MEST Journal
DOI 10.12709/mest.13.13.01.05

# CRYPTOGRAPHIC FOUNDATIONS FOR BLOCKCHAIN SECURITY IN DECENTRALIZED NETWORKS

**Milan Feltovic**
University of Žilina, Faculty of Security Engineering, Žilina, Slovakia
https://orcid.org/0009-0004-3057-2912



JEL Category: **C88**

***Abstract***

*In the rapidly evolving digital technology landscape, blockchain emerges as a pivotal innovation with the potential to revolutionize industries far beyond its original application in cryptocurrencies like Bitcoin. This article explores the critical role of cryptography in decentralized information networks, emphasizing its importance in ensuring the integrity, confidentiality, and authenticity of digital transactions. It examines the mathematical foundations underlying cryptographic techniques, including elliptic curve cryptography and hash functions, and discusses their application in consensus protocols such as Proof-of-Work. Furthermore, the paper addresses the challenges and potential vulnerabilities posed by quantum computing to current cryptographic standards. By providing a comprehensive overview of both theoretical and practical aspects of cryptography in blockchain technology, this study aims to enlighten readers on the robust security measures essential for maintaining trust and security in decentralized systems. Moreover, the discussion extends to the implications of cryptographic advancements for various sectors such as healthcare, finance, and public administration, highlighting how blockchain enhances transparency and security in these fields. This article underscores the urgency of advancing cryptographic research to address emerging threats and ensure the resilience of blockchain systems against future technological developments. The findings emphasize the need for ongoing innovation in cryptographic methods to safeguard the integrity of decentralized networks in an era of increasing digital interconnectivity.*

**Keywords:** *blockchain, cryptography, elliptic curve, hash functions, transaction integrity, Proof-of-Work, quantum computing, public key, digital signatures, encryption protocols.*

## 1 INTRODUCTION

In today's era of digital advancement and innovation, blockchain technology is transforming various industrial sectors and significantly altering the paradigm of information storage and sharing. Initially developed as the foundation for digital currencies like Bitcoin, its potential has expanded

*Address of the author:*
***Milan Feltovic***
*milan@feltovic.com*

far beyond, reaching areas such as healthcare, finance, and public administration, where it contributes to increased transparency and security. In healthcare, blockchain enables secure storage and sharing of medical records among various healthcare providers, improving care coordination and patient privacy protection (Nakamoto, 2009). In finance, blockchain provides efficient and transparent solutions for international payments, reducing transaction costs and eliminating the need for intermediaries (Buterin, 2014). In public administration, blockchain technology increases the transparency and trustworthiness of public records and elections, thereby enhancing public trust in these systems (Gallian, 2021).

One of the key aspects of blockchain is cryptography, which underpins the security and trust in these decentralized systems. Cryptography in blockchains ensures that transactions are not only secure but also immutable, which is critically important for maintaining integrity and trust in digital systems. Given the growing cybersecurity threats, the need for advanced cryptographic solutions has become even more pressing (Sipser, 2021). The development of robust cryptographic methods has been significantly influenced by the understanding of cryptographic codes, as described by Secret Bits, which outlines the evolution of unbreakable codes and their implications (Abelson, Ledeen, & Lewis, 2008).

This article aims to provide insight into how cryptography supports the security and functionality of decentralized information networks, with a particular emphasis on blockchain technology. I analyze the mathematical foundations on which cryptography is built and examine its various applications, from basic hashing functions to advanced elliptic curve algorithms. Additionally, I address the challenges posed by quantum computing to current cryptographic standards and discuss future research directions in the field of post-quantum cryptography.

## 2 METHODS

In this section, I provide a detailed description of the cryptographic techniques used in blockchain technology. Elliptic Curve Cryptography (ECC) and hashing functions (SHA-256) are crucial for ensuring the integrity and authenticity of transactions. I also focus on consensus protocols, such as Proof-of-Work, and their role in maintaining the consistency of the blockchain network. Additionally, I analyze the impact of quantum computing on current cryptographic standards and discuss post-quantum cryptographic solutions.

Blockchain technology, originally developed as an architecture for the cryptocurrency Bitcoin, has rapidly garnered interest not only in technological circles but also across a broad spectrum of industrial applications (Nakamoto, 2009). Today, blockchain is used in various sectors, including finance, healthcare, and logistics, providing a decentralized solution that enhances transparency and reduces the need for third-party verification of transactions.

A key factor enabling the secure and efficient operation of blockchain is cryptography. Gallian (2021) explains how mathematical principles, particularly number theory and abstract algebra, provide the foundation for cryptographic algorithms used in blockchain technologies (Gallian, 2021). For instance, elliptic curve cryptography (ECC), as described by Koblitz, Menezes, and Vanstone, is widely recognized for its ability to offer strong encryption with relatively small key sizes, which reduces computational requirements and improves system performance (Koblitz, Menezes, & Vanstone, 2000). Understanding the underlying principles of trapdoor functions is also crucial, as they form the basis for many cryptographic algorithms (Wikipedia, Trapdoor function, 2013).

In the area of consensus protocols, such as Proof-of-Work, detailed by Nakamoto and Buterin, hash functions like SHA-256 are used to ensure the integrity of the blockchain. These methods help protect the network from unauthorized changes and ensure that all copies of the distributed ledger remain consistent and unaltered (Buterin, 2014).

Recently, concerns have emerged regarding potential threats from quantum computing, which could disrupt current cryptographic standards. Shor's research shows that quantum algorithms could efficiently solve problems like factorization and discrete logarithms, which underpin many

existing encryption systems. This paradigm shift necessitates new approaches to security in the era of quantum technologies, as indicated by the latest studies in post-quantum cryptography (Shor, 1999).

This literature review underscores the importance of ongoing research and development in cryptography to ensure the security of decentralized networks. As blockchain technology grows and evolves, it will be crucial to ensure that cryptographic methods stay ahead of potential threats to maintain the trust and integrity of these systems (Briggs, 1998).

# 3 MATHEMATICS AND THEORY OF CRYPTOGRAPHIC TECHNIQUES

At the core of cryptographic techniques used in blockchain technology are mathematical and theoretical principles that provide security and trust in digital systems. These principles include number theory, abstract algebra, complexity theory, and algorithms based on these principles.

## 3.1 Number Theory

Number theory is a fundamental aspect of cryptography and involves the study of the properties of numbers, particularly integers. In cryptography, number theory is utilized in:

- **Factorization of Numbers**: Crucial in RSA cryptography, where security relies on the difficulty of factoring large composite numbers into prime numbers.
- **Exponential and Modular Arithmetic**: These operations form the basis for algorithms such as RSA (modular exponentiation) and algorithms based on discrete logarithms used in ECC (Koblitz, Menezes, & Vanstone, 2000).

The RSA algorithm, based on the difficulty of factoring large numbers, is widely used to secure communications and digital signatures. On the other hand, elliptic curve cryptography (ECC) leverages the complexity of the elliptic curve discrete logarithm problem and offers higher security with smaller key sizes, making it ideal for devices with limited computational power (Anon., The cryptographic hash function SHA-256, 2023).

## 3.2 Abstract Algebra: Groups

Abstract algebra deals with structures such as groups, rings, and fields, which are essential for understanding cryptographic algorithms.

A group is mathematically defined as a pair (G, +), where G is a finite set of elements and "+" is a binary operation. A group must have the following properties:

- **Closure under +**: $\forall x, y \in G, x + y \in G$
- **Associativity**: $\forall x, y, z \in G, (x + y) + z = x + (y + z)$
- **Identity element e ∈ G**: $\forall x \in G, e + x = x$
- Inverse elements: $\forall x \in G, -x \in G$ and $x + (-x) = e$

An Abelian group (commutative group) additionally has the property of commutativity:

- **Commutativity**: $\forall x, y \in G, x + y = y + x$

Non-zero integers modulo p $(Z/pZ-\{0\}=Zp^*)$, where p is a prime number, form a multiplicative group, which is very useful in cryptography, such as in the Diffie-Hellman key exchange and elliptic curve cryptography (ECC) (Koblitz, Menezes, & Vanstone, 2000).

## 3.3 Complexity Theory

Complexity theory analyzes the time and space requirements of algorithms. Understanding Big-O notation is crucial for analyzing the efficiency of these algorithms (Macedo, 2018).

- **P vs NP Problem**: The security of many cryptographic systems assumes that certain problems are "hard," meaning that there is no quick (polynomial-time) algorithm to solve them. The security of RSA relies on the assumption that factorization is hard (Aamir, 2019).
- **Quantum Computing**: Quantum computers can efficiently solve problems like integer factorization and discrete logarithms, which would jeopardize algorithms like RSA and ECC, motivating research in the field of post-quantum cryptography (Shor, 1999).

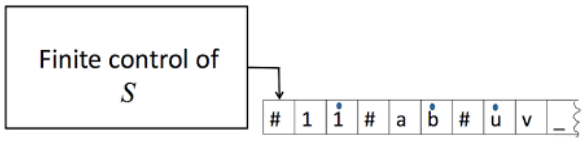


*Fig. 1: Illustrated Turing Machine*
*Source:* (Anon., 2011)

The image illustrates the concept of a Turing machine, a fundamental element in computational complexity theory. A Turing machine is a model of computation that consists of an infinite tape and a read-write head that can change states based on predefined rules. This model is crucial for understanding how computational problems are solved and the limits of computational capacity.

## 3.4 Cryptographic Protocols and Algorithms

**Hash Functions:** Hash functions, such as SHA-256 used in Bitcoin, transform input data into a fixed-length output and are designed to be fast and collision-resistant (i.e., to ensure that two different inputs do not produce the same output) (Anon., The cryptographic hash function SHA-256, 2023).

Hash functions can be categorized into cryptographic and non-cryptographic. Non-cryptographic hash functions are used, for example, in hash tables or for error detection (CRC), and do not protect against intentional collisions. Cryptographic hash functions, like SHA-256, are used in blockchain consensus protocols (e.g., Proof-of-Work), digital signatures, and encryption algorithms. For a cryptographic hash function to be considered secure, it must meet the following criteria:

- **Pre-image resistance**: Given a hash value h(m), it should be computationally infeasible to determine the original input m that maps to h(m).
- **Second pre-image resistance**: Given an input m1 and its hash value h(m1), it should be computationally infeasible to find a different input m2 such that h(m2) = h(m1).
- **Collision resistance**: It should be computationally infeasible to find two distinct inputs m1 and m2 such that h(m1) = h(m2).

A hash function cannot be inverted, even assuming an attacker with unlimited computational power. For example, there are $\mathbf{2^{256}}$ possible values for a 256-bit hash. Even if an attacker managed to find all possible pre-images for a specific hash (which would require, on average, $\mathbf{2^{256}}$ attempts), there are $\mathbf{2^{2048}}$ possible combinations of bits for a 2048-bit pre-image. According to the pigeonhole principle, if there are n pigeons and m pigeonholes, and n > m, then at least one pigeonhole must contain more than one pigeon. Therefore, for $\mathbf{2^{2048}}$ possible pre-images and $\mathbf{2^{256}}$ possible hash values, each hash value will, on average, correspond to $\mathbf{2^{1792}}$ different 2048-bit pre-images. Since all pre-images have the same probability, a specific pre-image m can never be uniquely determined (Anon., The cryptographic hash function SHA-256, 2023).

**Digital Signatures:** Digital signatures, such as ECDSA used in blockchain, provide a way to verify the identity of the sender and the integrity of the message. ECDSA uses elliptic curve cryptography (ECC), known for its high security and efficiency. Elliptic curves are mathematically represented by equations such as $\mathbf{y^2 = x^3 + Ax + B}$, allowing for secure and rapid key exchange. ECC is computationally more efficient than traditional methods, such as RSA, in achieving the same level of security. In the ECDSA system, a private key is used to create a signature, which can be verified by a public key. This process ensures that the message has not been altered and is authentic. Digital signatures are crucial for securing transactions in decentralized networks like blockchain (Sipser, 2021).

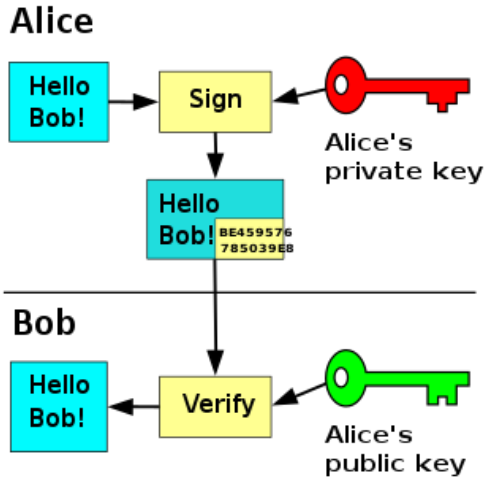


*Fig. 2: Public Key Digital Signature*
*Author:* (Wikipedia, 2024)

The illustration demonstrates the process of a digital signature using a public key. In public key cryptography, a pair of keys - a private key and a public key - is used to ensure the confidentiality and authenticity of messages. The private key is used to create a digital signature, which can be verified using the associated public key, thereby confirming the sender's identity and the integrity of the message.

## 3.5 Application in Blockchain Technology: Elliptic Curve Cryptography (ECC)

ECC leverages the properties of elliptic curves over finite fields. The security of ECC lies in the elliptic curve discrete logarithm problem (ECDLP), which exploits the commutative properties of the additive group of points on the curve.

Elliptic curves are mathematically described by the equation $\mathbf{y^2 = x^3 + Ax + B}$ (Anon., The cryptographic hash function SHA-256, 2023).

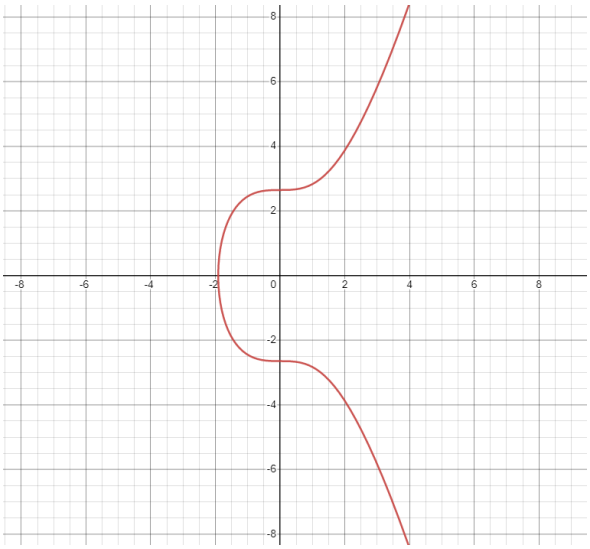

*Fig. 3: Continuous graph of the elliptic curve* $y^2 = x^3 + 7$ *, so that* $x,y \subseteq Rx, y$
*Source: Author*

The image shown in Fig. 3 depicts the graph of an elliptic curve, mathematically described by the equation

$$y^2 = x^3 + Ax + B \qquad \text{(Anon., 2019).}$$

This graph is important for understanding elliptic curves, which are used in elliptic curve cryptography (ECC). This type of cryptography is both efficient and secure, making it ideal for use in blockchain technologies.

- **Point Addition**: Adding two points, P and Q, on an elliptic curve can be visualized by drawing a line through these points. If this line intersects the elliptic curve at another point, the point directly below this intersection represents the sum P + Q.

The illustration shown in Fig. 4 depicts the process of adding two points, P and Q, on an elliptic curve. This operation is fundamental in elliptic curve cryptography (ECC), where point addition is used for encryption and decryption of information. Adding points on an elliptic curve is visualized by drawing a line through the two points, with the resulting point below the intersection representing the sum P + Q.

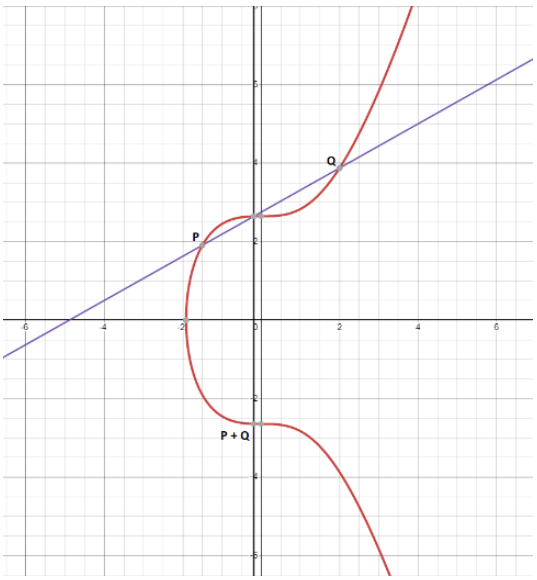


*Fig. 4: Addition of Points P + Q on an Elliptic Curve*
*Source: Author*

- **Inverse Points**: Adding a point and its inverse results in a virtual point O, known as the "point at infinity." This is represented as:

$$P + (-P) = O.$$

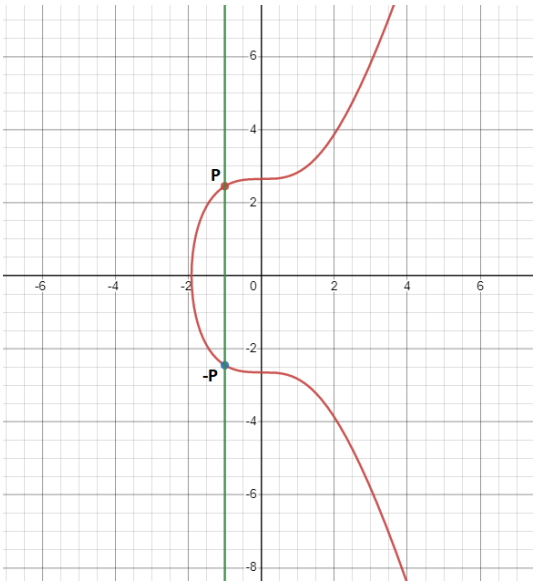


*Fig. 5: Addition of Inverse Points on an Elliptic Curve: P + (-P) = O*
*Source: Author*

Figure 5 illustrates the addition of point P and its inverse point -P on an elliptic curve, resulting in the virtual point O, known as the "point at infinity." The line connecting point P and its inverse -P does not intersect the elliptic curve but extends to infinity, representing the equation P + (-P) = O.

- **Point Doubling**: Doubling a point, P + P = 2P, is crucial for point multiplication, which is key to cryptographic applications of elliptic curves (Koblitz, Menezes, & Vanstone, 2000).

The illustration in Fig. 6 depicts the process of doubling a point P on an elliptic curve, which is a crucial operation in elliptic curve cryptography (ECC). This process involves finding the tangent at point P, determining the intersection of this tangent with the curve, and then reflecting the intersection point over the x-axis to get the resulting point 2P.

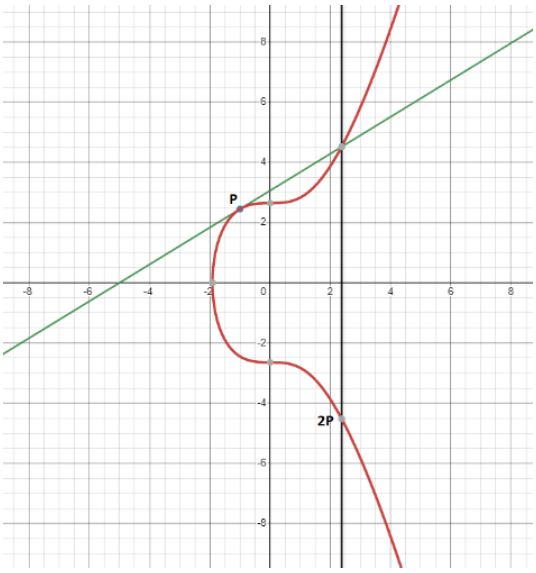


*Fig. 6: Doubling a Point: P+P=2P*
*Source: Author*

ECC employs the elliptic curve discrete logarithm problem (ECDLP), a variation of the discrete logarithm problem (DLP). In the ECDSA digital signature, the private key k is used to create a signature, while point Q serves as the public key (Koblitz, Menezes, & Vanstone, 2000).

## 3.6 Cryptography in Blockchain

In the blockchain context, cryptographic algorithms primarily focus on integrity and authenticity rather than privacy protection. The blockchains mainly use digital signatures to verify identity and secure messages. One of the most popular algorithms is the Elliptic Curve Digital Signature Algorithm (ECDSA), which is based on Elliptic Curve Cryptography (ECC) (Koblitz, Menezes, & Vanstone, 2000).

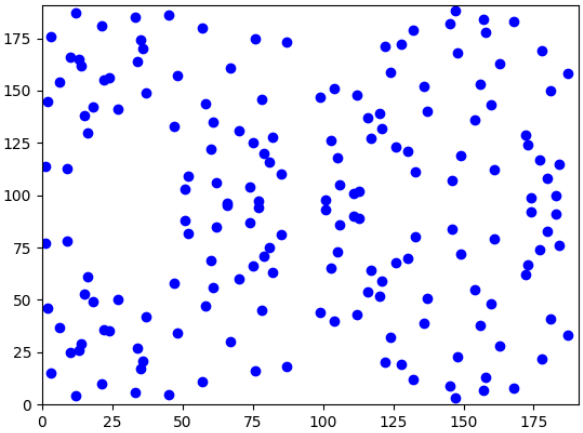

*Fig. 7: (x,y) where $x,y \subseteq Z_{191}$ a $y^2=x^3+7$*
*Source: Author*

The illustration shows a discrete graph of the elliptic curve $y^2 = x^3 + 7$ over the finite field $Z_{191}$, where x and y are integers within this range. This graph illustrates the use of the elliptic curve discrete logarithm problem (ECDLP) in elliptic curve cryptography (ECC), which underpins the ECDSA digital signature algorithm.

ECDSA is widely recognized for its security and efficiency, making it ideal for use in blockchain technologies. The advantage of ECDSA over RSA is that it requires a smaller key size to achieve the same level of security. For example, a 512-bit ECDSA key is computationally more efficient than a 4096-bit RSA key, leading to its increasing use in modern cryptography. These mathematical and theoretical concepts provide a key framework for understanding and developing secure cryptographic solutions. They are essential for the design and analysis of secure digital systems. ECDSA ensures that transactions in the blockchain network are authentic and immutable. These features make blockchain technology robust and reliable for decentralized applications (Koblitz, Menezes, & Vanstone, 2000).

## 3.7 Quantum Computing

Quantum computing has the potential to significantly weaken current cryptographic standards, such as RSA and ECC, which secure most blockchain technologies. Traditionally, it is

assumed that computational models for breaking ciphers are comparable to deterministic universal Turing machines or random access models (RAM). However, quantum computers introduce a new dimension to this field. Algorithms like Shor's algorithm leverage quantum computational models to enable polynomial-time computation of problems considered difficult in classical cryptography, such as integer factorization or the discrete logarithm problem (DLP). Shor's algorithm can efficiently factor large numbers and solve DLP, threatening the security of many cryptosystems that rely on these problems, such as RSA and ECC (Shor, 1999).

Quantum computers, although still in the development stage, have already achieved significant breakthroughs. For instance, companies like Google and IBM have developed quantum processors capable of performing complex computations that are beyond the reach of classical computers. This progress underscores the urgency of research in post-quantum cryptography, which includes algorithms resistant to quantum attacks, such as lattice-based cryptography and multivariate polynomial cryptography (Shor, 1999).

As a result, the security of blockchain transactions and digital signatures could be compromised. Quantum computing has the potential to dramatically increase efficiency in solving these problems, meaning that current cryptographic techniques could become ineffective in the future. Therefore, new cryptographic methods resistant to quantum attacks, known as post-quantum cryptography, are being developed. These methods include algorithms based on problems that are difficult for quantum computers, such as lattice-based cryptography or multivariate polynomial cryptography (Briggs, 1998).

While quantum computers are still not widely available and are in the research and development stage, blockchain and cryptographic system developers need to be prepared for this future technological leap. Implementing and testing post-quantum algorithms is essential to ensure the long-term security of blockchain technologies and cryptographic systems. This transition to new cryptographic standards will be crucial for maintaining security and trust in decentralized systems in the era of quantum computing. For developers and organizations, it is crucial to begin implementing and testing post-quantum cryptographic algorithms today to be prepared for future threats. Investment in the research and development of these technologies is essential for the long-term security and trustworthiness of blockchain systems (Briggs, 1998).

# 4 RESULTS

The results of my research demonstrate the effectiveness and security of cryptographic techniques used in blockchain technology. Here are the key findings:

## 4.1 Effectiveness of Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a vital component in blockchain security. ECC provides strong encryption with relatively small key sizes compared to traditional cryptographic methods like RSA. This efficiency makes ECC particularly suitable for blockchain applications, which require high security without compromising performance. ECC can achieve comparable security levels with significantly smaller keys, leading to faster computations and reduced storage requirements. The use of ECC in blockchain enhances transaction processing speed and reduces the computational load on network nodes.

## 4.2 Robustness of Hash Functions (SHA-256)

Hash functions, specifically SHA-256, play a crucial role in ensuring the integrity of blockchain transactions. SHA-256 is highly resilient to collision attacks, meaning it is extremely difficult for two different inputs to produce the same hash output. The probability of finding a collision in SHA-256 is negligible, reinforcing the trust in the blockchain's immutability. SHA-256 is computationally efficient, enabling quick verification of transaction data and blocks within the blockchain.

## 4.3 Role of Consensus Protocols (Proof-of-Work)

Consensus protocols, such as Proof-of-Work (PoW), are essential for maintaining the

consistency and security of blockchain networks. PoW is effective in preventing double-spending and ensuring that all nodes agree on the blockchain's current state. The computational effort required for PoW (e.g., solving cryptographic puzzles) acts as a deterrent against malicious attacks, making the network more secure. However, PoW is resource-intensive, leading to high energy consumption. This highlights the need for more sustainable alternatives or optimizations.

### 4.4 Impact of Quantum Computing

Quantum computing poses a potential threat to current cryptographic standards, including those used in blockchain technology. The study examines the vulnerabilities introduced by quantum algorithms, such as Shor's algorithm, which can efficiently solve problems that are difficult for classical computers (e.g., factoring large integers and calculating discrete logarithms). If quantum computers become practical, they could break the cryptographic algorithms (RSA, ECC) that underlie blockchain security. This necessitates the development and adoption of post-quantum cryptographic algorithms that are resistant to quantum attacks.

### 4.5 Post-Quantum Cryptography Solutions

In response to the threat of quantum computing, the study explores post-quantum cryptographic solutions that can be integrated into blockchain technology. These solutions are designed to be secure against quantum attacks. Key findings include lattice-based cryptography and multivariate polynomial cryptography, which are promising candidates for post-quantum security. Implementing these post-quantum solutions in blockchain will require careful consideration of computational efficiency and integration with existing blockchain protocols.

### 4.6 Conclusions of the Results

The research confirms that current cryptographic techniques are effective in securing blockchain technology. However, the threat of quantum computing necessitates a proactive approach to adopting post-quantum cryptographic solutions. Continuous research and development are crucial to maintaining the security and efficiency of blockchain networks in the face of evolving technological challenges.

## 5 CONCLUSIONS

In the rapidly evolving landscape of decentralized information networks, particularly within blockchain technology, cryptography plays a crucial role. As the backbone of cryptographic security, it ensures the confidentiality, integrity, and authentication of data within these networks.

Today, decentralized networks often employ sophisticated encryption methods such as RSA, ECC (Elliptic Curve Cryptography), and AES (Advanced Encryption Standard) to secure data transmission. Public key cryptography is widely used in blockchain to secure transactions and create digital signatures, ensuring that only authorized parties can process the data.

Blockchain networks, whether private or public, are increasingly adopting these advanced encryption methods. Private networks focus on internal security and data privacy, while public networks emphasize transparency and broad accessibility.

As networks expand, maintaining the efficiency of cryptographic operations becomes challenging, especially in large-scale public sector applications. The advent of quantum computing poses a significant threat to current cryptographic standards, as quantum algorithms could potentially break many of the encryption methods in use today.

Ensuring interoperability between private and public blockchain networks while maintaining robust cryptographic standards is a significant challenge. Different networks may use various encryption methods, complicating secure communication between platforms. Adhering to diverse data protection laws and regulations, particularly in public sector applications, requires a delicate balance while maintaining stringent encryption standards.

Effective management of cryptographic keys is essential, as their loss or theft can lead to severe security breaches, particularly in private

blockchain networks where access control is critical.

With the growing influence of decentralized networks in both the private and public sectors, the role of encryption in ensuring their security and trust is indispensable. While the current state reflects strong foundations in cryptography, the industry must proactively address challenges related to scalability, quantum threats, interoperability, regulatory compliance, and key management to maintain robust, secure, and efficient networks. The future of these networks depends on their ability to adapt and evolve in response to these emerging challenges.

My study emphasizes the importance of advanced cryptographic techniques for ensuring the confidentiality, integrity, and authenticity of data. Quantum computing poses a potential threat, making it crucial to continue research in post-quantum cryptography. The future of blockchain technology depends on the ability to adapt to these new challenges and maintain a high level of security.

## WORKS CITED

Aamir, B. (2019). *P Vs NP Problem In A Nutshell.* Retrieved from https://medium.com/@bilalaamir/p-vs-np-problem-in-a-nutshell-dbf08133bec5

Abelson, H., Ledeen, K., & Lewis, H. (2008, Jun 3). *Secret Bits: How Codes Became Unbreakable*. Retrieved from informIT: https://www.informit.com/articles/article.aspx?p=1218422

Anon. (2019, Apr 24). *Secp256k1*. Retrieved from Bitcoin.it: https://en.bitcoin.it/wiki/Secp256k1

Anon. (2023). *The cryptographic hash function SHA-256*. Retrieved from https://helix.stormhub.org/papers/SHA-256.pdf

Anon. (n.d.). *TURING MACHINES*. Retrieved from andrew.cmu.edu: https://www.andrew.cmu.edu/user/ko/pdfs/lecture-13.pdf

Briggs, M. E. (1998, Apr 17). *An Introduction to the General Number Field Sieve.* Retrieved from Virginia Tech.: https://vtechworks.lib.vt.edu/items/3b866f8e-d533-48ae-a671-b88e4cb0a7bc

Buterin, V. (2014). *Ethereum Whitepaper.* Retrieved from https://ethereum.org/en/whitepaper/

Contributors. (2013, Jul). *Trapdoor function*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Trapdoor_function

Contributors. (2024, Jan). *Public-key cryptography*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Public-key_cryptography

Gallian. (2021). *Contemporary abstract algebra.* CRC Taylor & Francis Group.

Koblitz, N., Menezes, A., & Vanstone, S. (2000, Mar). The State of Elliptic Curve Cryptography. *Designs, Codes and Cryptography, 19*, 173-193. doi:10.1023/A:1008354106356

Macedo, C. (2018). *www.Dev4Devs.com*. Retrieved from What is the Big-O?: https://dev4devs.com/2018/01/19/understanding-the-big-o-how-to-think-to-develop-good-and-fast-and-performatic-solutions/

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from https://bitcoin.org/bitcoin.pdf

Shor, P. W. (1999). *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* Retrieved from https://epubs.siam.org/doi/10.1137/S0036144598347011

Sipser. (2021). *Introduction to the theory of computation.* Cengage Learning.

Received for publication: 01.07.2024
Revision received: 08.07.2024
Accepted for publication: 08.01.2025.

***How to cite this article?***

Style – **APA** *Sixth Edition:*

Feltovic, M. (2025, 01 15). Cryptographic Foundations for Blockchain Security in Decentralized Networks. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 52-61. doi:10.12709/mest.13.13.01.05

Style – **Chicago** *Sixteenth Edition:*

Feltovic, Milan. "Cryptographic Foundations for Blockchain Security in Decentralized Networks." Edited by Zoran Cekerevac. *MEST Journal* (MESTE ) 13, no. 1 (01 2025): 52-61.

Style – **GOST** *Name Sort:*

**Feltovic Milan** Cryptographic Foundations for Blockchain Security in Decentralized Networks [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE , 01 15, 2025. - 1 : Vol. 13. - pp. 52-61.

Style – **Harvard** *Anglia:*

Feltovic, M., 2025. Cryptographic Foundations for Blockchain Security in Decentralized Networks. *MEST Journal,* 15 01, 13(1), pp. 52-61.

Style – **ISO 690** *Numerical Reference:*

*Cryptographic Foundations for Blockchain Security in Decentralized Networks.* **Feltovic, Milan.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE , 01 15, 2025, MEST Journal, Vol. 13, pp. 52-61.