akter, ASM Johirul Islam

School of Business and Technology, Emporia State University, Emporia, USA
Email: afrojabnkdu@gmail.com

How to cite this paper: Akther, A., Arobee, A., Al Adnan, A., Auyon, O., Akter, F., Akter, A. and Islam, A.J. (2026) Blockchain as a Platform for Artificial Intelligence (AI) Transparency. *Journal of Computer and Communications*, **14**, 79-98.
https://doi.org/10.4236/jcc.2026.148005

Received: July 30, 2026
Accepted: August 25, 2026
Published: August 28, 2026

Abstract

As artificial intelligence (AI) systems become increasingly complex and autonomous, concerns over transparency and accountability have intensified. The "black box" problem in AI decision-making limits stakeholders' ability to understand, trust, and verify outcomes, particularly in high-stakes sectors such as healthcare, finance, and autonomous systems. Blockchain technology, with its decentralized, immutable, and transparent characteristics, presents a potential solution to enhance AI transparency and auditability. This paper explores the integration of blockchain with AI to improve decision traceability, data provenance, and model accountability. By leveraging blockchain as an immutable record-keeping system, AI decision-making can become more interpretable, fostering trust among users and regulatory compliance. However, challenges such as scalability, integration complexity, and computational overhead must be addressed to fully realize this synergy. Using a narrative literature review and conceptual analysis, this study synthesizes existing research and proposes a framework for blockchain-enhanced AI transparency, and highlights practical applications, benefits, and limitations. The findings suggest that blockchain could be a foundational technology for ensuring AI systems remain accountable, ethical, and aligned with regulatory standards.

Keywords

Artificial Intelligence (AI), Blockchain, AI Transparency, Black Box Problem, Decentralization

1. Introduction

Artificial intelligence (AI) continues to transform various sectors, including healthcare, finance, transportation, driving innovation and efficiency. However, as AI systems become more complex and autonomous, their decision-making processes often lack transparency, leading to what is commonly known as the "black box" problem. This opacity undermines trust among users and stakeholders, posing a significant barrier to the broader adoption of AI technologies. The trust deficit is particularly pronounced in high-stakes sectors, where AI-driven decisions can have profound ethical, legal, and safety implications [1]. Transparency in AI refers to the clarity and interpretability of decision-making processes within AI systems. It is crucial for validation, debugging, and building trust, both from an ethical standpoint and for practical implementation [2]. Transparent AI systems allow users to understand and challenge decisions, fostering accountability and compliance with regulatory standards such as the General Data Protection Regulation (GDPR) [3]. Despite advancements in explainable AI (XAI), many AI models, particularly deep learning systems, remain opaque, making it difficult to trace or justify their decisions.

Although transparency, explainability, interpretability, traceability, and auditability are closely related in discussions of trustworthy AI, they describe distinct properties. Transparency is the broader degree to which relevant information about an AI system, including its data sources, model characteristics, development processes, governance procedures, and decision records, is made available to appropriate stakeholders. Interpretability refers to the extent to which the internal operation of a model or the relationship between its inputs and outputs can be understood by humans. Explainability concerns the ability to provide understandable reasons or justifications for a particular AI prediction or decision, including through post-hoc techniques when the underlying model is inherently difficult to interpret. Traceability refers to the ability to reconstruct the history of an AI decision by identifying the data, model version, system events, and other relevant artifacts associated with it. Auditability refers to the ability of authorized parties to inspect and verify these records and assess whether the system operated according to specified technical, organizational, or regulatory requirements.

Within this distinction, blockchain primarily contributes to traceability and auditability by providing cryptographically verifiable and tamper-evident records of AI-related events. Recording the provenance of an input, the identity or hash of a model version, the time of execution, and the resulting output can help investigators reconstruct and verify how an AI system was operated. However, such an immutable decision record does not independently reveal the reasoning of a complex AI model. For opaque models such as deep neural networks, explanation still requires complementary interpretability or explainability mechanisms, including techniques such as SHAP, LIME, counterfactual explanations, or other model-specific approaches. Blockchain can preserve and verify these explanations, but it should be viewed as an accountability and provenance layer rather than an explanation mechanism in itself.

Blockchain technology offers unique features that can address AI transparency challenges. Known for its core attributes, decentralization, immutability, and transparency, blockchain provides a structured way to record and trace the decision-making process in AI systems [4]. Each transaction recorded on a blockchain is time-stamped and cryptographically linked to previous transactions, creating an auditable trail that enhances security and trustworthiness [5]. By integrating blockchain with AI, organizations can create verifiable records of selected decision events, data provenance, model versions, and system updates, thereby strengthening traceability and auditability. When combined with appropriate explainability techniques, such records can also support the verification and governance of explanations provided for AI-driven decisions [6] [7].

This research aims to explore the potential of blockchain technology in enhancing AI transparency, auditability, and trust. Specifically, it seeks to answer the following research questions:

1) How can blockchain be leveraged to enhance AI transparency and explainability?

2) What are the key challenges and limitations of integrating blockchain with AI?

3) How can blockchain-based AI transparency frameworks align with existing regulatory and ethical standards?

By documenting the development, deployment, and operational phases of AI within a blockchain framework, this study evaluates whether such integration can make AI decision-making processes more understandable and acceptable to a broader audience.

This study adopts a narrative literature review and conceptual analysis to examine how blockchain technology may contribute to transparency, traceability, auditability, and accountability in artificial intelligence systems. The literature considered in this paper was selected based on its relevance to five interconnected areas: AI transparency and explainability, blockchain fundamentals, blockchain-AI integration, AI governance and accountability, and regulatory and ethical considerations. Academic journal articles, conference papers, scholarly books, institutional reports, and relevant regulatory publications were considered where they contributed theoretical, technical, or governance perspectives to the research questions. Rather than applying the formal screening and exhaustive search procedures of a systematic review, the literature was evaluated conceptually according to its relevance to the proposed blockchain-AI transparency framework, its contribution to understanding benefits and limitations, and its applicability to high-stakes domains such as healthcare, finance, and autonomous systems. The reviewed literature was then synthesized thematically to identify recurring transparency challenges, potential blockchain-enabled mechanisms, implementation constraints, and areas requiring further research.

2. The Challenge of AI Transparency

Artificial intelligence (AI), particularly in its more sophisticated forms such as deep learning, has introduced unprecedented capabilities in data analysis and decision-making. However, these advances have also brought significant challenges, chiefly the opacity of the decision-making processes. This opacity, often referred to as the "black box" problem, describes situations where the internal workings of AI systems are not visible or understandable to users or stakeholders [8]. The concern is that if users cannot see or understand how decisions are made, they cannot verify the fairness, accuracy, or safety of these decisions.

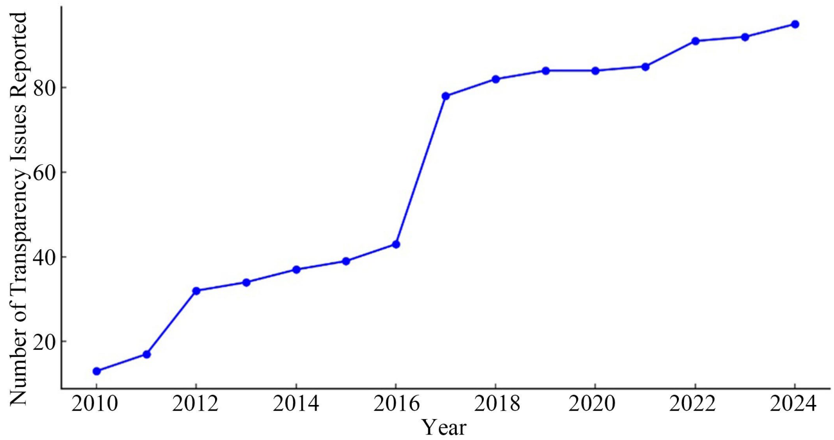

Figure 1. Key challenges affecting AI transparency (source: authors' conceptualization based on insights synthesized from scholarly articles and relevant newspaper reports)

The necessity for transparency (**Figure 1**) becomes crucial in sectors where decisions have significant consequences:

Healthcare: In healthcare, AI systems are used for diagnosing diseases, recommending treatments, and managing patient data. The accuracy and explicability of AI decisions can directly affect patient outcomes and safety [9].

Finance: In finance, AI determines credit ratings, manages investments, and detects fraud. Decisions need to be transparent to ensure fairness, avoid biases, and comply with regulations like the General Data Protection Regulation (GDPR), which includes rights to explanation [3].

Autonomous Driving: For autonomous vehicles, AI systems make real-time decisions about navigation and safety. Transparency is essential to build user trust and facilitate regulatory approval [10]. Transparency is important for fairness and regulatory accountability, including compliance with GDPR safeguards applicable to personal-data processing and certain automated decision-making practices.

The primary technical challenge in enhancing transparency is the inherent complexity of machine learning models, especially deep neural networks. These models involve large numbers of parameters and layers, which makes understanding their function and predicting their behavior difficult. This complexity is compounded by the stochastic nature of many AI algorithms, where even slight changes in input data or initial conditions can significantly alter outcomes. **Table 1** reveals several approaches have been proposed to tackle the transparency issue in AI.

Table 1. Sectors impacted by ai transparency challenges.

Sector	Impact of AI Transparency	Citations
Healthcare	In healthcare, AI's role in diagnosing diseases, recommending treatments, and managing patient data demands high transparency to ensure patient safety and treatment efficacy.	[9]
Finance	AI systems in finance determine credit ratings, manage investments, and detect fraud. Transparency is crucial to ensure fairness, avoid biases, and comply with regulations.	[3]
Autonomous Driving	For autonomous vehicles, transparent AI decision-making is essential for safety, user trust, and regulatory approval.	[10]
Legal	AI applications in the legal sector, such as predictive policing and recidivism risk assessment, require transparency to prevent biases and uphold legal standards and fairness.	[11]
Employment	In employment, AI tools are used for screening resumes and automating hiring decisions. Transparency helps ensure non-discriminatory practices and adherence to employment laws.	[12]
Retail	AI in retail enhances customer experience through personalized recommendations and inventory management. Transparency is needed to protect consumer data and ensure privacy.	[13]

Table 2. Strategies for improving ai transparency.

Strategy	Description	References
Simplification of Models	Using simpler models such as decision trees or linear regression that are more interpretable compared to complex models like neural networks. These are easier to understand but may offer less analytical power.	[14]
Development of Interpretability Tools	Tools like LIME and SHAP have been developed to make the output of complex models more interpretable to users, allowing for better understanding of how decisions are made.	[15]
Incorporating Transparency by Design	Embedding transparency into the AI development process to ensure systems are understandable from the beginning, rather than attempting to add explanations to pre-existing models.	[16]

Transparency is not only a technical requirement but also an ethical imperative. Ethical guidelines for AI, such as those proposed by the EU's High-Level Expert Group on Artificial Intelligence, emphasize respect for human autonomy, prevention of harm, fairness, and explicability as key requirements [17]. Regulatory frameworks are also evolving to address these challenges, emphasizing the need for transparency (Table 2) to ensure that AI systems do not perpetuate biases or make unjustifiable decisions.

Addressing the transparency challenge in AI is critical for its ethical application and broader acceptance, especially in high-stakes domains. Ongoing research into interpretability, the development of new tools, and the creation of robust regulatory frameworks are essential to ensuring that AI systems operate transparently and are accountable for their decisions.

3. Blockchain Fundamentals

Blockchain technology, initially popularized by the cryptocurrency Bitcoin, is fundamentally a distributed ledger that records transactions across multiple computers in such a way that the registered transactions cannot be altered retroactively [18]. This technology provides a robust framework for facilitating transactions without the need for a trusted third party, such as a bank or regulatory agency [5] [19]. This section explores the core characteristics of blockchain technology, decentralization, immutability, and transparency—and their implications for enhancing AI transparency. Decentralization refers to the distribution of control and authority across all network participants. Unlike traditional centralized systems where a single entity has control, blockchain distributes the control to all participating nodes in the network. This not only eliminates a single point of failure but also increases resistance to malicious activities [20]. In the context of AI, decentralization can democratize data handling, allowing multiple stakeholders to participate in training and decision-making processes of AI models. This is particularly beneficial in scenarios like federated learning, where multiple entities collaborate to improve a model while maintaining control over their own data.

Immutability in blockchain refers to the characteristic that, once a transaction has been recorded in the distributed ledger, it cannot be altered or deleted by any single party. This is ensured through cryptographic hash functions and the consensus mechanisms that require majority approval from all nodes in the network for changes to be made [21]. For AI systems, immutability means that every decision, data input, model adjustment, and output can be permanently recorded and verified. This assures stakeholders of the integrity of the data used and the decisions made by AI systems, which is critical in sectors requiring high levels of auditability such as healthcare and financial services.

Transparency in blockchain technology means that all transactions and their details are visible to anyone who has access to the network. While individual user identities can be protected through pseudonyms, the transactions themselves are open to scrutiny [22]. Transparency helps in making AI systems more understandable and accountable. Stakeholders can trace the decision-making process, understand the data inputs and outputs, and verify the actions taken by an AI system. This level of openness is vital for building trust, particularly in applications affecting public services or consumer rights.

Practical Applications and Challenges

Blockchain's integration with AI has practical applications in numerous fields. For example, in supply chain management, blockchain can provide a transparent, immutable record of product provenance and handling, which can be combined with AI to optimize logistics and predict supply chain disruptions [23]. Despite its potential, blockchain faces challenges such as scalability, energy consumption, and complexity integration with existing technologies. These challenges need to be addressed to fully harness the power of blockchain in AI transparency [24]. The fundamental characteristics of blockchain, decentralization, immutability, and transparency, offer a strong foundation for addressing the transparency issues in AI systems. By embedding these features into AI workflows, stakeholders can achieve a higher degree of trust and accountability, paving the way for more responsible and acceptable AI applications.

4. Integrating Blockchain with AI

The integration of blockchain technology with artificial intelligence (AI) systems (**Table 3**) presents a transformative approach to enhancing transparency, accountability, and trust in AI operations. Blockchain's core features, decentralization, immutability, and transparency, can significantly augment AI functionalities in various ways, from decision-making processes to data handling and model management. Immutability in blockchain should be understood as tamper resistance rather than absolute unchangeability. Once a transaction is confirmed and incorporated into the ledger, modifying its historical record becomes difficult because records are cryptographically linked and validated according to the network's consensus protocol. However, the strength of this immutability depends on the blockchain architecture, governance model, consensus mechanism, validator structure, and underlying security assumptions. Different blockchain systems use different procedures for validating transactions, and consensus does not necessarily require approval from a majority of all network nodes. In permissioned blockchains, for example, transaction validation may be performed by a defined set of authorized participants according to established governance and consensus rules. Therefore, blockchain provides varying degrees of tamper resistance and verifiability depending on how the network is designed and governed.

4.1. Tracking and Recording Decisions

Every decision made by an AI system, from simple classifications to complex predictive analytics, can be recorded on a blockchain. This recording process includes the inputs, decision-making parameters, and outputs of the AI system. Such a transparent and immutable record ensures that every decision is traceable and auditable. This feature is particularly valuable in environments where decisions must be explainable and verifiable, such as in regulatory compliance or legal investigations [25]. Implementing this would require linking AI decision-making processes directly to a blockchain interface, where each decision triggers a transaction on the blockchain. This could be facilitated through smart contracts that automatically execute and record transactions when certain conditions are met (**Figure 2**). In a practical blockchain-AI architecture, sensitive datasets, large model files, detailed parameters, and high-volume AI outputs should generally remain off-chain in secure databases, encrypted storage, or controlled data repositories. The blockchain should instead store cryptographic hashes, timestamps, model-version identifiers, data-provenance metadata, access or authorization records, and references to the corresponding off-chain artifacts. When an AI decision is audited, the hash of the retrieved off-chain artifact can be compared with the hash recorded on the blockchain to verify that the underlying data or model has not been altered. This hybrid architecture preserves blockchain-based traceability and integrity while reducing storage overhead, protecting sensitive information, and avoiding the impracticality of placing large AI datasets and model artifacts directly on-chain.

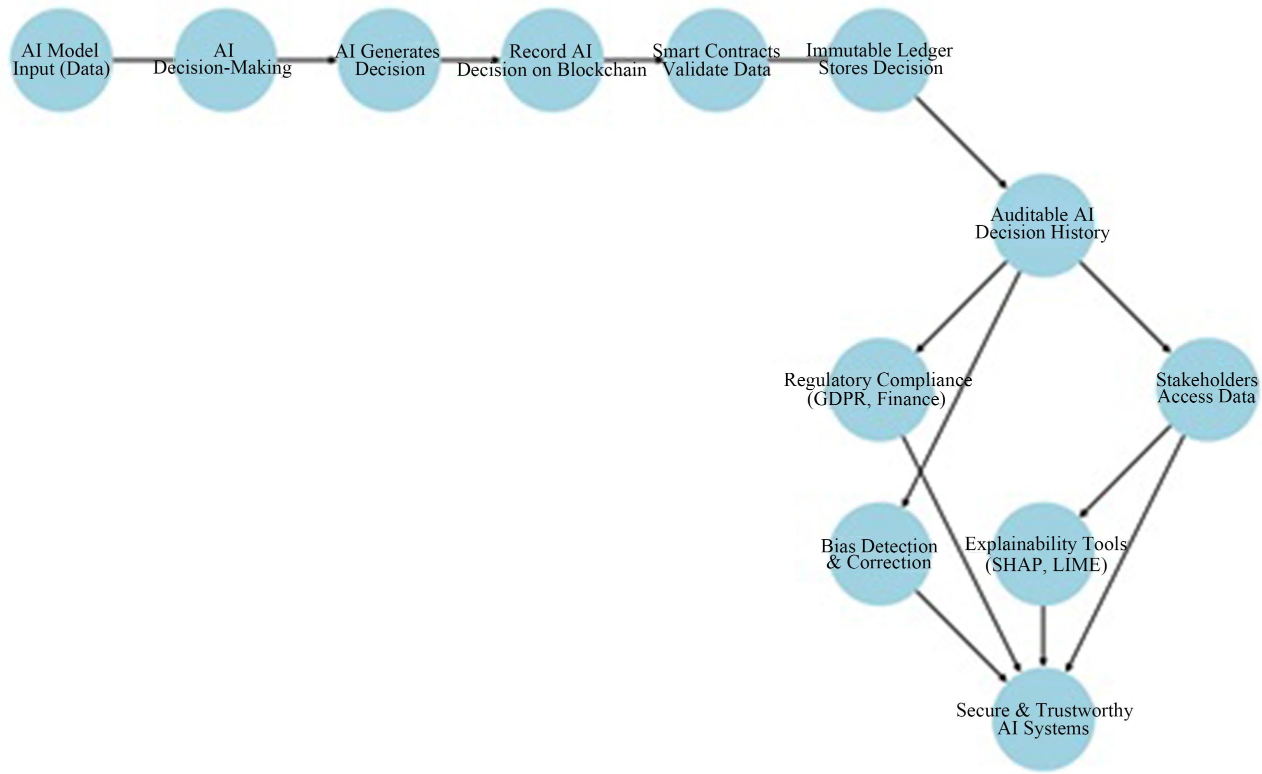

Figure 2. Blockchain enhanced ai transparency framework (source: authors).

4.2. Considerations for Blockchain Architectures and AI Model Variability

While blockchain technology offers promising solutions for enhancing AI transparency, the selection of appropriate blockchain architecture is crucial for optimizing its effectiveness. Existing blockchain frameworks, such as Ethereum, Hyperledger Fabric, and Corda, each have unique characteristics that impact their suitability for recording AI decision-making processes. Ethereum, with its smart contract capabilities, provides a decentralized and programmable infrastructure, while Hyperledger Fabric offers permissioned ledger functionality, which may be preferable in enterprise or regulatory environments. Corda, designed for financial applications, emphasizes privacy and efficient transaction validation. A comparative analysis of these architectures would provide deeper insight into their applicability for AI governance and auditability.

Furthermore, the degree to which blockchain enhances AI transparency depends on the underlying AI model. Neural networks, decision trees, and ensemble learning models exhibit varying levels of interpretability. Decision trees, for instance, are inherently transparent due to their rule-based structure, while deep neural networks (DNNs) function as "black boxes", making their decision-making processes less interpretable. Blockchain's role in ensuring AI transparency may therefore differ depending on the model in question. Integrating blockchain with explainability frameworks such as SHAP (Shapley Additive Explanations), LIME (Local Interpretable Model-agnostic Explanations), or counterfactual reasoning could enhance the traceability and verifiability of AI-driven decisions across different model types. Future research should explore how blockchain's immutable ledger can be effectively leveraged to store model explanations, thereby improving accountability and regulatory compliance in AI applications.

Table 3. Integrating blockchain with AI.

Integration Aspect	Description	Impacts and Benefits	References
Tracking and Recording Decisions	Cryptographic hashes, provenance metadata, model-version identifiers, timestamps, and references to AI decision artifacts are recorded on-chain, while sensitive data, model parameters, and large outputs remain securely stored off-chain. This process ensures transparency and auditability.	Enhances the explainability and verifiability of AI decisions, crucial in environments requiring regulatory compliance or legal scrutiny.	[25]
Data Handling and Usage	Blockchain logs details about the datasets used by AI, including data provenance, usage, and changes.	Ensures data integrity and consistency, critical for applications where data history influences outputs, such as financial forecasting or clinical support systems.	[26]
Model Management	Blockchain manages AI models, tracking versions, updates, performance metrics, and deployment records.	Facilitates understanding of AI model lifecycle, aids in identifying which models were used and why, and supports rollback features to previous model versions if needed.	[27]

4.3. Data Handling and Usage

Blockchain can be used to log the datasets utilized by AI systems throughout their learning and operational processes. This includes recording details about data provenance, access, and changes over time. By using blockchain to monitor data handling, stakeholders can ensure the integrity and consistency of data used by AI systems. This is crucial for applications where data sources and history significantly influence the system's outputs, such as in financial forecasting or clinical decision support systems [26]. A blockchain ledger could capture metadata about each dataset accessed by the AI system, including who provided the data, when it was used, and any alterations made. This process not only aids in tracking data lineage but also helps in maintaining compliance with data governance standards and privacy regulations.

4.4. Model Management

Blockchain can facilitate the management of AI models, including their versions, updates, performance metrics, and deployment records. This aspect of blockchain integration helps maintain a chronological log of model evolution. Effective model management is critical for understanding the lifecycle of AI models, particularly in complex systems where multiple models are tested and deployed over time. Recording model changes on a blockchain can aid developers and stakeholders in identifying which models were used in specific instances and why changes were made [27]. Blockchain can store hashes of model versions along with detailed descriptions and performance metrics. Each time a model is updated, a new entry is made in the blockchain, creating an immutable history of the model's development and use. This approach can also support rollback features where an earlier model version can be reinstated from the blockchain records if needed.

Integrating blockchain with AI can significantly enhance the transparency, reliability, and auditability of AI systems. This integration not only addresses trust issues associated with AI but also paves the way for new standards in the development and deployment of trustworthy AI systems. By recording every key action and decision on a blockchain, stakeholders can ensure that AI systems are not only powerful and efficient but also accountable and open to scrutiny.

5. Potential Benefits of Using Blockchain for AI Transparency

5.1. Increased Trust

Trust is foundational to the broader acceptance and adoption of AI systems, particularly in sectors where decisions have significant implications, such as healthcare, finance, and autonomous systems. Blockchain can enhance trust in AI by providing a transparent, immutable record of all AI operations, including data inputs, decision-making processes, and outputs. This transparency ensures that AI decisions are not only visible but also verifiable, making it easier for users and stakeholders to trust the output generated by AI systems [28]. By allowing stakeholders to audit and validate AI decisions through blockchain records, any anomalies or biases in AI operations can be detected and addressed. This leads to improved trust, which is crucial for industries that rely on public confidence to operate effectively.

5.2. Enhanced Security

Security concerns in AI involve unauthorized data access, tampering, and potential misuse of AI technologies. Blockchain addresses these issues with its inherent security features such as cryptographic hash functions, consensus algorithms, and distributed network architecture, which ensure that once a transaction is added to the blockchain, it cannot be altered or deleted by any single entity without detection [29]. Implementing blockchain within AI frameworks can protect against tampering and enhance the overall security of AI systems. For example, in AI-driven supply chain solutions, blockchain can secure data across the network, from the manufacturer to the end consumer, ensuring that all decisions and transactions are accurately recorded and resistant to fraud.

Threat Model and Security Assumptions

The proposed blockchain-AI framework assumes several potential threat actors. First, an internal administrator, developer, or system operator may attempt to modify or delete AI decision records after an unfavorable or erroneous outcome. Blockchain can mitigate this risk by providing cryptographically linked, tamper-evident records whose alteration can be detected through ledger verification. Second, authorized users, data providers, sensors, or external systems may submit inaccurate, manipulated, or misleading inputs to the AI system. Blockchain can preserve the provenance and history of such inputs, but it cannot independently guarantee that the original information was truthful or accurate. Third, unauthorized parties may attempt to access sensitive audit logs, decision metadata, or provenance records. Appropriate authentication, role-based access control, encryption, and permission management are therefore required, particularly in enterprise and regulated environments. Finally, in a permissioned blockchain, organizations or validators with administrative or governance authority may collude, misuse privileges, alter access policies, or exercise excessive control over validation. The security of the system therefore depends not only on blockchain technology but also on validator distribution, governance rules, consensus configuration, key management, and organizational controls.

Compared with conventional centralized audit logging, blockchain can provide additional protection where multiple independent stakeholders require a shared, verifiable record and no single participant should have unilateral authority to rewrite the audit history. However, blockchain does not prevent malicious or inaccurate data from being entered initially, nor does it eliminate insider threats, compromised credentials, or governance failures. Its primary security contribution in this context is strengthening record integrity, provenance verification, tamper evidence, and shared auditability.

5.3. Regulatory Compliance

Blockchain-based auditability should not be interpreted as automatically ensuring compliance with the GDPR or other AI-governance requirements. Where AI decision records contain personal or decision-related information, an immutable ledger may create tension with principles such as data minimization and with data-subject rights such as erasure. The GDPR also places safeguards around certain decisions based solely on automated processing that produce legal or similarly significant effects. Accordingly, personally identifiable information, sensitive input data, detailed decision outputs, and large AI artifacts should generally remain off-chain [30]. The blockchain should instead contain only the minimum information necessary for verification, such as cryptographic hashes, timestamps, model-version identifiers, provenance metadata, and non-sensitive references to securely maintained off-chain records.

This hybrid architecture can better reconcile auditability with privacy requirements. If an off-chain personal record must be corrected or erased where legally required, the underlying information can be removed or modified without placing the personal data itself permanently on the ledger; the remaining on-chain hash would function primarily as evidence that a particular artifact existed or was processed at a given point in time. Access to both on-chain audit metadata and off-chain records should also be governed through appropriate authentication, authorization, encryption, and role-based controls. However, the compatibility of a particular blockchain implementation with GDPR requirements remains dependent on its architecture, the nature of the information recorded, the purpose and legal basis of processing, retention requirements, and the allocation of responsibilities among participating organizations. Therefore, blockchain should be described as a technology that may support regulatory accountability and evidence preservation, rather than as a mechanism that guarantees regulatory compliance.

Similarly, AI governance requires more than immutable record keeping. Under the EU AI Act, applicable high-risk AI systems are subject to requirements concerning record keeping, transparency, and human oversight, among other obligations. Blockchain-based logs may help support evidence and traceability for such governance processes, but they do not replace the broader organizational and technical safeguards required by the regulatory framework.

5.4. Enhancing the Framework and Practical Applications

While the proposed framework for integrating blockchain with AI transparency outlines key principles, it requires further elaboration to establish a more comprehensive and implementable model. A well-defined architectural framework detailing the interaction between blockchain components (e.g., smart contracts, distributed ledgers, and consensus mechanisms) and AI models (e.g., neural networks, decision trees, and reinforcement learning systems) would provide clearer insights into how blockchain can enhance AI transparency in practical scenarios. Additionally, a conceptual diagram or system architecture illustrating the data flow, decision verification process, and auditability features within a blockchain-integrated AI system would significantly improve the framework's clarity and applicability.

Beyond theoretical discussions, the paper lacks empirical evidence or case studies demonstrating successful implementations of blockchain-enhanced AI transparency. Several real-world applications highlight the potential of this integration.

5.4.1. Healthcare—AI-Powered Diagnostics and Blockchain for Auditability

A study by Kuo *et al.* (2017) explored how blockchain technology can enhance electronic health records (EHRs) by ensuring data integrity and patient consent tracking. When combined with AI-driven diagnostic tools, blockchain can provide an immutable record of diagnostic decisions, allowing medical practitioners to verify how AI-derived conclusions were reached. This approach enhances trust in AI-powered medical decision-making, particularly in critical diagnoses like oncology and radiology [9].

5.4.2. Finance—Fraud Detection and Blockchain-Based Transaction Transparency

In financial applications, AI is widely used for fraud detection and risk assessment. Wang *et al.* (2018) demonstrated that integrating AI with blockchain enhances fraud detection models by ensuring transaction traceability and preventing data manipulation [27]. AI models can analyze transaction patterns, while blockchain serves as a tamper-proof ledger to maintain the integrity of AI's decision-making history, thereby improving compliance with regulations like the General Data Protection Regulation (GDPR) [3].

5.4.3. Autonomous Systems—Blockchain for Explainable AI in Self-Driving Vehicles

AI-driven autonomous vehicles rely on deep learning models to process sensor data and make real-time driving decisions. However, McAllister *et al.* (2017) argue that a lack of transparency in these decisions remains a critical challenge for regulatory approval [10]. By storing decision logs on blockchain, regulators and manufacturers can audit vehicle behavior in accident scenarios, ensuring accountability and legal compliance. Companies such as Bosch and IBM have initiated projects using blockchain to secure autonomous driving data, reinforcing AI's explainability and reducing liability concerns.

Table 4. Potential benefits of using blockchain for ai transparency.

Benefit	Explanation and Impact	References
Increased Trust	Blockchain enhances trust in AI by making AI decisions auditable and understandable, providing a transparent record of AI operations. Impact: This visibility allows users and stakeholders to verify AI decisions, essential for trust, particularly in critical sectors like healthcare and finance.	[28]
Enhanced Security	Blockchain's security features, such as cryptographic hashes and consensus algorithms, protect AI systems from tampering and unauthorized access. Impact: This secures data across networks, crucial for AI-driven processes where data integrity is fundamental, such as in supply chains.	[29]
Regulatory Compliance	Blockchain supports compliance with regulations that demand transparency and accountability in AI, such as the GDPR. Impact: Blockchain's audit trails help organizations demonstrate compliance effectively, crucial for operations impacted by automated decision-making regulations.	[30]

While these case studies provide promising insights, further empirical validation is required to measure the performance of blockchain-enhanced AI transparency in diverse sectors. Future research should focus on developing and testing blockchain-AI integration models in real-world environments, assessing their impact on scalability, efficiency, and regulatory compliance. Conducting comparative analyses of different blockchain architectures (e.g., Ethereum, Hyperledger, Corda) within AI-driven decision-making frameworks would offer valuable insights into selecting the most suitable infrastructure for enhancing AI transparency. By incorporating empirical data and practical implementations, this research can better inform policymakers, industry stakeholders, and researchers about the viability of blockchain as a foundational technology for AI governance.

Integrating blockchain with AI offers significant benefits (**Table 4**) that can address some of the key challenges currently faced by AI technologies, particularly in terms of trust, security, and regulatory compliance. The decentralized, immutable, and transparent nature of blockchain makes it an ideal technology to enhance the accountability and trustworthiness of AI systems, thereby facilitating wider adoption and more responsible use of AI across various sectors.

6. Challenges and Considerations in Integrating Blockchain with AI

6.1. Scalability

Blockchain technology, particularly when based on proof-of-work (PoW) consensus mechanisms, often struggles with scalability issues. The inherent design of many blockchains limits their transaction throughput, which can lead to delays and increased costs for recording transactions [31]. AI systems, especially those requiring real-time data processing and decision-making, need high-speed data access and processing capabilities. The slow transaction speeds and potential bottlenecks of blockchain can significantly hinder the performance of AI applications that depend on large datasets and immediate responses, such as those used in autonomous driving or real-time financial trading [32].

6.2. Complexity

Integrating blockchain with AI adds a layer of complexity to both systems. Blockchain networks require maintenance of consensus protocols, execution of smart contracts, and management of cryptographic keys, among other aspects. The added complexity could impact on the overall efficiency and performance of AI systems. For instance, the computational overhead required to maintain blockchain integrity and execute smart contracts can divert resources away from core AI processing tasks, potentially degrading system performance [33].

6.3. Technological Integration

Both AI and blockchain are sophisticated technologies that operate on different paradigms. AI involves adaptive learning processes and probabilistic logic, while blockchain is based on deterministic and immutable record-keeping. Bridging the technological gap requires meticulous architectural planning and integration. The challenge lies in ensuring that blockchain does not impede the learning efficiency of AI or its ability to update and adapt dynamically to new data. This integration must be thoughtfully designed to maintain the strengths of both technologies without compromising their core functionalities [34].

6.4. Addressing Challenges in Blockchain-AI Integration

While blockchain technology presents a promising approach for enhancing AI transparency, its implementation is not without challenges. The paper acknowledges key limitations such as scalability and integration complexities; however, potential solutions and mitigation strategies for these issues remain underexplored. One primary scalability concern arises from blockchain's consensus mechanisms, particularly Proof-of-Work (PoW), which can be computationally intensive and result in low transaction throughput [35]. Alternative consensus protocols, such as Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), and Directed Acyclic Graphs (DAGs), could mitigate these concerns by improving processing speed and reducing energy consumption. Additionally, layer-2 scaling solutions such as sharding, rollups, and state channels have been proposed to enhance blockchain efficiency without compromising security or decentralization. Future research should evaluate the feasibility of these approaches in AI-integrated blockchain systems.

Another critical challenge pertains to energy consumption, particularly in blockchains utilizing PoW-based mechanisms. The high computational requirements of PoW contribute to significant energy expenditures, raising concerns about sustainability. Exploring energy-efficient blockchain frameworks, such as Hyperledger Fabric, which employs a permissioned and optimized consensus mechanism, or Ethereum's transition to PoS, could provide insights into more sustainable blockchain applications for AI governance. Assessing the trade-offs between decentralization, security, and energy efficiency will be essential for developing AI-integrated blockchain solutions that align with environmental sustainability goals.

Beyond technical concerns, the ethical implications of using blockchain for AI transparency require deeper examination. While blockchain enhances auditability and accountability, it also raises questions regarding data privacy and anonymization. The immutability of blockchain records, while beneficial for maintaining an auditable history, could conflict with privacy regulations such as the General Data Protection Regulation (GDPR), which mandates the right to be forgotten. Solutions such as zero-knowledge proofs (ZKPs), homomorphic encryption, and privacy-preserving smart contracts could help balance transparency with data protection. Additionally, blockchain's role in mitigating AI biases and ensuring fair decision-making processes must be further explored to address ethical concerns surrounding algorithmic accountability and governance. A practical mitigation is therefore to avoid placing personal data directly on-chain and instead store only cryptographic hashes and minimal provenance metadata on the ledger, while keeping personal and erasable records in access-controlled off-chain storage.

Future research should focus on developing hybrid models that integrate privacy-preserving blockchain mechanisms with AI explainability frameworks to ensure a balance between transparency, efficiency, and ethical compliance. These considerations will be critical in fostering the responsible and scalable deployment of blockchain-integrated AI systems.

Table 5. Challenges and considerations in integrating blockchain with AI.

Challenge Category	Description	Specific Issues and Impacts	References
Scalability	Blockchain, especially using proof-of-work (PoW) mechanisms, faces scalability issues due to limited transaction throughput.	AI systems requiring real-time data processing find blockchain's slow transaction speeds a significant bottleneck. This is critical in applications needing immediate responses, like autonomous driving or real-time financial trading.	[31]
Complexity	Integrating blockchain adds complexity due to the need for maintaining consensus protocols, managing cryptographic keys, and executing smart contracts.	The additional computational overhead can reduce the efficiency and performance of AI systems. Resources needed to maintain blockchain integrity and execute smart contracts may divert from core AI tasks, affecting overall system performance.	[33]
Technological Integration	AI and blockchain operate on fundamentally different paradigms: AI on adaptive learning and probabilistic logic, and blockchain on deterministic and immutable record-keeping.	Bridging the gap between these technologies requires careful planning to ensure that the integration does not compromise the functionality of either system. The challenge is to design a system where blockchain supports AI's dynamic learning and updating capabilities without hindering its efficiency.	[34]

The integration of blockchain and AI (**Table 5**) offers significant potential benefits but also presents considerable challenges. Addressing these challenges requires ongoing research, technological innovation, and perhaps most importantly, collaborative efforts between experts in both fields to devise solutions that harness the strengths of both technologies without undue compromise.

7. Conclusion

Blockchain's attributes of decentralization, immutability, and transparency make it a transformative tool for enhancing AI transparency and trustworthiness. By creating a clear, auditable trail of AI decisions and data usage, blockchain has the potential to demystify complex AI operations, ensuring that stakeholders, regulators, and end-users can verify and understand AI-driven processes. This enhanced accountability is particularly crucial in high-stakes sectors such as healthcare, finance, and autonomous systems, where explainability and ethical considerations play a pivotal role in decision-making. However, the integration of blockchain and AI is not without challenges. Scalability issues, stemming from blockchain's transaction speed and storage limitations, must be addressed to handle the vast volumes of AI-generated data efficiently. Additionally, the computational complexity of merging AI inference mechanisms with blockchain's immutable nature necessitates the development of optimized consensus algorithms, hybrid architectures, and privacy-preserving techniques to ensure both efficacy and efficiency.

8. Call to Action & Future Directions

Realizing the full potential of blockchain in enhancing AI transparency requires sustained interdisciplinary research and industry collaboration. Moving forward, efforts should focus on:

1) Developing Scalable Blockchain-AI Frameworks—Advancing layer-2 solu-

tions, sharding, and hybrid architectures to address blockchain's throughput and storage limitations.

2) Enhancing AI Explainability via Blockchain—Integrating explainability tools (SHAP, LIME, counterfactual reasoning) directly into blockchain-verified AI models.

3) Exploring Regulatory Alignment—Establishing frameworks that ensure compliance with data privacy laws (GDPR, AI Act) while maintaining transparency.

4) Validating Blockchain-AI Applications—Conducting real-world case studies in critical sectors to measure feasibility, security, and efficiency.

The urgency of blockchain-AI research cannot be overstated. As AI continues to shape industries and societies, ensuring its transparency, fairness, and accountability will be imperative for ethical AI adoption. By leveraging blockchain's capabilities, we have the opportunity to establish a new paradigm for AI governance—one that fosters trust, mitigates risks, and ensures responsible AI deployment at scale.

While there are hurdles to overcome, the potential benefits of integrating blockchain with AI are transformative. With strategic innovation, policy alignment, and industry adoption, blockchain-enhanced AI can redefine trust and security in automated decision-making, paving the way for a more transparent, explainable, and ethically aligned future.

Declaration of Generative AI and AI-Assisted Technologies in Manuscript Preparation

During the preparation of this manuscript, the authors used ChatGPT (OpenAI) to assist with language refinement, sentence organization, sequencing of ideas, grammatical improvement, and overall readability. The tool was used to improve the presentation and clarity of the authors' written material.

The research concept, literature selection, conceptual analysis, arguments, proposed framework, interpretation, conclusions, and intellectual contributions were developed by the authors. ChatGPT was not treated as a source of scholarly evidence, and the authors independently reviewed and verified the accuracy, relevance, and appropriateness of the manuscript content and references. All AI assisted suggestions were carefully reviewed, revised where necessary, and approved by the authors. The authors take full responsibility for the accuracy, integrity, originality, and final content of the manuscript.

Author Contributions

Afroja Akther: Conceptualization, methodology, investigation, literature review, conceptual analysis, framework development, original draft preparation, review and editing, and project administration.

Ayesha Arobee: Conceptualization, methodology, investigation, literature review, conceptual analysis, framework development, original draft preparation, and review and editing.

Abdullah Al Adnan: Investigation, literature review, conceptual analysis, visualization, original draft preparation, and preparation of tables and figures.

Omum Auyon: Investigation, literature review, conceptual analysis, visualization, original draft preparation, and preparation of tables and figures.

Farhad Akter: Investigation, literature review, conceptual analysis, original draft preparation, and review and editing.

Antura Akter: Investigation, literature review, visualization, original draft preparation, and review and editing.

ASM Johirul Islam: Conceptualization, framework development, supervision, critical review, review and editing, and overall research guidance.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., *et al.* (2018) AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, **28**, 689-707. https://doi.org/10.1007/s11023-018-9482-5

[2] Burrell, J. (2016) How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms. *Big Data & Society*, **3**, 1-12. https://doi.org/10.1177/2053951715622512

[3] Goodman, B. and Flaxman, S. (2017) European Union Regulations on Algorithmic Decision Making and a "Right to Explanation". *AI Magazine*, **38**, 50-57. https://doi.org/10.1609/aimag.v38i3.2741

[4] Christidis, K. and Devetsikiotis, M. (2016) Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, **4**, 2292-2303. https://doi.org/10.1109/access.2016.2566339

[5] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://assets.pubpub.org/d8wct41f/31611263538139.pdf

[6] Le, V. (2024) Integrating Blockchain and Machine Learning for Continuous Auditing: Challenges and Strategies. Bachelor's Thesis, Aalto University.

[7] Ebers, M., Hoch, V.R.S., Rosenkranz, F., Ruschemeier, H. and Steinrötter, B. (2021) The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). *J*, **4**, 589-603. https://doi.org/10.3390/j4040043

[8] Hossain, M.I., Al Banna, H., Arobee, A., Jawed, S., Akter, F. and Akter, F. (2025) Technology as a Driver of Strategic Survival: Rethinking Business Models and Strategy. *International Journal of Business and Technology Management*, **7**, 245-252.

[9] Rajkomar, A., Dean, J. and Kohane, I. (2018) Machine Learning in Medicine. *New England Journal of Medicine*, **380**, 1347-1358. https://doi.org/10.1056/nejmra1814259

[10] McAllister, R., Gal, Y., Kendall, A., Van Der Wilk, M., Shah, A., Cipolla, R. and Weller, A. (2017) Concrete Problems in AI Safety. arXiv preprint arXiv:1606.06565.

[11] Brantingham, P.J., Valasik, M. and Mohler, G.O. (2018) Does Predictive Policing Lead to Biased Arrests? Results from a Randomized Controlled Trial. *Statistics and*

Public Policy, **5**, 1-6. https://doi.org/10.1080/2330443x.2018.1438940

[12] Kim, P.T. (2016) Data-Driven Discrimination at Work. *William & Mary Law Review*, **58**, Article 4.

[13] Viswanathan, J. (2024) Artificial Intelligence: Transforming the Future of Retail. *International Journal of Science and Research*, **13**, 174-178. https://doi.org/10.21275/sr24901234506

[14] Lipton, Z.C. (2016) The Mythos of Model Interpretability. *Queue*, **16**, 31-57. https://doi.org/10.1145/3236386.3241340

[15] Ribeiro, M.T., Singh, S. and Guestrin, C. (2016) "Why Should I Trust You?": Explaining the Predictions of Any Classifier. *Proceedings of the* 22*nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Francisco, 13-17 August 2016, 1135-1144.

[16] Doshi-Velez, F. and Kim, B. (2017) Towards a Rigorous Science of Interpretable Machine Learning. arXiv preprint arXiv:1702.08608.

[17] Smuha, N.A. (2019) The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence. *Computer Law Review International*, **20**, 97-106. https://doi.org/10.9785/cri-2019-200402

[18] Hussain, M.I., Bhuiyan, M.K.I., Sumon, S.A., Akter, S., Hossain, M.I. and Akther, A. (2024) Enhancing Data Integrity and Traceability in Industry Cyber Physical Systems (ICPS) through Blockchain Technology: A Comprehensive Approach. *Advances in Artificial Intelligence and Machine Learning*, **4**, 2883-2907. https://doi.org/10.54364/aaiml.2024.44168

[19] Hossain, M.I., Hussain, M.I., Arobee, A., Zim, M.N.F., Badhon, M.B. and Akter, S. (2025) Balancing Innovation and Sustainability: Learn the Potential Impact on the Environment of Bitcoin Mining. *Journal of Knowledge Management Practice*, **25**, 1-19. https://doi.org/10.62477/jkmp.v25i1.487

[20] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017 *IEEE International Congress on Big Data* (*BigData Congress*), Honolulu, 25-30 June 2017, 557-564. https://doi.org/10.1109/bigdatacongress.2017.85

[21] Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V. (2016) Blockchain Technology: Beyond Bitcoin. *Applied Innovation*, **2**, 6-10.

[22] Tapscott, D. and Tapscott, A. (2016) Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World. Penguin.

[23] Kshetri, N. (2018) 1 Blockchain's Roles in Meeting Key Supply Chain Management Objectives. *International Journal of Information Management*, **39**, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

[24] Swan, M. (2015) Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

[25] O'Leary, D.E. (2017) Configuring Blockchain Architectures for Transaction Information in Blockchain Consortiums: The Case of Accounting and Supply Chain Systems. *Intelligent Systems in Accounting*, *Finance and Management*, **24**, 138-147. https://doi.org/10.1002/isaf.1417

[26] Kuo, T.T., Kim, H.E. and Ohno-Machado, L. (2017) Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications. *Journal of the American Medical Informatics Association*, **24**, 1211-1220. https://doi.org/10.1093/jamia/ocx068

[27] Wang, Y. and Kogan, A. (2018) Designing Confidentiality-Preserving Blockchain-Based Transaction Processing Systems. *International Journal of Accounting Infor-*

mation Systems, **30**, 1-18. https://doi.org/10.1016/j.accinf.2018.06.001

[28] Fernandez-Carames, T.M. and Fraga-Lamas, P. (2020) A Review on the Use of Blockchain for the Internet of Things. *IEEE Access*, **6**, 32979-33001. https://doi.org/10.1109/access.2018.2842685

[29] Dai, H.N., Zheng, Z. and Zhang, Y. (2019) Blockchain for Internet of Things: A Survey. *IEEE Internet of Things Journal*, **6**, 8076-8094. https://doi.org/10.1109/jiot.2019.2920987

[30] Voigt, P. and Von dem Bussche, A. (2017) The EU General Data Protection Regulation (GDPR). Springer International Publishing.

[31] Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., *et al*. (2016) On Scaling Decentralized Blockchains. In: *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 106-125. https://doi.org/10.1007/978-3-662-53357-4_8

[32] Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H. (2018) Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*, **14**, 352-375. https://doi.org/10.1504/ijwgs.2018.095647

[33] Hawlitschek, F., Notheisen, B. and Teubner, T. (2018) The Limits of Trust-Free Systems: A Literature Review on Blockchain Technology and Trust in the Sharing Economy. *Electronic Commerce Research and Applications*, **29**, 50-63. https://doi.org/10.1016/j.elerap.2018.03.005

[34] Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K. (2016) Where Is Current Research on Blockchain Technology—A Systematic Review. *PLOS ONE*, **11**, e0163477. https://doi.org/10.1371/journal.pone.0163477

[35] Akther, A., Sultana, T., Arobee, A., Badhon, M.B., Akter, F. and Eashrak, N. (2025) Investigating How Quantum Cryptographic Techniques Can Enhance the Security of Blockchain-Based Artificial Intelligence (AI) Models. *Journal of Knowledge Management Practice*, **25**, 1-10. https://doi.org/10.62477/jkmp.v25i4.535