electronics

MDPI

Editorial

Security, Privacy, Confidentiality, and Trust in the Blockchain: From Theory to Applications

Mikolaj Karpinski [1,2,*], Oleksandr Kuznetsov [3,4,5,*] and Roman Oliynykov [6,7]

1 Department of Software Engineering, University of the National Education Commission, 30-084 Krakow, Poland
2 Department of Cybersecurity, Ternopil Ivan Puluj National Technical University, 46001 Ternopil, Ukraine
3 Department of Cybersecurity of Information Systems, Networks and Technologies, V.N. Karazin Kharkiv National University, 61022 Kharkiv, Ukraine
4 Department of Political Sciences, Communication and International Relations, University of Macerata, Via Crescimbeni, 62100 Macerata, Italy
5 Department of Theoretical and Applied Sciences, eCampus University, Via Isimbardi 10, 22060 Novedrate, Italy
6 Input Output (IOG Singapore Pte Ltd.), 4 Battery Road, Singapore 049908, Singapore; roman.oliynykov@iohk.io
7 Education and Research Institute of Computer Sciences and Artificial Intelligence, V.N. Karazin Kharkiv National University, 61022 Kharkiv, Ukraine
* Correspondence: mikolaj.karpinski@uken.krakow.pl (M.K.); oleksandr.kuznetsov@uniecampus.it (O.K.)

1. Introduction

From the financial and medical sectors to various supply chains, most industries have seen a sea change due to the blockchain [1,2]. This transformation poses unparalleled challenges regarding security, privacy, and trust. The decentralized nature of blockchain systems leads to complex security considerations that the incoming solution package needs to address innovatively [3,4].

Recent developments in blockchain applications have pointed to several critical challenges [5–7]: security vulnerability in smart contracts, leakage in the privacy of transaction data, and several attack vectors on consensus mechanisms. Integrating the blockchain with emerging technologies such as the Internet of Things (IoT) and artificial intelligence further aggravates these challenges and has created urgent requirements for efficient security frameworks and privacy preservation mechanisms.

This Special Issue, "Security, Privacy, Confidentiality, and Trust in the Blockchain", addresses the pressing challenges that have arisen with regard to this technology. This Special Issue of *Electronics* brings together recent research contributions related to the theoretical foundations and practical applications of blockchain security. The collected works span several domains, from advanced cryptographic primitives to real-world blockchain applications in underwater communications and autonomous systems.

The papers in this Special Issue introduce new approaches to the enhancement of the security and privacy of blockchains, ranging from NTRU-based encryption schemes to smart contract vulnerability detection methods and novel applications of zero-knowledge proofs. Most of the selected works focus on practical implementations that show exactly how theoretical security notions are implemented into concrete blockchain solutions.

This Special Issue was established as a result of the increasing interest in holistic solutions to blockchain security challenges. The selected papers represent significant advances in addressing these challenges while maintaining the balance between security, efficiency,

check for updates

Received: 27 January 2025
Accepted: 28 January 2025
Published: 1 February 2025

Citation: Karpinski, M.; Kuznetsov, O.; Oliynykov, R. Security, Privacy, Confidentiality, and Trust in the Blockchain: From Theory to Applications. *Electronics* **2025**, *14*, 581. https://doi.org/10.3390/electronics14030581

and usability. We hope that through these contributions, further research and developments in blockchain security will be fostered, leading to more robust and trustworthy blockchain systems.

2. Overview of Contributions

The papers in this Special Issue represent important advances in several domains of blockchain security and privacy. Their contributions can be systematically analyzed from the perspectives of their key technological innovations and practical applications.

In light of such scenarios, one suggested key encapsulation scheme based on NTRU presented by He and Xu (Contribution 1) proposes a completely different approach to secure data transmission underwater. In this scheme, ring sampling techniques are used for compact NTRU trapdoor generation in order to minimize communication overheads without affecting security. Underwater acoustic channel characteristics are integrated, while they propose using temporary identity information in order to guarantee confidentiality and reliability. Their experimental validation shows very good performance metrics, achieving the required ciphertext security while meeting the strict requirements of underwater acoustic communication.

Zhang et al. (Contribution 2) propose an approach for to detection of vulnerabilities in smart contracts. This approach is based on heterogeneous contract semantic graphs combined with the pre-training method, which represents a significant jump compared to classical approaches. The developed technique shows increased precision, recall, and F1 scores while detecting four common and harmful types of smart contract vulnerability.

Other significant contributions in this area of privacy-preserving data management include that by Shibano et al. (Contribution 3), who develop a system for the secure processing of private IPFS. The zero-knowledge proofs, as implemented by these authors with the Groth16 protocol of zk-SNARKs, ensure that the authentication of data occurs with privacy maintained. The ability of this system to prevent unauthorized secondary distribution through recipient name embedding adds an extra layer of grassroot security.

Kuznetsov et al. (Contribution 4) show the state of the art regarding the optimization of cryptographic primitives based on dynamic cost function adjustments performed in heuristic searches. Their approach achieves a success rate of 100% in finding 8-bit bijective S-boxes with maximal nonlinearity. It requires iterations of the order of magnitude of 50,000; this is relatively efficient compared to contributions from previous studies. This is an important contribution to the area of symmetric system security.

Juárez and Bordel (Contribution 5) present a more sophisticated dual-layer blockchain architecture for VANETs. The proposed system can neutralize malicious behaviors with an efficacy of up to 86% thanks to several innovative reputation assessment frameworks combined with Bayesian inference principles. This model succeeds in dealing with some security challenges of vehicular ad hoc networks without losing its operational efficiency.

The work of Mbonu, Maple, and Epiphaniou (Contribution 6) focuses on the security of federated learning by introducing a blockchain-based secure aggregation mechanism. These authors overcome the problem of a single point of failure in the traditional architecture of federated learning using a centralized server and secure model aggregation simultaneously. In addition, the efficiency of training and the model convergence rate are drastically improved by implementing a fault-tolerant server together with a callback mechanism.

This Special Issue also includes innovative work in cryptocurrency security, including the study by Buu and Kim, (Contribution 7) who develop a disentangled prototypical graph convolutional network for phishing scam detection. Their model achieves significant improvements in F1 scores and AUC metrics, demonstrating the effectiveness of combining disentanglement mechanisms with prototypical learning for fraud detection.

In Kim et al.'s (Contribution 8) study, the authors address metaverse security-related challenges with an effective solution—a decentralized identifier-based authentication scheme—that copes relatively well with various private avatar identities in a very secure way, as demonstrated by the rich experimental validation and security analysis performed by the authors.

Castellon et al. (Contribution 9) study blockchain-enabled multi-robot coordination in terms of energy efficiency for information gathering. Their implementation of an energy-efficient protocol as a proof-of-work showed a reduction of up to 14% in energy consumption while maintaining secure coordination among robots. Their work effectively demonstrates practical scalability with up to 10 robots and effectively rejects data that have been tampered with by malicious entities.

Kang et al. (Contribution 10) present a fresh approach to the detection of malicious contracts using a lightweight deep learning model. Their Gredeeptector detects malicious contracts with 92.3% accuracy and simultaneously reduces the model file size by 41.5% compared to baseline approaches. In particular, the implementation of explainable AI for identifying important instructions makes their solution particularly suitable for IoT environments.

Taken together, these findings provide advanced theoretical contributions with practical implementations for blockchain security. Each paper addresses a specific challenge by taking into account a rigorous definition of the security standard to be enforced while considering the application's applicability.

3. Key Findings and Impact

The research presented in this Special Issue highlights some critical milestones achieved in areas of technological advancement in security and privacy in the blockchain. It integrates post-quantum cryptography into the blockchain, mainly through NTRU-based schemes that have shown feasible solutions for protecting blockchain communications in challenging environments. This is important because the emergence of quantum computers threatens modern cryptographic systems.

The security of smart contracts emerges as an important area of concern, and to address this issue new methods of detection can achieve much better accuracy rates. Methods comprising a combination of semantic graph analysis and pre-training techniques provide a leap forward in the field of vulnerability detection. This will directly contribute to addressing highly critical challenges related to the security of the blockchain because of the immutable nature of smart contracts once they are deployed.

Zero-knowledge proofs and secure distributed storage systems provide very significant advances in the preservation of privacy. The successful implementation of these technologies in practice, through novel products like private IPFS, bridges the gap between theoretical and real-world privacy requirements for applications. Among these implementations are those that preserve data authenticity while guaranteeing privacy, an important balance to consider in blockchain systems.

Energy efficiency in blockchain security mechanisms is another major development. The optimization of proof-of-work protocols and the development of lightweight detection models show that the requirements regarding security can be met without excessive computational overheads. This is one of the basic challenges in the adoption of blockchain technology: the trade-off between security and resource consumption.

This Special Issue also discusses the successful applications of blockchain security in emerging domains. From underwater communication to metaverse authentication, research has proven the versatility of blockchains in securing diversified applications. These implementations provide useful blueprints for future security solutions in specialized domains.

It thus follows that cross-domain integration would be one of the research trends in this Special Issue, especially when considering blockchains either combined with artificial intelligence or with IoT. Indeed, many papers show successful fusions resulting in robust and efficient security solutions, thereby also indicating the future research directions in blockchain security research and development.

Taken together, the selected papers provide advanced theoretical contributions with practical implementations for blockchain security. Each paper addresses a specific challenge by taking into account a rigorous definition of the security standard to be enforced while considering the application's applicability.

4. Future Research Directions

This Special Issue brings together several promising areas in which blockchain security may be investigated in the future. The integration of post-quantum cryptography remains to be further advanced, especially regarding optimizations needed for resource-constrained environments. The successes with NTRU-based schemes indicate the possibility of other post-quantum approaches showing promise in blockchain systems.

The security of smart contracts still remains in its development stages. While current approaches for vulnerability detection have great potential, much is yet to be achieved in real-time detection and the automation of correction mechanisms. Combining formal verification approaches with machine learning techniques might help in achieving less vulnerable features.

Another important research direction is privacy preservation in cross-chain interactions. While blockchain systems are becoming increasingly interconnected, establishing how to balance privacy preservation with interoperability represents a very important research direction. Zero-knowledge proof systems should be further optimized for complex cross-chain transactions.

Improving energy efficiency in security mechanisms is a process of continuous innovation. The use of lightweight security protocols that preserve strong protections while minimizing resource consumption remains an open challenge that faces the developers of IoT and edge computing applications.

The metaverse, along with the management of one's digital identity, is where new security risks are arising. The integration of virtual environments with blockchain-based authentication needs to be furthered. Special focus should be provided to scalability, while not compromising either user experience or security.

5. Conclusions

This Special Issue highlights several significant advances regarding the security, privacy, and trust mechanisms in blockchains. The ten papers together therefore show advancements in many domains, ranging from theoretical cryptography to practical applications, and from post-quantum cryptography solutions to energy-efficient security protocols.

The research in this Special Issue presents effective solutions to the critical challenges regarding blockchain security, while also indicating other areas requiring further investigation in future research activities. Meanwhile, these studies also demonstrate the maturity of this topic, because advanced cryptographically strong principles are adapted and combined effectively with practical perspectives. Noteworthy results are presented with regard to smart contract security analysis, privacy provision, and the development of resource-efficient security primitives.

These works lay the foundations for future researchers in studies on blockchain security. They show how strong and efficient security solutions may effectively coexist with or support more practical efficiency improvements. When developing security frame-

works and their methodologies in blockchain technology, these studies will act as valuable references for researchers and practitioners.

We would like to thank all the authors, reviewers, and editorial staff who have contributed to this Special Issue. Their contributions have enhanced our understanding of blockchain security and will influence future developments in this rapidly developing area.

Author Contributions: Conceptualization and methodology, writing—original draft preparation, O.K.; formal analysis, M.K.; writing—review and editing, M.K. and R.O. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement: The datasets generated during and/or analyzed during the current study are available from the corresponding author upon reasonable request.

Conflicts of Interest: Author Roman Oliynykov was employed by the company Input Output (IOG Singapore Pte Ltd.). The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

List of Contributions

1. He, P.; Xu, M. An NTRU-Based Key Encapsulation Scheme for Underwater Acoustic Communication. *Electronics* **2025**, *14*, 405.
2. Zhang, J.; Lu, G.; Yu, J. A Smart Contract Vulnerability Detection Method Based on Heterogeneous Contract Semantic Graphs and Pre-Training Techniques. *Electronics* **2024**, *13*, 3786.
3. Shibano, K.; Ito, K.; Han, C.; Chu, T.; Ozaki, W.; Mogi, G. Secure Processing and Distribution of Data Managed on Private InterPlanetary File System Using Zero-Knowledge Proofs. *Electronics* **2024**, *13*, 3025.
4. Kuznetsov, O.; Poluyanenko, N.; Frontoni, E.; Kandiy, S.; Karpinski, M.; Shevchuk, R. Enhancing Cryptographic Primitives through Dynamic Cost Function Optimization in Heuristic Search. *Electronics* **2024**, *13*, 1825.
5. Juárez, R.; Bordel, B. Augmenting Vehicular Ad Hoc Network Security and Efficiency with Blockchain: A Probabilistic Identification and Malicious Node Mitigation Strategy. *Electronics* **2023**, *12*, 4794.
6. Mbonu, W.; Maple, C.; Epiphaniou, G. An End-Process Blockchain-Based Secure Aggregation Mechanism Using Federated Machine Learning. *Electronics* **2023**, *12*, 4543.
7. Buu, S.; Kim, H. Disentangled Prototypical Graph Convolutional Network for Phishing Scam Detection in Cryptocurrency Transactions. *Electronics* **2023**, *12*, 4390.
8. Castellon, C.; Khatib, T.; Roy, S.; Dutta, A.; Kreidl, O.; Bölöni, L. Energy-Efficient Blockchain-Enabled Multi-Robot Coordination for Information Gathering: Theory and Experiments. *Electronics* **2023**, *12*, 4239.
9. Kim, M.; Oh, J.; Son, S.; Park, Y.; Kim, J.; Park, Y. Secure and Privacy-Preserving Authentication Scheme Using Decentralized Identifier in Metaverse Environment. *Electronics* **2023**, *12*, 4073.
10. Kang, Y.; Kim, W.; Kim, H.; Lee, M.; Song, M.; Seo, H. Malicious Contract Detection for Blockchain Network Using Lightweight Deep Learning Implemented through Explainable AI. *Electronics* **2023**, *12*, 3893.

References

1. Abou Jaoude, J.; George Saade, R. Blockchain Applications—Usage in Different Domains. *IEEE Access* **2019**, *7*, 45360–45381. [CrossRef]
2. Alruwaili, F.F.; Alabduallah, B.; Alqahtani, H.; Salama, A.S.; Mohammed, G.P.; Alneil, A.A. Blockchain Enabled Smart Healthcare System Using Jellyfish Search Optimization With Dual-Pathway Deep Convolutional Neural Network. *IEEE Access* **2023**, *11*, 87583–87591. [CrossRef]

3. Apat, H.K.; Sahoo, B. A Blockchain Assisted Fog Computing for Secure Distributed Storage System for IoT Applications. *J. Ind. Inf. Integr.* **2024**, *42*, 100739. [CrossRef]
4. Cheng, H.; Lo, S.-L.; Lu, J. A Blockchain-Enabled Decentralized Access Control Scheme Using Multi-Authority Attribute-Based Encryption for Edge-Assisted Internet of Things. *Internet Things* **2024**, *26*, 101220. [CrossRef]
5. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on Blockchain Based Smart Contracts: Applications, Opportunities and Challenges. *J. Netw. Comput. Appl.* **2021**, *177*, 102857. [CrossRef]
6. Shafay, M.; Ahmad, R.W.; Salah, K.; Yaqoob, I.; Jayaraman, R.; Omar, M. Blockchain for Deep Learning: Review and Open Challenges. *Clust. Comput.* **2023**, *26*, 197–221. [CrossRef] [PubMed]
7. Kuznetsov, O.; Sernani, P.; Romeo, L.; Frontoni, E.; Mancini, A. On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security. *IEEE Access* **2024**, *12*, 3881–3897. [CrossRef]