MEST Journal
DOI 10.12709/mest.12.12.02.12

FROM THEORY TO PRACTICE: THE ROLE OF CRYPTOGRAPHY IN SECURING BLOCKCHAIN NETWORKS

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

CC BY

JEL Category: **C88**

Abstract

Blockchain technology has evolved from its origins in cryptocurrencies to become a fundamental component of secure digital interactions across diverse sectors, including healthcare, finance, and public administration. This article delves into the theoretical and practical applications of cryptography within blockchain networks, emphasizing key cryptographic functions, algorithms, and protocols such as RSA, elliptic curve cryptography (ECC), and SHA-256. It scrutinizes the use of digital signatures for transaction verification and the crucial role of hash functions in ensuring data integrity. Additionally, the article presents practical examples of symmetric and asymmetric encryption methods, underscoring their significance in maintaining privacy and security. The study also highlights the emerging challenges posed by quantum computing and explores ongoing research in post-quantum cryptography. Furthermore, it provides insights into the advancements in cryptographic techniques essential for the robustness of decentralized networks. By linking theoretical frameworks with practical implementations, this article aims to offer a comprehensive understanding of the cryptographic security measures pivotal for the future of blockchain technology.

Keywords: *Elliptic curve cryptography (ECC), RSA algorithm, SHA-256, proof-of-work, digital signature, post-quantum cryptography, cryptographic protocol.*

1 INTRODUCTION

In the ever-evolving digital landscape, blockchain technology has emerged as a transformative force with the potential to revolutionize industries far beyond its initial application in cryptocurrencies like Bitcoin (Nakamoto, 2009). As blockchain continues to gain traction across various sectors, including healthcare, finance, and public administration, the need for robust security measures becomes increasingly critical. At the heart of blockchain security lies cryptography, a field that provides the essential tools and techniques to ensure the integrity, confidentiality, and authenticity of digital transactions (Stormhub, 2023).

This article delves into the theoretical and practical aspects of cryptography within blockchain networks, highlighting how these techniques are

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

employed to secure decentralized systems. We will explore fundamental cryptographic functions, algorithms, and protocols such as RSA, elliptic curve cryptography (ECC), and SHA-256, which form the backbone of blockchain security (Koblitz, Menezes, & Vanstone, 2000). Additionally, we will examine the role of digital signatures in verifying transaction authenticity and the importance of hash functions in maintaining data integrity (Briggs, 1998).

Moving from theory to practice, this article will provide real-world examples of how cryptographic techniques are implemented in blockchain platforms like Bitcoin and Ethereum (Shor, 1999). We will also discuss the emerging challenges posed by quantum computing and the ongoing research in post-quantum cryptography aimed at safeguarding blockchain networks against future threats (n.d., 2008).

By bridging theoretical concepts with practical applications, this article aims to enhance understanding of the critical role cryptography plays in securing blockchain networks and to provide insights into the future directions of blockchain security (Wikipedia, 2024).

This article focuses on addressing three key research questions.

R_1 - What key cryptographic functions and algorithms are used in blockchain networks?

R_2 - How these cryptographic techniques are implemented on various blockchain platforms?

R3 - What are the main challenges and future directions in cryptography for blockchain development?

2 METHODS

To answer the first two research questions, I analyzed technical documentation and case studies from major blockchain platforms such as Bitcoin and Ethereum. To address the third question, I evaluated current research publications on the impact of quantum computing on cryptographic standards and conducted expert interviews with cryptography specialists.

Blockchain technology, initially developed as the underlying architecture for the cryptocurrency Bitcoin, has rapidly evolved into a subject of significant interest across various industries. Its application now spans finance, healthcare, logistics, and beyond, providing decentralized solutions that enhance transparency and reduce the need for third-party verification in transactions. At the core of blockchain's secure and efficient operation lies cryptography (Buterin, 2024).

Cryptographic Functions, Algorithms, and Protocols: Cryptographic functions are essential for securing data and communications in blockchain networks. They ensure confidentiality, data integrity, and authentication, forming the backbone of secure transactions. Key cryptographic algorithms such as RSA (Rivest-Shamir-Adleman) and elliptic curve cryptography (ECC) leverage mathematical principles to provide robust security (Koblitz, Menezes, & Vanstone, 2000). RSA relies on the difficulty of factoring large numbers, while ECC uses the complexity of the elliptic curve discrete logarithm problem, offering higher security with smaller key sizes, which is crucial for devices with limited computational power (Briggs, 1998).

Cryptographic protocols like SSL/TLS (Secure Sockets Layer/Transport Layer Security) and IPsec (Internet Protocol Security) play a vital role in securing communications over networks (Shor, 1999). These protocols use cryptographic algorithms to encrypt data and ensure secure data transmission, preventing unauthorized access and tampering (n.d., 2008).

The importance of cryptography in blockchain technologies and decentralized networks is not just theoretical. Real-world examples of attacks and security incidents demonstrate how critical it is to implement cryptographic methods correctly. For instance, in 2014, Mt. Gox, at that time, the largest bitcoin exchange in the world, became a victim of a massive hacking attack. The attackers exploited a flaw in the Bitcoin protocol implementation known as "transaction malleability" and stole approximately 850,000 bitcoins, worth around $450 million at that time (Decker & Wattenhofer, 2014). This incident highlighted the importance of cryptographic protocols' proper implementation in blockchain systems.

Hash Functions, Algorithms, and Protocols:

Hash functions are integral to blockchain technology, ensuring data integrity and

authenticity (Wikipedia, 2024). A hash function transforms input data of any size into a fixed-size string of characters, typically a hash value. The SHA-256 (Secure Hash Algorithm 256-bit) is widely used in blockchain for creating secure and unique digital fingerprints of data (Wikipedia, 2022B).

In blockchain, hash functions are used in consensus protocols like Proof-of-Work (PoW). In PoW, miners compete to solve complex mathematical puzzles based on hash functions, ensuring that each block added to the blockchain is valid and secure (Cormen, Leiserson, Rivest, & Stein, 2022). This mechanism not only maintains the integrity of the blockchain but also prevents double-spending and fraud (Rolland, 2015).

The importance of correct implementation of hashing functions and cryptographic protocols was dramatically illustrated by the Heartbleed bug in 2014. This critical flaw in the popular cryptographic software library OpenSSL allowed attackers to access sensitive information, including private keys (Durumeric, et al., 2014). The incident underscored the necessity of regular security audits of cryptographic libraries and the proper implementation of protocols.

Digital Signatures: Functions, Algorithms, and Protocols: Digital signatures are cryptographic techniques that provide authentication, integrity, and non-repudiation of digital messages and transactions. They ensure that a message or transaction has been created by a known sender and has not been altered in transit (Wiki, 2019).

Algorithms such as RSA and ECDSA (Elliptic Curve Digital Signature Algorithm) are commonly used for creating digital signatures (n.d., 2011). RSA, with its foundation in number theory, and ECDSA, leveraging the elliptic curve discrete logarithm problem, offer secure methods for verifying digital signatures (Camilamacedo86, 2018). These algorithms are essential in blockchain for signing transactions, ensuring they are authorized and legitimate (Aamir, 2019).

Protocols like PGP (Pretty Good Privacy) use digital signatures to secure email communications, highlighting the widespread application of these cryptographic techniques beyond blockchain (Boehme, Christin, Edelman, & Moore, 2015).

The importance of correctly implementing ECC was highlighted in the case of Blockchain.info in 2015. A flaw in the random number generator of this popular Bitcoin wallet led to the creation of weak private keys. The quick detection and resolution of the issue prevented a potentially massive loss of bitcoins (Courtois, Emirdag, & Valsorda, 2014). This incident underscores that even a small error in the cryptographic algorithms implementation can have serious consequences.

Quantum Computing and Cryptography: One of the emerging challenges in the field of cryptography is the advent of quantum computing. Quantum computers have the ability to solve complex mathematical problems exponentially faster than classical computers. Therefore, they pose a significant threat to current cryptographic standards (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016). Algorithms like Shor's algorithm can efficiently factor large numbers and solve discrete logarithms, potentially breaking RSA and ECC-based cryptographic systems (Zohar, 2015).

To address this threat, researchers are developing post-quantum cryptographic algorithms resistant to quantum attacks (Antonopoulos, 2014). These new algorithms aim to provide security even in the presence of powerful quantum computers, ensuring the continued integrity and blockchain network security (Bonneau, et al., 2015).

2.1 Cryptographic Functions in Blockchain

RSA and ECC in Blockchain: RSA (Rivest-Shamir-Adleman) and elliptic curve cryptography (ECC) are essential cryptographic algorithms used to secure blockchain networks. RSA is based on the difficulty of factoring large numbers when ECC relies on the complexity of the elliptic curve discrete logarithm problem. Both algorithms provide robust security for key exchange and digital signatures.

Bitcoin utilizes ECC, specifically the Elliptic Curve Digital Signature Algorithm (ECDSA), to ensure the authenticity of transactions. When a user initiates a transaction, their private key generates a digital signature, which is then verified using the corresponding public key (Briggs, 1998; Shor, 1999). This process ensures that the transaction was initiated by the legitimate owner of the funds.

Protocols Utilizing Cryptographic Functions: Cryptographic protocols such as SSL/TLS (Secure Sockets Layer/Transport Layer Security) and IPsec (Internet Protocol Security) are crucial for securing communications over networks. These protocols use cryptographic algorithms to encrypt data and ensure their secure transmission, preventing unauthorized access and tampering (n.d., 2008).

In blockchain networks, SSL/TLS protocols can be used to secure communication between nodes, ensuring that data transmitted across the network remains confidential and unaltered (Wikipedia, 2024).

2.2 Hash Functions in Blockchain

SHA-256 in Bitcoin Proof-of-Work: Hash functions are essential for ensuring data integrity and authenticity in the blockchain. SHA-256 (Secure Hash Algorithm 256-bit) is widely used in blockchain for creating secure and unique digital fingerprints of data (Wikipedia, 2022B).

In Bitcoin, miners compete to solve complex mathematical puzzles based on SHA-256. Miners must find a hash value that meets a specific criterion, which requires substantial computational effort. Once a miner finds a valid hash, he can add a new block to the blockchain. This process secures the network by making it computationally infeasible for malicious actors to alter the blockchain (Cormen, Leiserson, Rivest, & Stein, 2022).

Data Integrity and Tamper-Proofing: Hash functions ensure that any changes to the input data result in a completely different hash value, making it easy to detect tampering (Rolland, 2015).

When a transaction is added to a blockchain, its details are hashed and included in a block. Any alteration in the transaction details would result in a different hash value, alerting the network to potential tampering (Wiki, 2019). This mechanism ensures the integrity and immutability of blockchain data (n.d., 2011).

2.3 Digital Signatures in Blockchain

ECDSA for Transaction Verification: Digital signatures provide authentication and integrity for blockchain transactions. ECDSA is widely used in blockchain to ensure that transactions are authorized and legitimate (Camilamacedo86, 2018).

Both Bitcoin and Ethereum use ECDSA for transaction verification. When a user signs a transaction with their private key, it creates a digital signature. The network nodes then use the public key to verify the signature, ensuring the transaction is valid and has not been altered (Aamir, 2019).

Ensuring Transaction Authenticity: Digital signatures ensure that transactions are initiated by legitimate users and have not been altered during transmission (Boehme, Christin, Edelman, & Moore, 2015).

In blockchain-based voting systems, digital signatures can be used to verify voter identities and ensure that votes are cast legitimately. Each vote is digitally signed by the voter and verified by the network, preventing fraudulent voting and ensuring the integrity of the election process (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016).

2.4 Cryptography and Encryption in Practice

Cryptography and encryption are fundamental components of blockchain technology, ensuring the confidentiality, integrity, and authenticity of data within decentralized networks (Zohar, 2015). This section explores the practical applications of symmetric and asymmetric encryption in blockchain, highlighting their roles in securing communications, protecting data, and enabling trustless transactions (Antonopoulos, 2014).

2.4.1 Symmetric Encryption in Blockchain

Symmetric Encryption (AES): Symmetric encryption, where the same key is used for both, encryption and decryption, is highly efficient for securing large amounts of data. The Advanced Encryption Standard (AES) is a widely adopted symmetric encryption algorithm known for its speed and security (Bonneau, et al., 2015).

In blockchain applications for healthcare, patient records can be encrypted using AES before being stored on the blockchain. This ensures that sensitive medical information remains confidential

and is only accessible to authorized parties with the decryption key (Nakamoto, 2009). By using AES, healthcare providers can protect patient privacy while leveraging the transparency and immutability of blockchain technology (Buterin, 2024).

Efficient Data Protection: Symmetric encryption is particularly useful for protecting data at rest and ensuring the confidentiality of large datasets (Stormhub, 2023).

Blockchain platforms can use AES to encrypt large volumes of data stored within the network. For example, a decentralized storage solution like IPFS (InterPlanetary File System) can encrypt files using AES, ensuring that even if data is distributed across multiple nodes, it remains secure and accessible only to those with the appropriate decryption keys (Koblitz, Menezes, & Vanstone, 2000).

2.4.2 Asymmetric Encryption in Blockchain

Asymmetric Encryption (RSA and ECC): Asymmetric encryption, which uses a pair of keys (public and private) for encryption and decryption, is essential for secure key exchange and digital signatures. RSA (Rivest-Shamir-Adleman) and elliptic curve cryptography (ECC) are two prominent asymmetric encryption algorithms (Briggs, 1998).

In blockchain networks, asymmetric encryption is used to secure exchange keys over public channels. For instance, when a user wants to share a symmetric encryption key with another user, they can encrypt it using the recipient's public key (RSA or ECC). Only the recipient, who possesses the corresponding private key, can decrypt and access the symmetric key, ensuring secure communication (Shor, 1999).

Digital Signatures: Asymmetric encryption also underpins digital signatures, which provide authentication and ensure the integrity of messages and transactions (n.d., 2008).

Bitcoin and Ethereum use the Elliptic Curve Digital Signature Algorithm (ECDSA) to verify transactions. When a user initiates a transaction, it is signed with their private key, creating a digital signature. Network nodes then use the public key to verify the signature, ensuring the transaction is authentic and has not been tampered with. This mechanism prevents unauthorized transactions and maintains the integrity of the blockchain (Wikipedia, 2024).

2.4.3 Hybrid Encryption Approaches

Many blockchain applications use a hybrid approach, combining the efficiency of symmetric encryption with the security of asymmetric encryption (Wikipedia, 2022B).

In secure messaging applications built on blockchain, a hybrid approach is often used. Messages are encrypted using a symmetric key (e.g., AES), ensuring fast and efficient encryption. The symmetric key is then encrypted with the recipient's public key (RSA or ECC) and sent along with the message. This ensures that only the intended recipient can decrypt the symmetric key with their private key and subsequently decrypt the message. This method provides both efficiency and security in communication (Cormen, Leiserson, Rivest, & Stein, 2022).

2.4.4 Cryptographic Protocols and Practical Implementations

TLS/SSL for Secure Communications: Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide secure communication over a computer network (Rolland, 2015).

Blockchain nodes communicate with each other over the network, often using TLS/SSL to encrypt the data transmitted between nodes. This prevents eavesdropping and tampering by ensuring that all data exchanged between nodes remains confidential and authentic (Wiki, 2019).

IPsec for Network Security: Internet Protocol Security (IPsec) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session (n.d., 2011).

In private blockchain networks, IPsec can be used to secure communications between different nodes and data centers. By encrypting and authenticating IP packets, IPsec ensures that data transmitted over the network is protected from interception and tampering, providing a robust security layer for blockchain infrastructure (Camilamacedo86, 2018).

2.5 Case Studies

To illustrate the practical applications of cryptographic techniques in securing blockchain networks, this section examines specific case studies of prominent blockchain platforms (Aamir, 2019). We will explore how Bitcoin and Ethereum implement cryptographic functions, hash functions, digital signatures, and encryption to ensure the security and integrity of their networks. Additionally, we will look at other notable blockchain platforms such as Hyperledger Fabric and Ripple to understand their unique approaches to cryptographic security (Boehme, Christin, Edelman, & Moore, 2015).

2.5.1 Bitcoin

Cryptographic Techniques in Bitcoin: Bitcoin, the first and most well-known cryptocurrency, relies heavily on cryptographic techniques to secure its network. The primary cryptographic components used in Bitcoin include SHA-256, ECDSA, and Proof-of-Work (PoW) (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016).

- **SHA-256 and Proof-of-Work**: Bitcoin employs the SHA-256 hash function in its Proof-of-Work consensus mechanism. Miners compete to solve a complex cryptographic puzzle by finding a hash value that meets a specific criterion. This process requires significant computational effort, ensuring that new block creation is resource-intensive and secure. The first miner to solve the puzzle adds the new block to the blockchain and is rewarded with newly minted bitcoins (Zohar, 2015).
- **ECDSA for Transaction Verification**: Bitcoin uses the Elliptic Curve Digital Signature Algorithm (ECDSA) to ensure the authenticity of transactions. Each transaction is signed with the sender's private key, generating a digital signature. Network nodes verify this signature using the sender's public key, ensuring that the transaction was indeed authorized by the legitimate owner of the funds (Antonopoulos, 2014).
- **Example - Bitcoin Transaction**: When a user initiates a Bitcoin transaction, they sign the transaction data with their private key, creating a digital signature. This signature is then broadcast to the network, where nodes use the public key to verify the authenticity of the transaction. Once verified, the transaction is included in a block and added to the blockchain through the PoW process (Bonneau, et al., 2015).

2.5.2 Ethereum

Cryptographic Techniques in Ethereum: Ethereum, the second most well-known cryptocurrency after Bitcoin, employs various cryptographic techniques to secure its network and enable the functioning of smart contracts. The primary cryptographic components used in Ethereum include SHA-3, ECDSA, and the Proof-of-Stake (PoS) consensus mechanism (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016).

- **SHA-3 and Proof-of-Work/Proof-of-Stake:** Ethereum uses the SHA-3 (also known as Keccak-256) hash function for its cryptographic operations. Initially, Ethereum employed a Proof-of-Work (PoW) mechanism similar to Bitcoin, but it is gradually transitioning to Proof-of-Stake (PoS). In the PoS mechanism, block validators are selected based on the amount of ether (ETH) they hold and are willing to "stake" as collateral (Zohar, 2015).
- **ECDSA for Transaction Verification:** Like Bitcoin, Ethereum uses the Elliptic Curve Digital Signature Algorithm (ECDSA) to ensure transaction authenticity. Digital signatures are generated using the sender's private keys and verified using their public keys, ensuring that transactions are authorized by the legitimate owners of the funds (Zohar, 2015).
- **Example - Ethereum Transaction:** When users initiate transactions in Ethereum, they sign the transaction data with their private keys, creating a digital signature. This signature is then broadcast to the network, where nodes use the public key to verify the transaction's authenticity. Once verified, the transaction is included in a block and added to the blockchain through either the PoW or PoS mechanism (Bonneau, et al., 2015).

2.5.3 Hyperledger Fabric

Cryptographic Techniques in Hyperledger Fabric: Hyperledger Fabric is a modular and

configurable platform for building blockchain applications, designed primarily for enterprise use. It employs various cryptographic techniques to secure its network and manage identities.

- **Modular Cryptography:** Hyperledger Fabric allows the use of different cryptographic algorithms depending on the application needs. The most commonly used are ECDSA for digital signatures and hash functions like SHA-256 for ensuring data integrity (Zohar, 2015).
- **X.509 Certificates for Identity Management:** Hyperledger Fabric utilizes X.509 certificates to authenticate network participants. These certificates are issued by a Certificate Authority (CA) and are used to authenticate users and nodes within the network (Zohar, 2015).
- **Example - Transaction in Hyperledger Fabric:** When initiating a transaction in Hyperledger Fabric, the user creates a transaction proposal, which is signed with their private key and verified by other network members using their X.509 certificates. Once verified, the transaction is endorsed and added to the blockchain (Bonneau, et al., 2015).

2.5.4 Ripple

Cryptographic Techniques in Ripple: Ripple is a distributed system focused on fast and low-cost transactions, often used by financial institutions for cross-border payments. It employs several cryptographic techniques to secure its operations.

- **SHA-512Half:** Ripple uses a variant of SHA-512 called SHA-512Half for hashing transactions and other critical operations within the network. This algorithm ensures data integrity and processing speed (Zohar, 2015).
- **ECDSA and Ed25519 for Digital Signatures:** Ripple supports two main types of digital signatures - ECDSA and Ed25519. ECDSA is similar to Bitcoin and Ethereum, while Ed25519 offers higher speed and security for signing transactions (Zohar, 2015).
- **Example - Ripple Transaction:** When a user initiates a transaction in Ripple, the transaction data is signed using the user's private key, and the resulting digital signature is broadcast to the network. Validators in the network verify this signature, and once successfully verified, the transaction is added to the Ripple ledger (Bonneau, et al., 2015).

3 RESULTS

My analysis revealed that cryptographic functions like SHA-256 and algorithms such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) are fundamental pillars in securing blockchain transactions. SHA-256, a hashing function, is widely used in the Bitcoin network, where it transforms transaction inputs into a compact, 256-bit output, ensuring data integrity and immutability. On the other hand, Ethereum, aiming for higher efficiency and security, utilizes SHA-3 as part of its Proof-of-Work protocol. SHA-3 provides better resistance against cryptanalytic attacks compared to previous versions of hashing algorithms.

RSA and ECC algorithms are used for securing digital signatures and encryption in blockchain applications. RSA employs two key numbers – a public key and a private key – for encrypting and decrypting information, allowing secure key exchange even over unsecured channels. ECC, known for its efficiency with smaller key sizes and faster operations, is preferred in modern blockchain platforms like Ethereum for faster and more secure transactions.

One of the main challenges identified in my analysis is the security risks associated with the gradual development of quantum computers. Quantum computers pose a potential threat to traditional cryptographic schemes like RSA and ECC due to their ability to quickly solve factorization and discrete logarithm problems, on which these schemes are based. The growing need to develop post-quantum cryptography is crucial to prevent possible attacks that could compromise current encryption techniques and the overall integrity of blockchain networks.

4 CONCLUSIONS

As blockchain technology continues to evolve, addressing these future challenges will be critical to maintaining the security, efficiency, and trustworthiness of decentralized networks. Cryptographic techniques have proven to be

fundamental in securing blockchain platforms, enabling trustless transactions, and ensuring data integrity and privacy. The practical implementations of cryptographic algorithms like RSA, ECC, and SHA-256, along with digital signatures, have solidified the foundation of current blockchain systems.

However, the advent of quantum computing poses a significant threat to existing cryptographic standards. Post-quantum cryptography research is essential to develop algorithms that can withstand quantum attacks, ensuring the long-term security of blockchain networks. Scalability remains another critical challenge, with ongoing research into Layer 2 solutions, sharding, and other innovative approaches aimed at enhancing transaction throughput and reducing energy consumption.

Privacy and confidentiality are paramount, especially as public blockchains expose transaction details. Technologies such as Zero-Knowledge Proofs and zk-SNARKs offer promising solutions to maintain privacy without compromising the transparency and immutability of the blockchain. Additionally, regulatory and compliance frameworks must evolve with technological advancements to foster innovation while ensuring legal adherence. Integrating KYC and AML protocols into blockchain systems is a step towards achieving this balance.

Interoperability between diverse blockchain networks is also crucial for a connected ecosystem. Solutions like cross-chain protocols, atomic swaps, and blockchain bridges are being developed to facilitate seamless interactions across different platforms.

By staying ahead of these challenges through continuous research and development, the blockchain community can ensure that the technology remains robust and resilient in the face of emerging threats and opportunities. The ongoing advancements in cryptography, scalability, privacy, regulatory compliance, and interoperability will be instrumental in realizing the full potential of blockchain technology across various sectors, driving its sustained growth and adoption.

In conclusion, my findings highlight the critical role of advanced cryptography in the protection and sustainability of blockchain networks. It is essential to continue innovating and developing new cryptographic approaches to prevent security threats while simultaneously supporting the expansion and adoption of blockchain technologies across various sectors.

WORKS CITED

Aamir, B. (2019, Mar 25). *P Vs NP Problem In A Nutshell.* Retrieved from Medium: https://medium.com/@bilalaamir/p-vs-np-problem-in-a-nutshell-dbf08133bec5

Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking digital cryptocurrencies.* O'Reilly Media, Inc.

Boehme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213-238. Retrieved from https://www.aeaweb.org/articles?id=10.1257/jep.29.2.213

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies. *IEEE Symposium on Security and Privacy*, (pp. 104-121). Retrieved from https://ieeexplore.ieee.org/document/7163021

Briggs, M. E. (1998). *An introduction to the general number field sieve.* Blacksburg, Virginia: Virginia Polytechnic Institute and State University. Retrieved from https://vtechworks.lib.vt.edu/handle/10919/36618

Buterin, V. (2024, Mar 14). *Ethereum Whitepaper*. Retrieved Jul 03, 2024, from Ethereum.org: https://ethereum.org/en/whitepaper/

Camilamacedo86. (2018, Jan 19). *What is the Big-O?* Retrieved from Dev4Devs.com: https://dev4devs.com/2018/01/19/understanding-the-big-o-how-to-think-to-develop-good-and-fast-and-performatic-solutions/

Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2022). *Introduction to algorithms (4th ed.).* Cambridge, MA: MIT Press.

Courtois, N. T., Emirdag, P., & Valsorda, F. (2014). *Private key recovery combination attacks: On extreme fragility of popular bitcoin key management wallet and cold storage solutions in presence of poor RNG events*. Retrieved from Cryptology ePrint Archive, Paper 2014/848: https://eprint.iacr.org/2014/848

Decker, C., & Wattenhofer, R. (2014). Bitcoin transaction malleability and MtGox. *European Symposium on Research in Computer Security* (pp. 313-326). Cham: Springer. Retrieved from https://doi.org/10.1007/978-3-319-11212-1_18

Durumeric, Z., Li, F., Kasten, J., Amann, J., Beekman, J., Payer, M., & Halderman, J. A. (2014). The matter of heartbleed. *Proceedings of the 2014 Conference on Internet Measurement Conference*, (pp. 475-488). doi:10.1145/2663716.2663755

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

n.d. (2008, Jun 03). *Secret Bits: How Codes Became Unbreakable.* Retrieved from infirmIT: https://www.informit.com/articles/article.aspx?p=1218422

n.d. (2011, Spring). *Formal languages, Automata and Computation: Turing Machines.* Retrieved from Carnegie Mellon University in Qatar: https://www.andrew.cmu.edu/user/ko/pdfs/lecture-13.pdf

Nakamoto, S. (2009). *Bitcoin - A Peer-to-Peer Electronic Cash System*. Retrieved from 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.

Rolland, R. (2015). Randomness in cryptography. In *Lecture Notes in Computer Science.* Springer. Retrieved from https://link.springer.com/chapter/10.1007/978-3-319-18275-9_20

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review, 41*(2), 303-332. doi:10.1137/s0036144598347011

Stormhub. (2023, 05 09). *The cryptographic hash function SHA-256 MAII - FIB.* Retrieved Jul 03, 2024, from helix.stormhub.org: https://helix.stormhub.org/papers/SHA-256.pdf

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

Wikipedia. (2022B, Jun 27). *Public-key cryptography*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Public-key_cryptography

Wikipedia. (2024, Jun 25). *Trapdoor function*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Trapdoor_function

Zohar, A. (2015). Bitcoin: Under the hood. *Communications of the ACM, 58*(9), 104-113. Retrieved from https://cacm.acm.org/research/bitcoin/

Received for publication: 21.06.2024
Revision received: 05.07.2024
Accepted for publication: 09.07.2024

How to cite this article?

Style – **APA** *Sixth Edition:*

Feltovic, M. (2024, 07 15). From Theory to Practice: The Role of Cryptography in Securing Blockchain Networks. (Z. Čekerevac, Ed.) *MEST Journal, 12*(2), 93-102. doi:10.12709/mest.12.12.02.12

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

Feltovic, Milan. "From Theory to Practice: The Role of Cryptography in Securing Blockchain Networks." Edited by Zoran Čekerevac. *MEST Journal* (MESTE) 12, no. 2 (07 2024): 93-102.

Style – **GOST** *Name Sort:*

Feltovic Milan From Theory to Practice: The Role of Cryptography in Securing Blockchain Networks [Journal] // MEST Journal / ed. Čekerevac Zoran. - Belgrade – Toronto : MESTE, 07 15, 2024. - 2 : Vol. 12. - pp. 93-102.

Style – **Harvard** *Anglia:*

Feltovic, M., 2024. From Theory to Practice: The Role of Cryptography in Securing Blockchain Networks. *MEST Journal,* 15 07, 12(2), pp. 93-102.

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

From Theory to Practice: The Role of Cryptography in Securing Blockchain Networks. **Feltovic, Milan.** [ed.] Zoran Čekerevac. 2, Belgrade – Toronto : MESTE, 07 15, 2024, MEST Journal, Vol. 12, pp. 93-102.