Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2024.059318

EDITORIAL

Introduction to the Special Issue on the Bottleneck of Blockchain Techniques Scalability, Security and Privacy Protection

Shen Su[1,*], Daojing He[2] and Neeraj Kumar[3]

[1]Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, 510006, China

[2]School of Computer Science and Technology, Harbin Institute of Technology (Shenzhen), Shenzhen, 518055, China

[3]Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala, 147004, India

*Corresponding Author: Shen Su. Email: sushen@gzhu.edu.cn

Received: 04 October 2024 Accepted: 14 October 2024 Published: 31 October 2024

Blockchain technology has been extensively studied over the past decade as a foundation for decentralized information-sharing platforms due to its promising potential. Despite the success of existing blockchain architectures like Bitcoin, Ethereum, Filecoin, Hyperledger Fabric, BCOS, and BCS, current blockchain applications are still quite limited. Blockchain struggles with scenarios requiring high-speed transactions (e.g., online markets) or large data storage (e.g., video services) due to consensus efficiency limitations. Security restrictions pose risks to investors in blockchain-based economic systems (e.g., DeFi), deterring current and potential investors. Privacy protection challenges make it difficult to involve sensitive data in blockchain applications.

To address these bottlenecks, blockchain architectures need improved scalability, security, and privacy protection. For better transaction performance, current research directions include improving the consensus mechanism, sharding the blockchain network and transaction system, proposing transactions in batches (layer-2) or in parallel, and promoting interoperability. For better data storage capability, researchers mainly focus on on-chain and off-chain collaborative storage and storage provability. For better security protection, researchers reinforce the theoretical foundation of cryptographic technology, monitor and detect potential attacking threats in real-time, and conduct code audits and vulnerability mining on smart contracts. For better privacy protection, researchers involve homomorphic encryption, zero-knowledge proofs, MPC, and federated learning techniques in blockchain architecture.

After the call for papers, all submissions were reviewed by at least three experts, and 11 high-quality papers were accepted for this special issue. Below is a brief analysis of the published papers:

In [1], the authors studied deep learning-based methods for smart contract vulnerability detection. They first provided a brief overview of common vulnerability types in smart contracts. They then categorized and reviewed current deep learning-based tools for smart contract detection, classifying them based on their open-source status, data format, and feature extraction methods. They conducted a comparative analysis of these tools, selecting representative ones for experimental validation and comparing them with traditional tools in terms of detection coverage and accuracy. Based on their experimental results and the current state of research, they proposed a reference standard for developers of contract vulnerability detection tools. Additionally, they suggested forward-looking research directions for deep learning-based smart contract vulnerability detection.

In [2], the authors proposed a graph-based sharding scheme for public blockchain to improve transaction capacity and scalability. They first outlined the challenges of blockchain technology, particularly in transaction performance and scalability, which hinder its widespread adoption. Then They identified the main issues with current sharding mechanisms, namely excessive cross-shard transactions and uneven shard workloads. Their proposed graph-based sharding scheme aims to efficiently balance transaction distribution, mitigate cross-shard transactions, and even out workloads among shards. The authors conducted experiments to validate their approach, demonstrating that their scheme effectively reduces the cross-shard transaction ratio to 35%–56% and decreases transaction confirmation latency to 6 s in a blockchain with up to 25 shards.

In [3], the authors comprehensively explored the NFT ecological process and its associated security issues. They first outlined the rapid growth of the NFT market, highlighting the significant trading volume of $55.5 billion in 2022. Then, they identified the lack of academic research on NFT security as a critical gap. They divided the NFT life cycle into five stages and elaborated on the security issues at each stage. A novel matrix model was proposed to categorize NFT security issues. To substantiate their claims, the authors collected diverse data from social networks, the Ethereum blockchain, and NFT markets. Using this comprehensive dataset, they identified and analyzed nine key NFT security issues qualitatively and quantitatively. The study's significance lies in its thorough examination of NFT ecosystem security, emphasizing the need for increased attention and proactive measures to protect NFT holders and their digital assets.

In [4], the authors proposed a novel blockchain-based certificateless bidirectional authenticated searchable encryption model for cloud email systems named CL-BSE. They described the limitation of traditional email systems, which only allow one-way communication in terms of email searching. They developed a new model that combines cloud server storage with email server communication functions. This model enables data receivers and owners to search for relevant content using their trapdoors. They incorporated dual authentication functions: one for data owners during encryption and another using blockchain for identity verification. The authors formally defined CL-BSE and formulated a specific scheme based on their new system model. They analyzed the scheme's security using a formalized security model, demonstrating that it achieves multi-keyword ciphertext indistinguishability and multi-keyword trapdoor privacy against any adversary. Additionally, they conducted performance evaluations, comparing their scheme with existing ones to show its superior computational and communication efficiency.

In [5], the authors proposed a novel Encode-and CRT-based Scalability Scheme (ECSS) to address blockchain scalability challenges. They first identified the main issues hindering blockchain's broad-scale application, including reduced broadcast efficiency, increased communication overhead, and high storage costs. They developed ECSS, which categorizes nodes into distinct domains to reduce network diameter and enhance transmission efficiency. They implemented a compact block protocol and RS coding to streamline block transmission, reducing broadcast block size while maintaining reliability. Additionally, they utilized the Chinese remainder theorem to compress block bodies and map them to multiple modules for efficient storage. The authors established an experimental platform to evaluate ECSS's performance, conducting comprehensive assessments. Their empirical results demonstrated that ECSS achieves superior network scalability and stability, reducing communication overhead by 72% and total storage costs by 63.6%.

In [6], the authors proposed a novel decentralized reputation management mechanism for permissioned blockchain networks, addressing the limitations of traditional Proof of Authority (PoA) consensus. They first identified the main drawbacks of PoA, including centralization and

lack of anonymity due to the round-robin block proposal mechanism. The authors developed a two-part solution: an off-chain reputation evaluation and an on-chain reputation-aided consensus. They designed a method to evaluate nodes' reputations in blockchain networks and make it globally verifiable through smart contracts. Building upon traditional PoA, they proposed a reputation-aided PoA (rPoA) consensus that incentivizes nodes to form committees based on reputation authority, preventing block generation from being tracked. Additionally, they developed a reputation-aided fork-choice rule to promote network liveness. The authors conducted experiments to validate their approach, demonstrating that rPoA achieves higher security performance while maintaining transaction throughput compared to traditional PoA.

In [7], the authors proposed a novel Bitcoin address identification scheme based on joint multi-model prediction using address-entity mapping relationships. They expounded on the importance of identifying services operated by Bitcoin addresses for risk assessment and analysis. The authors developed a two-part solution: (1) extracting valuable features from given addresses for multi-class service identification and (2) implementing a joint prediction scheme for multiple learners based on address-entity mapping relationships. Their method involves performing address classification and entity clustering tasks separately, followed by graph-based maximization consensus. The authors conducted tests and evaluations on over 26,000 Bitcoin addresses to validate their approach. Their feature extraction method captured more useful features compared to existing approaches. The combined multi-learner model achieved an accuracy of 77.4%, surpassing the baseline classifier.

In [8], the authors proposed a secure and efficient certificateless signing scheme for electricity carbon quota trading based on blockchain technology. They first identified the vulnerabilities of carbon emission quotas in the electricity trading market, such as data forgery and tampering. Then, they developed a new certificateless signature scheme to address the security flaws in existing methods. Building upon this, they proposed an electricity carbon quota trading scheme that combines certificateless signatures with blockchain technology. Their approach ensures transaction validity and non-repudiation through certificateless signatures while achieving immutability and traceability via blockchain. The authors designed their scheme to validate transactions without requiring time-consuming bilinear pairing operations. They conducted a security analysis, demonstrating that their scheme achieves existential unforgeability under adaptive selective message attacks, provides conditional identity privacy protection, and resists replay attacks. Additionally, they evaluated their scheme's computational and communication performance, showing high efficiency.

In [9], the authors introduced NodeHunter, an Ethereum network detector that uses simulation technology to aggregate node records and their interconnections within the network. They highlighted the importance of Ethereum's peer-to-peer network and data-sharing protocol in ensuring the security of smart contracts. The authors developed NodeHunter to provide more comprehensive insights for network status analysis than previous detection methods. They conducted a three-month continuous surveillance of the Ethereum network using NodeHunter, collecting over two million node records and more than one hundred million node acquaintances. Their analysis of the gathered data revealed a significant security concern: approximately 49% or more of the node records were maliciously forged.

In [10], the authors proposed a novel approach combining lightweight blockchain technology with the Internet of Things (IoT) and homomorphic encryption. The authors first described the potential of blockchain technology in addressing centralized system challenges and the transformative impact of IoT on the Fourth Industrial Revolution. They then developed a lightweight blockchain solution to reduce IoT systems' computational burden and integration time. They incorporated the Okamoto Uchiyama encryption algorithm, known for its homomorphic properties, to enhance the privacy

and security of IoT-generated data. Integrating homomorphic encryption and blockchain technology creates a secure, decentralized platform for storing and analyzing sensitive supply chain data. This approach enables the development of new business models and allows decentralized applications to perform computations on encrypted data while maintaining privacy. The authors validated their system's security, demonstrating that it is comparable to standard blockchain implementations while benefiting from the unique homomorphic attributes of the Okamoto Uchiyama algorithm and the efficiency of the lightweight blockchain.

In [11], the authors proposed a blockchain-based mathematical model for multiple microgrids and microgrid aggregators' revenue in the context of distributed renewable energy. The authors highlighted the growing importance of distributed renewable energy in the deteriorating global environment and the potential of blockchain technology in achieving efficient energy consumption and multi-party supply. They developed a model incorporating microgrid users' electricity preferences, increasing their reliance on the blockchain market. They applied the one-master-multiple-slave Stackelberg game theory to determine the optimal energy dispatching strategy when each market entity pursues maximum revenue. The authors conducted simulations to validate their approach, demonstrating that their blockchain-based dynamic game model for the multi-microgrid market effectively increases the revenue of both microgrids and aggregators while improving renewable energy utilization.

Funding Statement: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Wang Z, Wang C, Wu W, Sun C, Wu Z. A blockchain-based game approach to multi-microgrid energy dispatch. Comput Model Eng Sci. 2024;138(1):845–63. doi:10.32604/cmes.2023.029442.
2. Yang X, Diao R, Liu T, Wen H, Wang C. Electricity carbon quota trading scheme based on certificateless signature and blockchain. Comput Model Eng Sci. 2024;138(2):1695–712. doi:10.32604/cmes.2023.029461.
3. Liu Y, Lin Z, Zhang Y, Jiang L, Wang X. "Half of the node records are forged?": the problem of node records forgery in ethereum network. Comput Model Eng Sci. 2024;138(2):1713–29. doi:10.32604/cmes.2023.030468.
4. Mohammed A, Wahab H. Enhancing IoT data security with lightweight blockchain and Okamoto Uchiyama homomorphic encryption. Comput Model Eng Sci. 2024;138(2):1731–48. doi:10.32604/cmes.2023.030528.
5. Zhang L, Zhang J, Toyoda K, Liu Y, Qiu J, Tian Z, et al. A bitcoin address multi-classification mechanism based on bipartite graph-based maximization consensus. Comput Model Eng Sci. 2024;139(1):783–800. doi:10.32604/cmes.2023.043469.
6. Sun Q, Bai F. An encode-and CRT-based scalability scheme for optimizing transmission in blockchain. Comput Model Eng Sci. 2024;139(2):1733–54. doi:10.32604/cmes.2023.044558.
7. Chen J, Shi L, Huang Q, Wang T, He D. On designs of decentralized reputation management for permissioned blockchain networks. Comput Model Eng Sci. 2024;139(2):1755–73. doi:10.32604/cmes.2023.046826.
8. Sun Y, Du X, Niu S, Yang X. Blockchain-based certificateless bidirectional authenticated searchable encryption scheme in cloud email system. Comput Model Eng Sci. 2024;139(3):3287–310. doi:10.32604/cmes.2023.043589.

9. Liao P, Liu C, Yin J, Wang Z, Cui X. NFT security matrix: towards modeling NFT ecosystem threat. Comput Model Eng Sci. 2024;139(3):3255–85. doi:10.32604/cmes.2024.043855.
10. Xu S, Wang Z, Wang L, Mihaljević M, Zhang S, Shao W, et al. A sharding scheme based on graph partitioning algorithm for public blockchain. Comput Model Eng Sci. 2024;139(3):3311–27. doi:10.32604/cmes.2023.046164.
11. Wu H, Peng Y, He Y, Fan J. A review of deep learning-based vulnerability detection tools for ethernet smart contracts. Comput Model Eng Sci. 2024;140(1):77–108. doi:10.32604/cmes.2024.046758.