# Integrating Blockchain with Large Language Models: A Comprehensive Systematic Investigation of Security, Optimization and Interoperability

Jinghao Hu

*School of Computing and Communications, Lancaster University, Lancaster, United Kingdom*

evan.huedu@gmail.com

**Abstract.** Blockchain technology, characterized by decentralization, transparency, and robust security, has garnered extensive attention across various sectors. Concurrently, Large Language Models (LLMs), particularly the Generative Pre-trained Transformer (GPT) series, have shown promising capabilities in enhancing blockchain security, transaction anomaly detection, and smart contract optimization. This paper systematically reviews recent advancements integrating blockchain technology with LLMs, focusing on applications related to consensus mechanism security, anomaly detection, smart contract auditing, and cross-chain interoperability. The analysis highlights critical limitations, including the interpretability challenges of LLMs, real-time processing bottlenecks, data privacy risks, and inadequate generalization across diverse blockchain platforms. Future research directions suggested include adopting explainable AI (XAI) techniques to enhance transparency, developing lightweight models to improve scalability, utilizing federated learning to protect data privacy, and exploring cross-domain transfer learning and meta-learning to boost generalization capabilities. This comprehensive review aims to clarify current developments, identify prevailing gaps, and provide valuable insights for future research on effectively integrating blockchain with LLM technologies.

## INTRODUCTION

Blockchain technology, characterized by decentralization, transparency, immutability, and robust security, has emerged as a transformative force across various sectors, including finance, healthcare, supply chain management, and data privacy protection. At its core, blockchain establishes trust in decentralized networks without relying on centralized authorities, significantly enhancing data integrity and transaction transparency [1, 2]. Concurrently, recent years have witnessed remarkable advancements in Large Language Models (LLMs), exemplified by the Generative Pre-trained Transformer (GPT) series [3, 4]. These models have demonstrated extraordinary capabilities in natural language processing, anomaly detection, and intelligent decision-making tasks, showcasing immense potential for interdisciplinary applications.

Recently, the intersection of blockchain technology and large language models has begun to garner significant attention within academic and industry circles. Researchers have actively explored integrating these advanced Artificial Intelligence (AI) models into blockchain systems to address existing technological challenges and open up novel application scenarios. For instance, He et al. systematically reviewed LLMs' applications for blockchain security, identifying their roles in enhancing smart contract auditing, anomaly detection in blockchain transactions, and automatic vulnerability remediation [3]. Similarly, Geren et al. proposed a holistic classification framework termed "BC4LLMs," emphasizing blockchain's potential to improve LLMs' security and safety by providing decentralized trust and verification mechanisms [5]. Luo et al. proposed another LLM-based framework, specifically exploring the integration of blockchain and large language models to enhance the trustworthiness of artificial intelligence systems through improved data authenticity and privacy protection [4]. Furthermore, Gai et al. developed a specialized tool named "BlockGPT," which utilizes large language models for detecting anomalies in blockchain transactions in real-time, notably improving both the efficiency and accuracy of transaction monitoring [6]. Despite these promising advancements, the current research landscape remains fragmented, with limited comprehensive reviews and comparative analyses available.

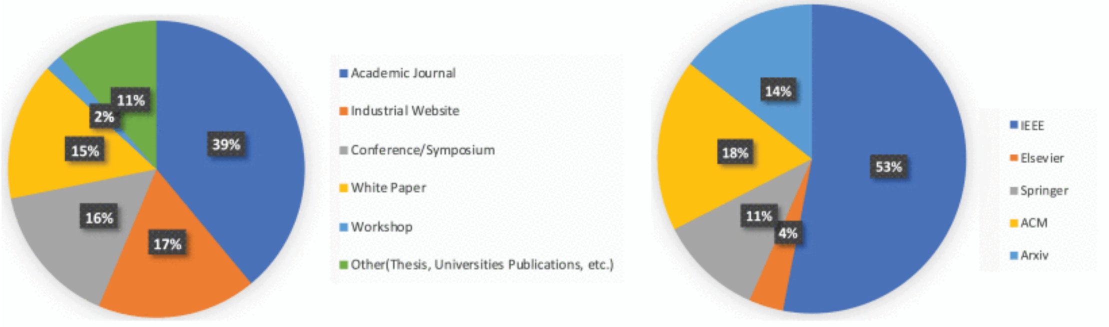
Given the rapid yet fragmented developments in integrating blockchain technology with large language models, this review aims to provide a comprehensive analysis and summary of existing literature. The motivation behind this research is to synthesize recent advancements, critically evaluate existing methodologies, identify prevalent gaps, and suggest promising future research directions within this emerging interdisciplinary domain. The remainder of this paper is organized as follows: Section 2 offers foundational insights into blockchain and large language models, providing readers with essential technical knowledge. Section 3 systematically reviews recent advancements in integrating LLMs within blockchain contexts, specifically emphasizing applications in blockchain security enhancement, smart contract optimization, and transaction anomaly detection. Section 4 provides a critical discussion, analyzing current research limitations, assessing unresolved challenges, and exploring potential future directions. Finally, Section 5 concludes this review by summarizing key findings, highlighting the significance of blockchain-LLM integration, and underscoring future research opportunities in this dynamic and evolving field.

# PRELIMINARIES OF BLOCKCHAIN AMD LARGE LANGUAGE MODLES

## Blockchain

Blockchain technology, defined as a decentralized digital ledger, ensures transparency, data integrity, and immutability without relying on centralized authorities [3]. By adopting consensus mechanisms and cryptographic algorithms, blockchain enables secure, verifiable, and tamper-proof transactions, greatly enhancing trust within distributed networks [5]. Its core features have driven transformative applications across diverse sectors such as finance, healthcare, and supply chain management [4].

The overall framework of blockchain typically consists of three fundamental components: blocks, nodes, and consensus mechanisms (Figure 1). Each block comprises a set of transactions and cryptographic hashes, securely linked to form an immutable chain [5]. Transactions within a blockchain undergo verification by distributed network nodes through consensus protocols such as Proof-of-Work (PoW), Proof-of-Stake (PoS), or Byzantine Fault Tolerance (BFT), ensuring transaction validity and preventing malicious alterations [4]. The validated blocks are then broadcasted and added to the chain, maintaining network synchronization and security.



(a) Invevstigated resources on consensus algorithms (b) Academic articles on consensus algorithms

**FIGURE 1.** Distribution of literature sources [2].

Blockchain technology exhibits several critical features, notably decentralization, transparency, immutability, and robust security. Decentralization eliminates single points of failure by distributing data across numerous nodes, thus significantly enhancing system resilience [3]. Transparency ensures that transactions are publicly verifiable, promoting trust among participants. Moreover, blockchain's immutability guarantees that once recorded, data cannot be modified retroactively, greatly enhancing data integrity [6]. These distinctive attributes facilitate its widespread adoption in various fields, including secure IoT systems, smart contract management, and anomaly detection in financial transactions [6, 7].

## Large Language Models

Large language models, exemplified by transformer-based models such as the GPT series, are advanced artificial intelligence systems designed primarily for Natural Language Processing (NLP) tasks [1]. These models utilize deep neural networks, particularly self-attention mechanisms, to efficiently handle large-scale textual data, significantly improving performance in text generation, sentiment analysis, and conversational AI applications [8]. Due to their powerful generalization capabilities, LLMs are capable of few-shot learning, enabling them to perform diverse NLP tasks with minimal additional training.

The core framework of large language models typically involves two main phases: pre-training and fine-tuning. In the pre-training phase, LLMs learn linguistic patterns and contextual relationships from massive unsupervised textual datasets. Subsequently, during the fine-tuning phase, these models are adapted to specific downstream tasks using supervised learning techniques [3] (Figure 2). Central to their architecture are embedding layers, self-attention blocks, and feed-forward neural networks, which collectively facilitate the understanding and generation of coherent text [5].

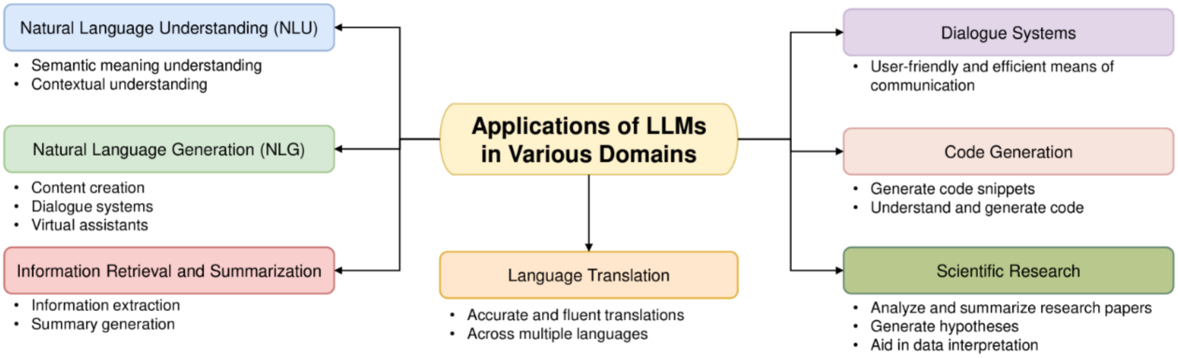

Applications of LLMs in Various Domains
Natural Language Understanding (NLU)
• Semantic meaning understanding
• Contextual understanding
Natural Language Generation (NLG)
• Content creation
• Dialogue systems
• Virtual assistants
Information Retrieval and Summarization
• Information extraction
• Summary generation
Language Translation
• Accurate and fluent translations
• Across multiple languages
Dialogue Systems
• User-friendly and efficient means of communication
Code Generation
• Generate code snippets
• Understand and generate code
Scientific Research
• Analyze and summarize research papers
• Generate hypotheses
• Aid in data interpretation

**FIGURE 2.** Application domains of large language models in blockchain security [3].

Large Language Models exhibit prominent features such as strong generalization capabilities, efficient handling of large-scale textual datasets, and adaptability to diverse application contexts. These distinctive characteristics have enabled LLMs to excel in numerous real-world applications, including automated anomaly detection, advanced conversational agents, and intelligent decision-making tasks in complex environments [8]. Recent advancements also demonstrate promising integration of LLMs with blockchain technology, providing enhanced security and real-time anomaly detection in blockchain-based systems [6].

# METHOD

## Consensus Mechanism

Security Consensus mechanisms are crucial in blockchain's ability to maintain decentralized agreement among nodes, ensuring network integrity and data consistency. However, as these mechanisms evolve in complexity, they become increasingly susceptible to sophisticated attacks and manipulation, necessitating innovative security enhancements.

He et al. conducted a systematic literature review, highlighting existing research that leverages large language models (LLMs) for smart contract security auditing [3]. Their review discusses approaches involving GPT models for performing multi-layered semantic inspections, beginning with scans for syntactic irregularities followed by deep analysis of contract logic to accurately identify vulnerabilities. The review indicates that such automated and comprehensive auditing methodologies can significantly reduce manual efforts, minimize false positives, and enhance detection accuracy.

Similarly, Luo et al. introduced the BC4LLM approach, integrating blockchain trust mechanisms with GPT-based trusted artificial intelligence systems [4]. This framework strengthens consensus mechanism security by improving validation processes and enabling sophisticated anomaly detection. BC4LLM effectively combines AI-driven semantic insights with blockchain's cryptographic security, thereby ensuring transaction authenticity and network reliability.

## Anomaly Detection in Blockchain

Blockchain transactions involve critical financial and informational exchanges, making timely anomaly detection essential to prevent substantial economic and operational risks. Traditional methods often struggle with scalability and real-time detection due to their limited semantic analysis capabilities.

Gai et al. developed the "BlockGPT" tool, employing GPT-based LLMs for effective real-time anomaly detection [6]. BlockGPT uses a two-phase process: first, it establishes a robust semantic model trained on historical transaction data, and second, it continuously compares live transactions against this model to instantly flag irregularities. This semantic approach significantly enhances anomaly detection speed and reduces fraudulent activities.

In a similar vein, Geren et al. proposed a comprehensive security framework named BC4LLMs, integrating LLMs within blockchain systems [5]. This framework leverages advanced semantic analysis capabilities of LLMs to continuously monitor transactions, swiftly identifying and alerting users of anomalies. Consequently, BC4LLMs significantly improves anomaly detection effectiveness, reinforcing blockchain security management.

## Smart Contract Security and Optimization

Smart contracts, automated agreements encoded on blockchain platforms, manage assets worth billions of dollars. However, vulnerabilities such as re-entrancy attacks and integer overflow errors can cause severe financial losses, highlighting the need for advanced detection and remediation techniques.

To address these vulnerabilities, Kushwaha et al. investigated the progress of employing LLMs for systematic analysis of smart contract security [9]. Their review discusses GPT-based semantic modeling approaches that have been used in existing research to deeply inspect smart contract code and proactively detect subtle vulnerabilities. Through iterative semantic learning, the model refines its capabilities, surpassing traditional static analysis tools by reducing manual effort and significantly improving vulnerability detection accuracy.

## Cross-chain Interoperability and Privacy Enhancement

Cross-chain interoperability and privacy protection are essential for secure and seamless data and asset exchanges across heterogeneous blockchain networks. Nevertheless, achieving these simultaneously poses significant technical challenges due to diverse protocols, consensus mechanisms, and stringent data privacy regulations.

Addressing these complexities, Yang et al. proposed a novel integration of blockchain technology with artificial intelligence, utilizing GPT-based large language models (LLMs) [8]. Their framework leverages AI's semantic capabilities to create intelligent semantic interoperability bridges between distinct blockchain networks. This method ensures secure and efficient cross-chain transactions and significantly enhances data privacy through advanced AI-driven privacy preservation techniques.

Further expanding on scalability and privacy, Rao et al. emphasized the use of AI models to improve blockchain scalability and privacy mechanisms [10]. Their approach integrates zero-knowledge proofs (ZKP) with advanced AI semantic modeling, offering a robust solution for secure, scalable, and private blockchain transactions.

# DISCUSSION

## Limitations and Challenges

In the integration of blockchain technology with LLMs, several limitations and challenges arise, impacting the technology's security, efficiency, and broader applicability. The primary challenges include:

Interpretability Limitations: The "black box" nature of large language models significantly limits the transparency and interpretability of their decision-making processes. Specifically, the opaque internal logic of LLMs reduces the reliability and security of blockchain technology. This lack of transparency complicates the auditing of smart contracts or blockchain transactions, making it difficult to accurately identify and mitigate potential risks, thus increasing the likelihood of financial losses and security vulnerabilities [3, 4].

Real-time and Scalability Challenges: Although LLMs possess robust data processing capabilities, they encounter substantial efficiency bottlenecks when handling real-time data streams and extensive blockchain transactions. These models often require considerable inference time, failing to meet the blockchain networks' demands for instant transaction validation and confirmation. Consequently, this reduces the response speed and scalability of blockchain transaction systems, restricting their practical applicability in large-scale deployment scenarios [6, 10].

Data Privacy and Security Risks: Large language models typically require extensive user data for training and operational analysis, raising the risk of data leakage. In applications combining blockchain and LLMs, sensitive user information might be inadvertently exposed or compromised, particularly during cross-chain transactions or data exchanges, exacerbating privacy concerns. Additionally, the complexity arising from diverse data sources and regulatory environments involved in cross-chain operations further intensifies the challenges associated with privacy protection and security management [8, 10].

Lack of Generalization Capability: Current large language models are primarily optimized on specific training datasets, leading to insufficient generalization performance across various blockchain platforms or specialized application scenarios. The accuracy and effectiveness of these models may significantly decrease when dealing with diverse blockchain architectures and transaction data. Therefore, deploying models across platforms or different application contexts presents significant adaptability challenges, limiting their generality and widespread usability [2, 7].

## Future Prospects

In response to the identified limitations and challenges, several potential solutions and future research directions can be explored:

Enhancements for Interpretability Limitations: The introduction of Explainable AI (XAI) technologies can significantly improve the transparency and interpretability of blockchain security audits and decision-making processes. XAI methodologies allow for clearer understanding and insights into LLM decision mechanisms, reducing uncertainty and risk in blockchain operations, particularly for smart contract verification and transaction validation [3, 4].

Real-time and Scalability Improvement Solutions: Future research should focus on developing lightweight LLM models or integrating edge computing technologies to enhance real-time processing capabilities. Leveraging edge computing can minimize latency and increase throughput, thereby addressing scalability bottlenecks and improving the efficiency of blockchain transaction systems in large-scale, real-time operational environments [6, 10].

Data Privacy and Security Protection Techniques: To protect sensitive data within blockchain networks, adopting technologies such as Federated Learning is recommended. Federated Learning provides robust privacy-preserving solutions by enabling distributed model training without exposing the underlying raw data, effectively preventing user data leaks. This approach is particularly beneficial in complex cross-chain interactions and stringent regulatory environments, where maintaining user confidentiality is paramount [8].

Strategies to Enhance Generalization Capability: Future research could benefit from focusing on cross-domain transfer learning and meta-learning techniques (domain adaptation, domain generalization). These methodologies aim to enhance the generalization capabilities of LLMs across different blockchain platforms and application scenarios, thereby improving their adaptability and reliability in diverse operational contexts [2].

## CONCLUSION

This paper provided a comprehensive review of recent advancements in the integration of blockchain technology with LLMs, highlighting the latest research developments across several crucial application domains. Specifically, the review investigated essential areas including consensus mechanism security, anomaly detection in blockchain transactions, smart contract optimization, and cross-chain interoperability with enhanced privacy.

Methodologically, the paper systematically analyzed existing literature to evaluate how LLMs have been employed to address specific challenges in blockchain technology. These included the security auditing of consensus mechanisms, real-time anomaly detection, optimization and security enhancements of smart contracts, and improvements in cross-chain data privacy and interoperability.

The key findings identified several significant limitations and challenges, such as interpretability constraints, real-time processing and scalability bottlenecks, data privacy concerns, and insufficient generalization capabilities of existing LLM models. These issues significantly impact blockchain's reliability, security, operational efficiency, and broader applicability.

For future research, this paper recommends further exploration into advanced methodologies, including XAI to improve transparency, lightweight and edge computing solutions for real-time scalability, Federated Learning to protect sensitive data, and cross-domain transfer learning or meta-learning to enhance model generalization. Such advancements could substantially strengthen the integration of blockchain with artificial intelligence, ensuring robust, scalable, and secure applications.

## REFERENCES

1. M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, and M. A. Hanif, “A survey on blockchain technology: Evolution, architecture and security,” IEEE Access 9, 61048–61073 (2021).
2. B. Lashkari and P. Musilek, “A comprehensive review of blockchain consensus mechanisms,” IEEE Access 9, 43620–43652 (2021).
3. Z. He, Z. Li, S. Yang, A. Qiao, X. Zhang, X. Luo, and T. Chen, “Large language models for blockchain security: A systematic literature review,” arXiv preprint arXiv:2403.14280 (2024).
4. H. Luo, J. Luo, and A. V. Vasilakos, “BC4LLM: Trusted artificial intelligence when blockchain meets large language models,” arXiv preprint arXiv:2310.06278 (2023).
5. C. Geren, A. Board, G. G. Dagher, T. Andersen, and J. Zhuang, “Blockchain for large language model security and safety: A holistic survey,” arXiv preprint arXiv:2407.20181 (2024).
6. Y. Gai, L. Zhou, K. Qin, D. Song, and A. Gervais, “Blockchain large language models,” arXiv preprint arXiv:2304.12749 (2023).
7. S. Kayikci and T. M. Khoshgoftaar, “Blockchain meets machine learning: A survey,” J. Big Data 11, Article No. 9 (2024).
8. Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, “Fusing blockchain and AI with Metaverse: A survey,” IEEE Open J. Comput. Soc. 3, 122–136 (2022).
9. S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, “Systematic review of security vulnerabilities in Ethereum blockchain smart contract,” IEEE Access 10, 6605–6621 (2022).
10. I. S. Rao, M. L. M. Kiah, M. M. Hameed, and Z. A. Memon, “Scalability of blockchain: A comprehensive review and future research direction,” Cluster Comput. 27, 5547–5570 (2024).