The Integration of Artificial Intelligence and Blockchain: Applications and Challenges in Economic Security and Data Privacy

Hongda Zhong*

Donald Bren School of Information & Computer Science, University of California - Irvine, 92606 Irvine, United States

Abstract. Artificial Intelligence (AI) and blockchain integrated have a transforming potential across many industries, most especially in enhancing data security, smoothing supply chains, or improving payment systems. While AI drives efficiency in the analysis of data, blockchain provides a secure, decentralized framework that ensures integrity through guaranteed transparency. The paper discusses the working relationship between AI and blockchain, focusing on their applications within economic transactions, supply chain traceability, and security within the Internet of Things (IoT). By integrating the predictive analytics of AI with blockchain's immutable ledger, a company can potentially handle any given risk in connected systems and amplify cybersecurity. Not that there are no challenges, such as scalability and integration with legacy systems, but this convergence indeed holds great promise and provides a robust solution to the demands placed on the digital economy and directions of future innovation. This review provides valuable insights for researchers and industry professionals seeking to utilize the combined strengths of AI and blockchain, offering a comprehensive understanding of how these technologies can address current security and efficiency challenges while laying a foundation for future advancements in digital infrastructure.

1 Introduction

These days, artificial intelligence tremendously develops all over the world, and in various fields, from automation to financial prediction, even in medical systems. The development of artificial intelligence not only assists in boosting the economy, but also helps to improve the quality of humans' daily lives. People are able to easily access artificial intelligence to help them in their study and work, since these artificial intelligences are more powerful than normal search engines. Artificial intelligence can give live examples and comprehensive solutions instead of matching relative words. As a result, people are more likely to depend on artificial intelligence. However, with the increase of dependence, people start to be concerned about how their information, including information that transfers to the artificial intelligence and the solutions produced by the artificial intelligence, is protected. The training

* Corresponding author: hongdaz1@uci.edu

for artificial intelligence requires numerous amounts of data, so there is probability of leaking and misusing information. And the news about leaking data and hacking frequently occurs which make people pay more attention to the security of artificial intelligence [1, 2]. That is because there could be some private information appearing in the dialogues between users and artificial intelligence, which may relate to their business decisions or even bank accounts. The security of artificial intelligence is not simply defined as how complex the transferred data between servers and clients is encrypted. But it also considers where the information is stored and who has the authority to access the stored data.

The development of artificial intelligence could be largely influenced by those queries regarding security. In order to solve this problem, there is a secure technique that can be considered to deploy——Blockchain. Blockchain, as a technique that is decentralized, has shown a high potential in cybersecurity and privacy protection. In addition, by using smart contract, there could be less probability for artificial intelligence to be modified by hackers. Therefore, the combination of blockchain and artificial intelligence may lead to an increase in user trust, which may allow them to use artificial intelligence and blockchain to assist their business decisions [3].

Nowadays, the development of technology allows people to make large progress in different aspects, like material science, computer science, physics, and so on. Among these fields, the application on economy is one of the most potential fields, that could be benefited by those two techniques. This is because the majority of frequently used blockchains, like Bitcoin, Ethereum, and etc., all receive distinguished feedback on those users. The extremely high value of the "coins" indicates the importance of the blockchain in economic field. Since the blockchain could provide a generally secure way that allows people to trade directly.

This paper focuses on the combination of artificial intelligence and blockchain to serve the economy, which may assist to predict the risk in the trade and protect the privacy of trade content. To be more specific, blockchain has an excellent ability to store, transfer, manage, and verify data, whereas artificial intelligence systems are strong at processing data and making automatic decisions. By combing these two techniques, there could be a boost or a tremendous change in the economy.

The review aims to provide a structured analysis beginning with an introduction to the basics of blockchain and AI integration, focusing on IoT security. It then summarizes methodologies from previous studies on combining AI with blockchain for enhanced data security and threat detection in IoT systems. A discussion follows, evaluating the advantages, applications, and limitations of these approaches, highlighting how AI-integrated blockchain improves accuracy in threat detection and data integrity. The review concludes by affirming the importance of AI-blockchain integration for IoT security, addressing current challenges, and suggesting directions for future research in data security for complex systems.

2 Preliminaries of blockchain and AI

Among all the rapid technological developments, blockchain and AI are two of the hottest innovations molding the future of business and society. In addition, blockchain can provide a decentralized, secure, and transparent framework for processing transactions intermediatory, thus instilling a feeling of trust among participants in all types of transactions. AI empowers machines to emulate human intelligence to make data-driven decisions and automate the most intricate tasks. It means that understanding the very basics of both technologies is important to appreciate how their convergence can solve a set of business challenges. This section outlines basic principles, workflows, key components, advantages, and limitations and also discusses integrated solutions opening up a host of strength leveraged by both blockchain and AI as drivers of innovation and efficiency in business processes.

2.1 Blockchain

Blockchain is a decentralized digital ledger technology that securely and transparently records transactions across multiple computers, eliminating the need for intermediaries by enabling peer-to-peer transactions. The workflow involves several key steps: a user initiates a transaction, which is then broadcast to a network of nodes. These nodes validate the transaction using consensus mechanisms such as Proof of Work or Proof of Stake. Validated transactions are grouped into a block, and the new block is added to the blockchain, becoming a permanent and immutable record.

The major entities that constitute blockchain include nodes, blocks, transactions, consensus mechanisms, and cryptographic hash functions. They are computers that build the network of nodes, blocks are containers holding batches of transactions, transactions mean records of asset transfers, consensus mechanisms are protocols to validate the transactions, whereas cryptographic hash functions ensure data integrity and security. The advantages to blockchain include decentralization, which reduces reliance on central authoritative agents; transparency in that all transactions can be visible to the participants of this network; it is robustly secured through cryptographic techniques against fraudulent activities; and immutable in that data cannot be retroactively altered.

2.2 Artificial intelligence

Artificial Intelligence (AI) refers to the simulation of human intelligence processes by machines, especially computer systems. It enables machines to learn from experience, adapt to new inputs, and perform tasks that typically require human intelligence. The AI workflow involves several key steps: data collection, where relevant information is gathered; data processing, which includes cleaning and organizing data for analysis; model training, where algorithms learn patterns from the data; inference, where the trained model makes predictions or decisions; and a feedback loop, where the model is continuously improved with new data.

The main components of AI include algorithms (sets of rules that guide data processing), machine learning models (systems that improve performance with experience), neural networks (AI models inspired by the human brain's structure), and datasets (large volumes of information for training and testing). AI offers significant advantages: it enhances efficiency by automating complex tasks, improves accuracy by reducing human error in data analysis, provides scalability by effectively handling large datasets, and fosters innovation by enabling new solutions across various fields.

3 Method

3.1 Payment

Blockchain technology has the potential to significantly enhance payment systems by enabling decentralized processes for customer identification and currency exchanges. By using blockchain's distributed ledger, these systems can offer quick, secure, and transparent transaction services. This improvement not only accelerates the speed of mobile payments but also enhances transparency, thereby reducing costs associated with traditional payment methods [4]. The elimination of intermediaries through decentralization leads to a more efficient payment infrastructure, fostering trust among users due to the immutable nature of blockchain records.

Moreover, the implementation of blockchain-based smart contracts offers secure and automated payment services by ensuring that transactions are tamper-proof and immutable.

Smart contracts are self-executing agreements with the terms directly written into code, which automatically enforce contractual clauses without the need for third parties [5]. However, despite their benefits, smart contracts can be vulnerable to coding errors or security flaws, which can lead to significant risks. To address these challenges, AI can be employed to monitor and analyze smart contracts for potential vulnerabilities. AI tools can conduct code audits, detect unusual patterns, and identify potential bugs or loopholes, thereby strengthening the overall security of smart contracts. This initiative-taking approach helps minimize risks of human error and fraud, further enhancing the reliability and efficiency of financial systems that utilize smart contracts. Importantly, blockchain technology holds significant potential to integrate with existing payment systems rather than fully replacing them. This integration allows for added security and automation without disrupting the current financial ecosystem [6]. By augmenting traditional payment infrastructures with blockchain features, financial institutions can enhance transaction security, reduce processing times, and lower operational costs. This collaborative approach ensures that the benefits of blockchain are realized while maintaining the stability and familiarity of established financial practices, leading to a more robust and efficient payment landscape.

In summary, blockchain technology can revolutionize payment systems by enhancing efficiency, security, and transparency. The use of decentralized ledgers, smart contracts, and AI-driven monitoring reduces reliance on intermediaries and mitigates risks associated with traditional payment methods. Integrating blockchain into existing financial infrastructures offers a practical approach to modernizing payment systems without causing disruption, ultimately leading to a more efficient, secure, and trustworthy payment system.

3.2 Supply chain management

Blockchain and AI technologies are significantly enhancing supply chain management by improving financial risk management, data tracking, and operational effectiveness, thereby promoting sustainable growth. The integration of these technologies allows for better analysis of financial risks through real-time data processing and secure transaction records. By providing accurate and timely information, businesses can make informed decisions, mitigate potential risks, and streamline operations, leading to increased efficiency and sustainability in supply chains [7].

In the pharmaceutical industry, the combination of AI and blockchain boosts transparency and security by enabling the traceability of drug products. This integration not only improves customer service by providing consumers with verified information about the origin and handling of medications but also tackles the critical issue of counterfeit drugs. By ensuring that every step in the supply chain is securely recorded and immutable, pharmaceutical companies can safeguard the integrity of their products, comply with regulatory requirements, and build trust with customers and partners [8].

Furthermore, integrating blockchain with the Internet of Things (IoT) in agricultural supply chains ensures a secure, auditable, and transparent record of product movement from farm to table. This synergy improves overall supply chain management by providing real-time tracking of agricultural products, enhancing food safety, reducing waste, and optimizing logistics. The secure data provided by blockchain and IoT technologies enables better decision-making, fosters transparency among all stakeholders, and promotes trust within the supply chain network [9].

By leveraging the combined strengths of AI, blockchain, and IoT, supply chain management across various industries can overcome traditional challenges related to transparency, security, and efficiency. This technological convergence leads to more resilient and sustainable supply chains, benefiting businesses, consumers, and the broader economy.

3.3 Data security

Blockchain technology significantly enhances data security in big data applications, particularly within the Internet of Things (IoT) ecosystem. By utilizing smart contracts, blockchain ensures secure data exchange between devices, preventing unauthorized access and tampering. The immutable and decentralized nature of blockchain records provides a robust framework for securing the vast amounts of data generated by IoT devices, addressing critical challenges related to data integrity and confidentiality [10]. Integrating AI with blockchain further enhances data security in IoT environments. AI can analyse network traffic patterns and detect anomalies that might indicate threats like DDoS attacks, enabling a more responsive and adaptive defence mechanism. For instance, AI models can be used to predict potential vulnerabilities within the blockchain system or identify suspicious activities in real-time, thus allowing for faster mitigation of cyber threats. This AI-enabled threat detection significantly improves the accuracy and efficiency of securing IoT devices, ensuring a robust and proactive approach to data security in cyber-physical systems [11].

Moreover, blockchain networks can incorporate cyber-insurance mechanisms to mitigate risks associated with cyber-attacks such as double spending. By employing game-theoretic approaches, blockchain systems can effectively manage cyber risks by incentivizing secure behaviour among participants and discouraging malicious activities. This integration adds an extra layer of security, ensuring that even if an attack occurs, the financial impact is minimized, and the system's integrity is maintained [12].

Furthermore, the decentralized ledger of blockchain technology improves data security by ensuring immutability and transparency in transaction processes. This feature is especially useful for protecting sensitive data, as it guarantees that once information is recorded on the blockchain, it cannot be altered or deleted. The transparency provided by blockchain allows for easier auditing and verification of data, enhancing trust among stakeholders and reducing the likelihood of data breaches. By safeguarding sensitive information through cryptographic techniques and distributed consensus, blockchain offers a powerful solution for enhancing data security across various applications [13].

By leveraging these capabilities, organizations can address growing concerns over data security in an increasingly connected world. The combination of AI-enabled threat detection, smart contracts, cyber-insurance models, and immutable ledgers within blockchain technology provides a comprehensive approach to protecting data integrity, confidentiality, and availability. This not only strengthens defences against cyber threats but also fosters trust and reliability in digital transactions and data exchanges.

4 Discussion

4.1 Limitations and challenges

A major challenge in using the blockchain with AI is related to the vulnerabilities looming within smart contracts. Even though smart contracts have opened up a world of automated and secure transactions, they can still be attacked when it comes to bugs in coding and security vulnerabilities. These usually tend to be points ignored several times by attacks from malicious hackers, sometimes related to losses of money or, worse, data. While AI can monitor and analyse smart contracts for these weaknesses, their effectiveness depends greatly on the quality of training data and the precision inherent in the models. The ability to have AI systems mine a wide range of potential vulnerabilities with very low false-positive rates is the challenge. Too many false positives stand in the way of operations, reducing real-world reliability.

In a general sense, the integration of AI with blockchain introduces two important challenges: energy demand and secure deployment. First of all, expandability issues arise, especially in large-scale environments, such as IoT networks. The whole decentralized structure of blockchain relies on node consensus for validating the transactions; this causes delays. If combined with the demand of AI for real-time analysis and detection of threats, it can hamper the performance due to an increased need for processing power-the speed of applications that are sensitive, such as payments. Thus, balancing blockchain security with the efficiency of processing that AI needs remain one of the most critical obstacles to Expandability.

Moreover, the compatibility with existing systems is complex and costly, with infrastructures of legacy finance, supply chains, and IoT resisting decentralized blockchain architecture. Transitioning into blockchain demands effort and resources in time, with efforts toward regulatory compliance, especially across diverse standards in different regions, further limiting expandability and adding to deployment complexity. Finally, there are also energy issues to be considered due to the heavy computational load of AI-driven blockchain solutions. Although energy efficiency is one of the prime considerations within industries like IoT, AI analytics and blockchain consensus mechanisms require immense power. Without innovative methods of clearing the extra energy consumption, wide diffusion would seem pretty challenging with environmental considerations growing critical.

Custom AI development also presents a number of challenges, more so on responsibility and security. Determining who shall create AI applications for specific blockchain applications requires immense trust in the developer's technical capability but also in his or her ability to write secure, reliable code. Ensuring AI code is free from security vulnerabilities is key, as any flaw might expose sensitive data or give entry points to malignant attacks. These risks need rigorous security audits, standardized protocols, and regular testing for containment. Setting clear guidelines and accountability on the AI development process remains problematic as this will, per nature, go against the decentralization.

4.2 Future prospects

This merger of AI and blockchain has tremendous benefits for the economic sectors in terms of enhanced security, transparency, and efficiency in general. Artificial intelligence immediately detects threats in real time, so this minimizes fraud cases when combined with the blockchain framework that secures data from breaches in payment systems. AI-driven blockchain in supply chain management optimizes logistical activities, allowing the ability for advanced data analysis that drives wiser decisions and resource management across many sectors. AI-driven anomaly detection for IoT security forms a powerful cybersecurity combination with blockchain's immutable ledger. The resulting synergy will be a resilient IoT ecosystem that covers data integrity and is dynamic in response to emerging security challenges.

In future developments, enhancing model accuracy will be essential to reduce error rates effectively. Advanced training techniques for AI algorithms, such as fine-tuning and transfer learning, can optimize it without overcomplicating the models, which will raise the precision of the prediction significantly. These can allow for smaller ratios of positive and negative false cases to pop up, yielding more reliable insights that could minimize security risks and operational inefficiencies within AI-blockchain applications.

In addition, local deployment of AI reduces operational costs and storage usage. Tuning of model parameters for the local environment enables AI systems to run leaner models that do not consume much computational resources and, of course, storage space. Thus, this customized approach minimizes resource utilization and thereby enhances system response

by reducing latency, hence a feasible approach for scalable deployment in IoT and other distributed networks.

To address energy consumption concerns, the adoption of a consensus mechanism such as the Proof of Stake (PoS) or Proof of Authority (PoA) may be considered viable options. Unlike traditional PoW (Prove of Work), which highly relies on computational intensiveness, PoS and PoA are energy-intensive to a lesser degree and, thus, could get more feasible in the case of large-scale blockchain networks. This ensures robust security, backing an eco-friendly consensus mechanism-a quite significant factor considering environmental sustainability.

Accountability among developers and teams will be well-preserved within well-defined responsibility models in the entire AI-blockchain development cycle. This will also provide a route to keeping up with security standards right at the beginning when clear aspects of roles and responsibilities are communicated in teams. Clearly defining acts of accountability not only assures code integrity but also generates trust among stakeholders. This builds a secure, collaborative environment for deploying advanced technologies.

While there are still significant hurdles, further refinement with AI and blockchain is bound to achieve unthought-of dimensions of efficiency and security. The road ahead will be in overcoming the limitations error rate of artificial intelligence, expandability challenges, difficulties in integrating these technologies into seamless adoption, and problems facing in developing custom artificial intelligences, thus preparing a path for transformational impact across various industries.

5 Conclusion

This paper provides a review of the combination between AI and blockchain, which holds immense promises for a wide array of sectors, right from payment systems to supply chains and IoT-much-needed security, transparency, and above all, efficiency. Real-time analysis capabilities with AI match the immutable and decentralized structure of blockchain to provide an exceptionally strong platform against cyber threats by detecting and mitigating them. However, these are faced by challenges including smart contract vulnerabilities, scalability for performance, and the complexity of integration with incumbent systems. Overcoming all these indeed needs further development in the development of models of AI, optimization of processes of blockchains in their decentralized nature, and finally the development of integration ways of smoothing into legacy systems. The evident challenges notwithstanding, the shared strengths of AI and blockchain raise a promising way toward digital infrastructures that are resilient and adaptive. With further research and innovation, this integration has the potential to fully revolutionize data security and operational efficiency, thus offering a balanced approach toward modernizing digital systems while ensuring their reliability and trustworthiness in an increasingly interconnected world.

References

1. IT Governance. In 2023, over 8.2 billion records were breached globally, including significant incidents like the Indian Council of Medical Research (ICMR) breach, which exposed over 815 million records. IT Governance. Retrieved from https://www.itgovernance.co.uk (2023).
2. Varonis. In the five years from 2017 to 2022, the number of healthcare data records breached in the U.S. rose from 5.3 million to 51.4 million. Varonis. Retrieved from https://www.varonis.com (2024).

3. B. K. Amrutha & B. Gomathy. Blockchain Integration in Artificial Intelligence: Benefits, Applications, Research Challenges. IJFMR, 5(6) (November-December 2023).
4. Y. Mohamed Adil. Intelligent Blockchain-Based Secure Framework for Transaction in Mobile Electronic Payment System. Int. J. Interact. Mob. Technol. (iJIM), 17(04), 37–46. https://doi.org/10.3991/ijim.v17i04.37671 (2023).
5. M. Sholeh, E. Y. Talahaturuson, M. Rizqi & A. B. Gumelar. Designing an Ethereum-based Blockchain for Tuition Payment System using Smart Contract Service. J. RESTI (Rekayasa Sistem Dan Teknologi Informasi), 6(2), 275-280 (2022).
6. A. A. Sitnik. Blockchain Technology in Payment Systems. Actual Problems of Russian Law, 16(5), 42-54 (2021).
7. K. Nethravathi, A. Tiwari, D. Uike, R. Jaiswal & K. Pant. Applications of Artificial Intelligence and Blockchain Technology in Improved Supply Chain Financial Risk Management. In: 2022 5th Int. Conf. on Contemp. Comput. and Informatics (IC3I), Uttar Pradesh, India, pp. 242-246 (2022).
8. S. D'souza, D. Nazareth, C. Vaz & M. Shetty. Blockchain and AI in Pharmaceutical Supply Chain. In: Proceedings of the Int. Conf. on Smart Data Intelligence (ICSMDI) (2021). Available at SSRN: https://ssrn.com/abstract=3852034.
9. Y. Farooqui & S. M. Parikh. Secure and Transparent Supply Chain Management using Blockchain and IoT. Int. J. on Recent Innov. Trends in Comput. Commun., 11(11s), 01–12. https://doi.org/10.17762/ijritcc.v11i11s.8064 (2023).
10. N. Nahar, F. Hasin & K. A. Taher. Application of Blockchain for the Security of Decentralized Cloud Computing. In: 2021 Int. Conf. on Information and Communication Technology for Sustainable Development (ICICT4SD), Dhaka, Bangladesh, pp. 336-340 (2021).
11. S. Wang, J. Zhang & T. Zhang. AI-enabled blockchain and SDN-integrated IoT security architecture for cyber-physical systems. Adv. Control Appl.: Eng. Ind. Syst., 6(2), e131 (2024).
12. S. Feng, Z. Xiong, D. Niyato, P. Wang, S. S. Wang & Y. Zhang. Cyber Risk Management with Risk Aware Cyber-Insurance in Blockchain Networks. In: 2018 IEEE Global Commun. Conf. (GLOBECOM), Abu Dhabi, UAE, pp. 1-7 (2018).
13. A. Jain, A. Kumar Tripathi, N. Chandra & P. Chinnasamy. Smart Contract enabled Online Examination System Based in Blockchain Network. In: 2021 Int. Conf. on Comput. Commun. Informatics (ICCCI), Coimbatore, India, pp. 1-7 (2021).