UNIVERSITETI POLIS

ICCSM 2025

BOOK OF PROCEEDINGS

1ST INTERNATIONAL CONFERENCE COMPUTER SCIENCES AND MANAGEMENT

WHERE DIGITAL & BUSINESS BECOME HUMAN

26-27 June 2025 | Tirana, Albania

ISBN 9789928347123

DOI 10.37199/c41000300

CONFERENCE CHAIR

Assoc. Prof. Merita Toska, POLIS University

PARTNER UNIVERSITIES

POLIS University, Albania
Université Lyon 2, France
Università Telematica San Raffaele, Italy
University of Western Macedonia, Greece
International University of Sarajevo, Bosnia & Herzegovina
Mother Teresa University, North Macedonia
Gebze Technical University, Turkey
Public International Business College, Kosovo
Rochester Institute of Technology – RIT Global Campus, Kosovo
Co-PLAN, Institute for Habitat Development, Albania
AI Hub Albania, Albania
Luralux, Albania

ORGANISING COMMITTEE

Dr. Blerta Mjeda
Dr. Emiliano Mankolli
Msc. Sonila Murataj
Msc. Andia Vllamasi
Msc. Klejda Hallaci
Msc. Erilda Muka
Msc. Armela Reka

SCIENTIFIC COMMITTEE

Dr. Albina Toçilla, POLIS University (Albania)
Dr. Sonia Jojic, POLIS University (Albania)
Dr. Ilda Rusi, POLIS University (Albania)
Dr. Ledian Bregasi, POLIS University (Albania)
Dr. Klodjan Xhexhi, POLIS University (Albania)
Dr. Endri Duro, POLIS University (Albania)
Dr. Remijon Pronja, POLIS University (Albania)
Dr. Vjosë Latifi, International Business Collage Mitrovica (Kosovo)
Dr. Agron Hajdari, International Business Collage Mitrovica (Kosovo)

Table of Contents

09

BLOCKCHAIN CRYPTOGRAPHY AND THE FUTURE OF DIGITAL CURRENCY SECURITY

DOI: 10.37199/c41000309

Erilda MUKA

Polis University, Tirana, Albania
erilda_muka@universitetipolis.edu.al
ORCID 0009-0001-4764-2145

Anna Maria KOSOVA

Polis University, Tirana, Albania
annamaria_kosova@universitetipolis.edu.al
ORCID 0009-0001-6998-5085

Blerina BEKTASHI

Polis University, Tirana, Albania
blerina_bektashi@universitetipolis.edu.al
ORCID 0009-0004-9875-558X

Abstract

Blockchain security is fundamentally based on several cryptographic mechanisms that maintain transaction integrity, confidentiality, and authentication, and it is the pinnacle of technology today. This paper analyses various cryptographic techniques embedded in blockchain. These techniques include data encryption, digital signatures, and hashing. The following discusses the different consensus mechanisms that enable scalability and integrity in a blockchain, with an emphasis on proof-of-work and proof-of-stake. Nevertheless, there are problems relating to 51% attacks, scalability issues and privacy concerns thereof in a blockchain. To assess users' knowledge and perceptions of blockchain technology security, we will conduct a survey to analyse levels of knowledge, usage trends, and concerns about digital currency security. The results will provide insight into current knowledge of blockchain cryptography and indicate possible areas for strengthening security.

Keywords*:* Blockchain Security, Attacks, Cryptography, Encryption, Digital Currency.

I. INTRODUCTION

Blockchain technology has quickly moved from an uncertain innovation to a vital component of the modern digital landscape, especially in finance and data security. At its most fundamental level, blockchain is a distributed ledger technology that enables tamperproof, transparent, and secure recording of transactions, with trust established without the involvement of third-party intermediaries (Narayanan et al., 2016). In the case of digital currencies, trust is provided through cryptographic proofs and consensus protocols rather than through banks and traditional financial institutions. One of the major aspects of blockchain technology is its use of cryptography to ensure the confidentiality, authenticity, and integrity of data. Cryptographic hashing, digital signatures, and asymmetric encryption are methods for securely initiating transactions and verifying them (Conti et al., 2018). Each transaction is digitally signed with the user's private key and verified by nodes using the corresponding public key. Some blockchains use cryptographic hash functions to form chains of blocks. If the data in a block is changed, the entire chain will be void (Bonneau et al., 2015). Consensus protocols are equally important to blockchain security, as they determine how nodes in the network agree on the validity of transactions.

Common blockchains like Bitcoin use proof-of-work (PoW) as a consensus mechanism, which is an energy-intensive process that reduces malicious activity (Nakamoto, 2008). Alternative mechanisms, such as proof-of-stake (PoS), have emerged to provide a similar, if not more secure, level of security with lower energy consumption (Saleh, 2021). Consensus protocols help generate trust, security, and accuracy in the blockchain system, yet financial actors in the blockchain ecosystem are often unaware of their meaning and significance. However, blockchain technology is not without fault. A majority attack, also called a 51% attack, occurs when a group of miners or validators becomes the majority holders of network power, posing a serious threat to blockchain networks (Li et al., 2020). Privacy is also a concern in cryptocurrency transactions, as although they are pseudonymous, transaction details are sometimes publicly accessible and can be traced using on-chain analysis tools. The scalability of blockchains is also an ongoing technical concern, as transaction throughput is often lower than that of asynchronous systems.

This study aims to integrate theoretical and empirical research better to understand the social and technological aspects of the challenges. The research utilised a user survey to examine public knowledge, use, and concerns regarding the security of blockchain-based digital currencies. The importance of developing and integrating digital finance into everyday economic life makes it critical to understand how cryptography and blockchain security intersect to design secure, trusted and inclusive financial systems (Zohar, 2015). The insights from this study will help better understand user knowledge gaps and potential weaknesses in current blockchain systems and inform the development of future secure digital currency ecosystems.

II. LITERATURE REVIEW

The rapid growth of blockchain technology has generated significant academic interest, spanning topics such as cryptography, cybersecurity, and digital finance. This literature review synthesises significant research on blockchain-based cryptographic components, consensus protocols, security weaknesses, and user knowledge of blockchain-based digital currencies. Blockchain's strength lies in leveraging conventional cryptography to secure data and build trust in decentralised systems. Data integrity in the blockchain framework is ensured through cryptographic hash functions, such as SHA-256, which is used in Bitcoin. These types of cryptosystems produce irretrievable tokens for any input, meaning that even if someone has the same input, they will receive a different token (Narayanan et al., 2016). This token is fundamental for linking blocks, because if you tampered with one block, you would have to recalculate all hashes, which is computationally impossible. Cryptographic confirmation also uses public-key-only signing to not only confirm authentication but also provide non-repudiation for blockchain-based transactions (Conti et al., 2018). Each transaction is signed with the sender's private key, and anyone receiving it can use the sender's public key to confirm that only the sender could have sent it and that it is legitimate. This use of cryptography eliminates the need to consult a centralised authority and ultimately makes the whole system more transparent and trustworthy. Consensus algorithms allow for the validation and recording of transactions in decentralised blockchain systems.

Proof-of-work (PoW) is the most widely known consensus mechanism, first proposed by Nakamoto (2008) in Bitcoin. PoW uses computational power to require nodes (miners) to solve complex mathematical proofs, which is often very resource-intensive in terms of computing power and electricity. Although PoW is effective at securing a blockchain network, it has been criticised for its environmental impact and scalability. Alternative consensus protocols have been developed, such as proof-of-stake (PoS), which assigns rights based on the amount of cryptocurrency a user is willing to hold and "stake" to validate blocks, which is less energy-intensive and still maintains some security (Saleh, 2021). The proof-of-stake consensus mechanism is particularly significant for the blockchain ecosystem, as Ethereum, a major blockchain platform, has migrated to PoS with its "Ethereum 2.0" upgrade. Despite cryptographic protections, blockchain systems are not susceptible to security risks. One of the most well-known security risks is the 51% attack, in which a collusion of malicious actors obtains control of more than 50% of a blockchain network's computing power, enabling them to manipulate transactions or double-spend digital currency (Li et al., 2020). This vulnerability becomes especially problematic for smaller blockchain networks with lower hash rates or lower decentralisation.

Another problem is the security ramifications of smart contracts, and the decentralised applications (dApps) that are part of that equation, on platforms like Ethereum. Smart contract exposures can result in large-scale exploits, as was the case in 2016, when hackers exploited a flaw in a smart contract to drain $60 million in Ether in the DAO attack (Atzei et al., 2017). Because blockchain is unchangeable, nothing can be undone once these contracts are deployed. There are also privacy issues that have been discussed; while many blockchains, like Bitcoin, provide pseudonymity, these transactions can be viewed publicly and traced. Transparency has raised concerns about user anonymity and data protection, and research has focused on privacy technologies such as zero-knowledge proofs and confidential transactions (Zhang et al., 2019). Most blockchain research has focused on technical studies. However, over the past several years, a handful of researchers have examined human issues, such as user awareness, trust, and the adoption of blockchain technologies. The research indicates that the public typically lacks a sophisticated understanding of the mechanisms that determine the security of blockchains (Alketbi et al., 2018). Uncertainty about digital currencies, driven by volatility, hacking incidents, and regulatory developments, has also been cited as a barrier to wider acceptance.

III. MATERIALS AND METHODS

To assess knowledge of blockchain security, a structured survey was designed for university students enrolled in Computer Science Bachelor's programs. This survey, on a 5-point Likert scale (from "strongly disagree" to "strongly agree"), assesses users' knowledge and perceptions of blockchain technology's security.

Key topics included levels of knowledge, usage trends, concerns about digital currency security, and students' personal experiences and perceptions of cryptography's effectiveness. The survey results will provide insight into current knowledge of blockchain cryptography and identify potential areas for strengthening security.

Participants included three groups of Computer Science students: 84 first-year, 93 second-year, and 96 third-year students, for a total of 273. The survey was created in Google Forms and distributed in person, by email, and via Google Classroom to ensure easy access and broad participation. Data were collected electronically, organised in Excel, and analysed using descriptive statistics in Excel and SPSS Statistics 27 to identify students' attitudes toward blockchain security.

The 10 questions were grouped into four sections:

- Section 1: User Information
- Section 2: Cryptography in Blockchain
- Section 3: Digital Currency Transaction Security
- Section 4: Blockchain Security and Future Challenges

Questions were as follows:

1) I have a good understanding of blockchain technology.
2) I have experience with digital currencies (e.g., Bitcoin and Ethereum).
3) I am familiar with the concept of hashing in blockchain.
4) Hashing is essential for ensuring the security of blockchain.
5) Asymmetric cryptography (public and private keys) is crucial for securing blockchain transactions.
6) Blockchain transactions are generally secure.
7) Digital currency transactions are vulnerable to attacks such as Man-in-the-Middle or Double-Spending.
8) I am confident that current blockchain security measures can effectively prevent fraud and unauthorised access.
9) Cryptography alone is sufficient to prevent manipulation of the transaction history in a blockchain.
10) I believe blockchain security threats will become more severe in the future.

The values of the questions are:

1 = strongly disagree,

2 = disagree,

3 = neutral,

4 = agree,

5 = strongly agree,

The interpretation of the mean values is in Table 1.

Mean value	Interpretation
1- 1.8	Strongly disagree (SD)
1.81- 2.6	Disagree (D)
2.61- 3.4	Neutral (N)
3.41- 4.2	Agree (A)
4.21- 5.0	Strongly Agree (SA)

Table 1. Mean values and interpretations

Source: Author's processing

IV. RESULTS

The survey data were collected using Google Forms and were initially processed in Excel to conduct exploratory visual analyses and note first-response patterns. To conduct a more formal, rigorous, and comprehensive evaluation, the dataset was subsequently imported into SPSS Statistics 27. In SPSS, descriptive statistics, including means, medians, standard deviations, and an important consistency check, were calculated to assess the data's reliability and students' opinions on establishing security in blockchain cryptography and digital currency. One important component of the analysis performed was to assess reliability using Cronbach's Alpha. The overall Cronbach's Alpha for the survey items was 0.872 (Table 2), indicating high internal consistency. This reliability score, as an overall indicator, supports the idea that the survey measures a defined latent factor, allowing the findings to be reliably interpreted.

Cronbach's Alpha	N of Items
.872	10

Table 2. Reliability Statistics

Source: Author's processing

Descriptive statistics were calculated for all of the questions (Q1-Q10) of the survey to define the overall response of the general participants (Table 3). The mean score for all questions ranged from 3.21 (Q2) to 3.92 (Q10). Since the means fell largely between 'Neutral' (3) and 'Agree' (4), the students ultimately appeared to exhibit just moderate strengths of understanding and agreement on blockchain security. These distributions are visually confirmed by the histograms, which show peaks around the "Neutral" and "Agree" categories for most questions. For example, Q4 (Hashing is critical to the security of blockchain) had a mean of 3.67, and the 'Agree' frequency was notable. At the same time, Q5 (Asymmetric cryptography (public and private keys) is critical to the security of blockchain transactions) had a mean of 3.79, with a significant number of 'Agree' responses.

	N	Range	Minimum	Maximum	Mean	Std. Deviation	Variance	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Q1	24	3.00	2.00	5.00	3.4167	.88055	.775	-.141	.472	-.610	.918
Q2	24	4.00	1.00	5.00	3.2083	1.21509	1.476	.200	.472	-1.057	.918
Q3	24	3.00	2.00	5.00	3.5417	.83297	.694	.103	.472	-.371	.918
Q4	24	3.00	2.00	5.00	3.6667	.91683	.841	-.356	.472	-.469	.918
Q5	24	3.00	2.00	5.00	3.7917	.83297	.694	-.066	.472	-.605	.918
Q6	24	3.00	2.00	5.00	3.4167	.82970	.688	.039	.472	-.338	.918
Q7	24	3.00	2.00	5.00	3.4167	.71728	.514	-.068	.472	-.058	.918
Q8	24	3.00	2.00	5.00	3.3333	.70196	.493	.244	.472	.234	.918
Q9	24	3.00	2.00	5.00	3.5000	.83406	.696	-.245	.472	-.343	.918
Q10	24	3.00	2.00	5.00	3.9167	.77553	.601	-.460	.472	.298	.918
Valid N (listwise)	24										

Table 3. Descriptive Statistics

Source: Author's processing

		Std. Error
Q1	Mean	.17974
Q2	Mean	.24803
Q3	Mean	.17003
Q4	Mean	.18715
Q5	Mean	.17003
Q6	Mean	.16936
Q7	Mean	.14641
Q8	Mean	.14329
Q9	Mean	.17025
Q10	Mean	.15830

Table 4. Descriptive statistics

Source: Author's processing

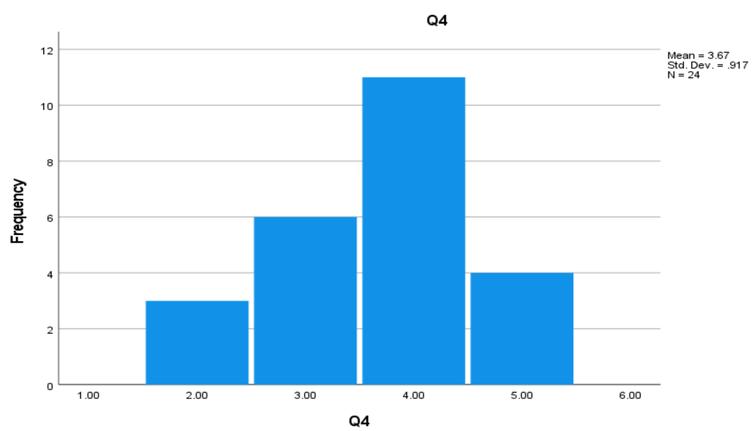

Figure 1. Q4 Frequency

Source: Author's processing

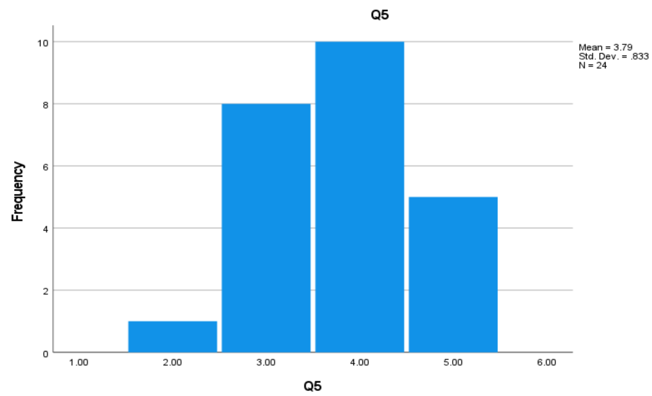

Figure 2. Q4 Frequency

Source: Author's processing

We further examined the distribution of agreement by separating the responses by the students' year of study (Year 1, 2, or 3). The average level of agreement across all questions varied slightly over the years; Year 1 students had an average score of 3.31, Year 2 students had 3.35, and Year 3 students had 3.43. These differences are small; however, they do indicate a subtle increase in agreement or understanding with the students' year of study. Interestingly, Year 2 students were noted in the documentation to have taken a Cybersecurity course and, as a result, did not show a marked difference compared with Year 3 students, suggesting that while the Cybersecurity course likely increased understanding, the overall disposition was generally similar or consistent across the latter years. The breakdown of the average level of agreement by individual question also varied by year of study. For example, Year 2 students showed a higher proportion of "Strongly Agree" responses to certain questions than Year 1 students, even though these questions were directly related to cryptographic concepts. This distinction by academic year provides a useful framework for analysing the different perspectives of computer science students regarding their understanding of blockchain security development.

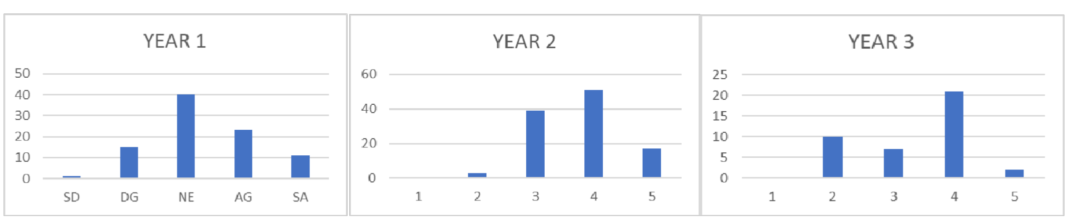

Figure 3. Frequency distribution

Source: Author's processing

V. CONCLUSIONS

The study aims to explore the foundational cryptographic principles of blockchain security and examine computer science students' understanding and perceptions of digital currency security. Survey responses showed that students ranged from moderate to high in their understanding of security concepts and their application. The mean score ranged from 'Neutral' to 'Agree' on each question posed to the participants. The internal consistency of the survey items was high (Cronbach's Alpha = 0.872), and the survey outcomes measurements can be considered reliable. Although students demonstrated a high level of understanding of blockchain security concepts, such as hashing and asymmetric cryptography, their responses showed slight differences across academic years. The trend of slightly higher average agreement scores from Year 1 to Year 3 reflects incremental development of knowledge and latent confidence among students as they progress through a computer science degree. Importantly, Year 2 students have a cybersecurity course, yet their perception scores for blockchain security were similar to those of Year 3 students. This suggests that while a specific course adds value, overall exposure to computer science concepts over extended periods contributes significantly to understanding. The importance of practical, interactive activities is reinforced in this study and is similar to effective technology use in other STEM education applications. Just as tools like the GeoGebra app, the Desmos Graphing Calculator, or any statistical software help visualise abstract mathematical concepts, provide hands-on experimentation, and draw meaningful conclusions with abstract ideas, similar approaches will be essential to help students understand how blockchain cryptography actually functions. Suppose we allow students to manipulate simulations or view visualisations of crypto processes, or to design their own simplified blockchain models. In that case, we create real opportunities for them to develop an intuitive understanding of security measures.

The apps that calculate results, like Wolfram Alpha or Microsoft Math Solver, which detail their answers, will grant teachers a degree of remote access to students' knowledge of advanced blockchain concepts that had previously been obscured. For instance, an app that detailed the steps of Hashing Algorithms or illustrated how changes to consensus mechanisms would affect projections would combine abstract principles with tangible, reasonable insights. The strength of testing and quiz apps, especially Google Forms/Quiz Mode, for immediate assessment of student comprehension, offers educators a torturous chain of opportunities to validate, clarify, and ultimately reinforce students' understanding of essential concepts in the blockchain security and cryptography space. At the end of the day, the interactive role of prospective student teachers in creating a technology-rich learning environment, as emphasised in the reference material for developing STEM courses, guided by the current digitalisation of currency security, with strong knowledge and confidence, is translated into simulations of real-world currency developments.

REFERENCES

Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in industries: A survey. *IEEE Access, 7*, 36500–36515. https://doi.org/10.1109/ACCESS.2019.2903554

Alketbi, A., Nasir, Q., & Talib, M. A. (2018). Blockchain for government services—Use cases, security benefits and challenges. *2018 15th Learning and Technology Conference (L&T)*, 112–119. https://doi.org/10.1109/LT.2018.8368508

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). *Proceedings of the 6th International Conference on Principles of Security and Trust*, 164–186. https://doi.org/10.1007/978-3-662-54455-6_8

Bertaccini, M. (2022). *Cryptography Algorithms: A guide to algorithms in blockchain, quantum cryptography, zero-knowledge protocols, and homomorphic encryption.* Packt Publishing.

Bhutta, M. N. M., et al. (2021). A survey on blockchain technology: Evolution, architecture and security. *IEEE Access, 9*, 61048–61073. https://doi.org/10.1109/ACCESS.2021.3072849

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies. *2015 IEEE Symposium on Security and Privacy*, 104–121. https://doi.org/10.1109/SP.2015.14

Chen, H., Wei, N., Wang, L., Mobarak, W. F. M., Albahar, M. A., & Shaikh, Z. A. (2024). The role of blockchain in finance beyond cryptocurrency: Trust, data management, and automation. *IEEE Access, 12*, 64861–64885. https://doi.org/10.1109/ACCESS.2024.3395918

Conti, M., Kumar, S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials, 20*(4), 3416–3452. https://doi.org/10.1109/COMST.2018.2842460

Fathalla, E., & Azab, M. (2024). Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimisations. *IEEE Access, 12*, 175969–175987. https://doi.org/10.1109/ACCESS.2024.3485602

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access, 8*, 21091–21116. https://doi.org/10.1109/ACCESS.2020.2968985

Islam, M. M., & In, H. P. (2024). An auditable, privacy-preserving, transparent unspent transaction output model for blockchain-based central bank digital currency. *IEEE Open Journal of the Computer Society, 5*, 671–683. https://doi.org/10.1109/OJCS.2024.3486193

Khan, I., Maghrabi, L. A., Sarwar, M. I., Naith, Q. H., & Nisar, K. (2023). Blockchain: A crypto-intensive technology—A comprehensive review. *IEEE Access, 11*, 141926–141955. https://doi.org/10.1109/ACCESS.2023.3342079

Koroglu, T., & Samet, R. (2024). Can there be a two-way hash function? *IEEE Access, 12*, 18358–18386. https://doi.org/10.1109/ACCESS.2024.3360217

Kuznetsov, O., Sernani, P., Romeo, L., Frontoni, E., & Mancini, A. (2024). On the integration of artificial intelligence and blockchain technology: A perspective about security. *IEEE Access, 12*, 3881–3897. https://doi.org/10.1109/ACCESS.2023.3349019

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems, 107*, 841–853. https://doi.org/10.1016/j.future.2017.08.020

Maldonado-Ruiz, D., Torres, J., El Madhoun, N., & Badra, M. (2022). Current trends in blockchain implementations on the paradigm of public key infrastructure: A survey. *IEEE Access, 10*, 17641–17655. https://doi.org/10.1109/ACCESS.2022.3145156

Mishra, D., & Phansalkar, S. (2025). Blockchain security in focus: A comprehensive investigation into threats, smart contract security, cross-chain bridges, and vulnerabilities detection tools and techniques. *IEEE Access, 13*, 60643–60671. https://doi.org/10.1109/ACCESS.2025.3556499

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction.* Princeton University Press.

Ramakrishna, D., & Shaik, M. A. (2025). A comprehensive analysis of cryptographic algorithms: Evaluating security, efficiency, and future challenges. *IEEE Access, 13*, 11576–11593. https://doi.org/10.1109/ACCESS.2024.3518533

Sadawi, A. A., Hassan, M. S., & Ndiaye, M. (2021). A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges. *IEEE Access, 9*, 54478–54497. https://doi.org/10.1109/ACCESS.2021.3070555

Saleh, F. (2021). Blockchain without waste: Proof-of-stake. *The Review of Financial Studies, 34*(3), 1156–1190. https://doi.org/10.1093/rfs/hhaa075

Shaikh, Z. A., et al. (2024). A new trend in cryptographic information security for Industry 5.0: A systematic review. *IEEE Access, 12*, 7156–7169. https://doi.org/10.1109/ACCESS.2024.3351485

Sinha, S. K., & Mukhopadhyay, D. (2024). Time-efficient hash key generation for a blockchain-enabled framework. *IEEE Access, 12*, 155867–155884. https://doi.org/10.1109/ACCESS.2024.3478845

Upadhyay, D., Gaikwad, N., Zaman, M., & Sampalli, S. (2022). Investigating the avalanche effect of various cryptographically secure hash functions and hash-based applications. *IEEE Access, 10*, 112472–112486. https://doi.org/10.1109/ACCESS.2022.3215778

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview.* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

Yang, Z., Alfauri, H., Farkiani, B., Jain, R., Pietro, R. D., & Erbad, A. (2024). A survey and comparison of post-quantum and quantum blockchains. *IEEE Communications Surveys & Tutorials, 26*(2), 967–1002. https://doi.org/10.1109/COMST.2023.3325761

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys, 52*(3), 1–34. https://doi.org/10.1145/3316481

Zohar, A. (2015). Bitcoin: Under the hood. *Communications of the ACM, 58*(9), 104–113. https://doi.org/10.1145/2701411