Analysis of Blockchain-Based Cryptographic Techniques: Strengths, Limitations, and Potential Solutions

Shrey Patel, Raj Patel, and Om Patel

Nirma University, Computer Science department ,
Ahmedabad, India

Abstract. Blockchain technology has emerged as a promising solution for secure and transparent transactions between parties without the need for intermediaries. One of the key features of blockchain technology is its use of cryptographic techniques to ensure the integrity, confidentiality, and authenticity of transactions. However, the effectiveness of these techniques in securing the blockchain system is not fully understood. This research paper aims to provide a comprehensive analysis of blockchain-based cryptographic techniques, including their strengths, limitations, and potential solutions.

The paper begins by providing an overview of the cryptographic techniques used in blockchain technology, including hash functions, digital signatures, public-key cryptography, and symmetric-key cryptography. It then examines the strengths and weaknesses of these techniques and their impact on the overall security of the blockchain system. For example, while hash functions are used to create a unique digital fingerprint of data, they can also be vulnerable to collision attacks, which can compromise the integrity of the data. Similarly, while public-key cryptography provides secure communication between parties without the need for a shared secret, it can be vulnerable to attacks such as man-in-the-middle attacks or key compromise.

The paper also explores the potential trade-offs between security and performance in blockchain-based cryptographic techniques. For example, while cryptographic techniques such as zero-knowledge proofs and ring signatures can enhance data privacy in blockchain systems, they can also add complexity and computational overhead, which can affect the performance of the system.

Furthermore, the paper examines potential solutions to address the limitations of existing techniques. For example, researchers are exploring the use of post-quantum cryptography to address the security challenges posed by quantum computers, which can compromise existing cryptographic techniques.

The paper concludes by providing recommendations for future research on blockchain-based cryptographic techniques, including the development of new techniques that balance security and performance and the exploration of innovative solutions to address the security challenges posed by emerging technologies.

Keywords: blockchain, cryptographic techniques, security, privacy, post-quantum cryptography.

1 Introduction

Decentralized and distributed ledger technology, commonly known as blockchain, enables secure and transparent transactions without the need for a trusted intermediary. It has garnered significant interest in the last few years for its potential to revolutionize various industries, such as finance, healthcare, and supply chain management. The security of blockchain technology depends heavily on the cryptographic methods employed to safeguard the integrity, confidentiality, and availability of data.

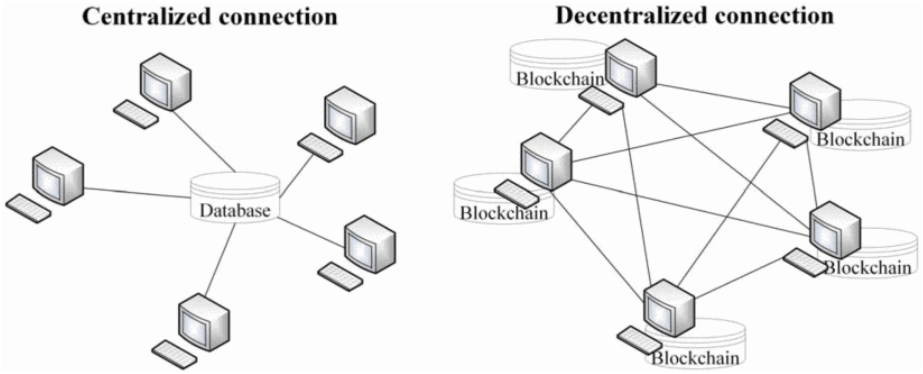

Fig. 1. Difference Between Centralised and Decentralised Connections

This paper analyzes the various blockchain-based cryptographic techniques and their strengths, limitations, and potential solutions. The paper first discusses the different cryptographic techniques used in blockchain, including hashing, digital signatures, encryption, and consensus mechanisms. The trade-offs between security and performance in blockchain-based cryptographic techniques are also examined. Potential solutions, such as post-quantum cryptography and homomorphic encryption, are explored. The paper concludes with the importance of continued research and development of new cryptographic techniques that balance security and performance.

2 Literature Review

In [11] The article provides a comprehensive survey of the various techniques and research directions related to blockchain security. The authors begin by

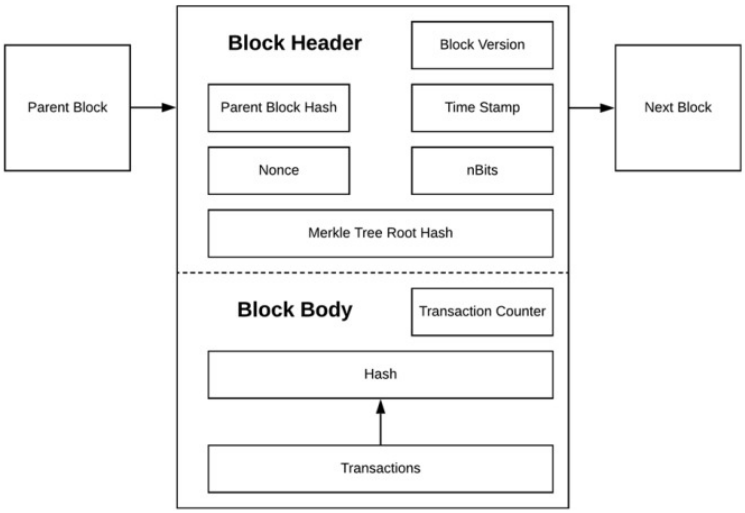

Fig. 2. Internals of a Block on Blockchain[10]

discussing the key features of blockchain technology and the challenges that need to be addressed in order to ensure its security. They then provide a detailed overview of the various security threats that blockchain networks are susceptible to, such as attacks on consensus mechanisms, double-spending attacks, and smart contract vulnerabilities.

The article also covers the various techniques that have been proposed to mitigate these security threats, including consensus algorithms, cryptographic techniques, and access control mechanisms. The authors also discuss the importance of incorporating these techniques into the design of blockchain systems from the outset, rather than attempting to retrofit them after the fact.

Finally, the article concludes with a discussion of the various research directions that are currently being pursued in the field of blockchain security. These include the development of new consensus algorithms, the use of artificial intelligence and machine learning techniques to enhance blockchain security, and the exploration of novel cryptographic approaches.

Overall, this article provides a valuable resource for anyone interested in the security of blockchain systems and the ongoing efforts to address the various security threats that they face.

In [7] The article proposes a hybrid blockchain-edge architecture for the management of electronic health records (EHRs) that leverages attribute-based cryptographic mechanisms to enhance the security and privacy of EHR data. The proposed architecture consists of two layers: an edge layer and a blockchain layer.

The edge layer is responsible for managing the EHR data and enforcing access control policies. The authors propose the use of attribute-based encryption (ABE) and attribute-based access control (ABAC) mechanisms to ensure that only authorized parties are able to access the EHR data. The edge layer also includes a secure enclave that provides a trusted execution environment for sensitive operations.

The blockchain layer is used to store the metadata associated with the EHR data, such as access logs and audit trails. The authors propose the use of a permissioned blockchain to ensure that only authorized parties are able to participate in the network.

The proposed architecture is evaluated through a prototype implementation and a series of experiments. The results demonstrate that the architecture is able to provide efficient and secure management of EHR data, while also ensuring the privacy of patient information.

Overall, this article provides a valuable contribution to the field of healthcare informatics by proposing a novel architecture for the management of EHR data that leverages blockchain and edge computing technologies, as well as attribute-based cryptographic mechanisms.

In [2] The article investigates the security challenges faced by smart homes and proposes the use of blockchain technology as a potential solution. The authors begin by discussing the various security threats that smart homes are susceptible to, such as unauthorized access, data theft, and privacy violations. They also discuss the limitations of existing security mechanisms in addressing these threats.

The authors then propose the use of blockchain technology as a potential solution to these security challenges. They argue that the decentralized and immutable nature of blockchain can enhance the security and privacy of smart home systems. The authors also propose the use of smart contracts to automate security policies and ensure their enforcement.

The article also includes a case study that demonstrates the potential benefits of using blockchain technology for smart home security. The authors implement a blockchain-based system for smart home access control and evaluate its performance through a series of experiments. The results show that the proposed system is able to provide efficient and secure access control while also ensuring the privacy of user data.

Overall, this article provides a valuable contribution to the field of smart home security by investigating the potential use of blockchain technology as a solution to the security challenges faced by smart homes. The case study presented in the article demonstrates the feasibility and potential benefits of using blockchain for smart home security.

In [18] The article proposes a novel blockchain-based privacy-preserving framework for online social networks (OSNs). The authors begin by discussing the privacy challenges faced by OSNs, such as data breaches and unauthorized access to user data. They argue that traditional security mechanisms, such as encryption

and access control, are not sufficient to address these challenges and propose the use of blockchain technology as a potential solution.

The proposed framework consists of three main components: a user profile management system, a content management system, and a consensus mechanism. The user profile management system is responsible for managing user identities and access control policies, while the content management system is responsible for managing user-generated content. The consensus mechanism ensures that all nodes in the network agree on the state of the system.

The authors also propose the use of zero-knowledge proofs (ZKPs) to enhance the privacy of user data. ZKPs allow users to prove that they have certain information without revealing the information itself. The authors argue that ZKPs can be used to verify user identities and access control policies without revealing sensitive information.

The proposed framework is evaluated through a prototype implementation and a series of experiments. The results demonstrate that the framework is able to provide efficient and secure management of user data while also ensuring the privacy of user information.

Overall, this article provides a valuable contribution to the field of online social network security by proposing a novel blockchain-based framework that leverages ZKPs to enhance the privacy of user data. The experimental results demonstrate the feasibility and potential benefits of using blockchain technology for OSN security.

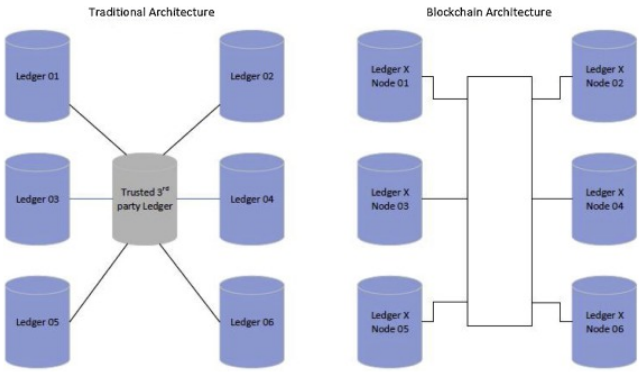

Fig. 3. Traditional Architecture v/s Blockchain Architecture[8]

3 Blockchain-Based Cryptographic Techniques

Blockchain-based cryptographic techniques are innovative methods that rely on cryptography and distributed ledger technology to ensure secure, transparent, and tamper-proof transactions. These techniques utilize complex mathematical algorithms to encrypt data, ensuring that it can only be accessed by authorized users with the correct private key. With blockchain-based cryptographic techniques, data can be securely shared across a network of nodes, creating a decentralized and immutable record of all transactions. The growing adoption of this technology across diverse industries, such as finance, healthcare, and supply chain management, highlights its potential to provide a higher level of security and transparency in transactions. Its ability to ensure the integrity of data and provide an immutable record of transactions has made it an attractive option for organizations seeking to enhance their operations and provide greater trust and confidence to their stakeholders. As such, the use of this technology is expected to continue to expand and evolve as organizations seek to harness its benefits and unlock new possibilities.

Following is the List of some of the Commonly used Cryptographic techniques used in blockchain-based systems:

- Hash functions
- Public-key cryptography (asymmetric cryptography)
- Elliptic Curve Cryptography (ECC)
- Digital signatures
- Consensus algorithms (e.g., Proof of Work, Proof of Stake)
- Merkle Trees
- Zero-knowledge proofs
- Ring signatures
- Homomorphic encryption
- Threshold signatures
- Multi-party computation
- Schnorr signatures

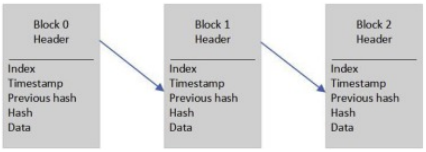

Fig. 4. Block Hash Verification

4 Techniques

4.1 Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a type of public-key cryptography that is based on the mathematics of elliptic curves. In ECC, encryption and decryption are performed using a pair of keys, consisting of a private key and a public key. The public key is used to encrypt data, and the private key is used to decrypt it. ECC is a highly secure form of cryptography, offering a level of security that is equivalent to RSA encryption, but with much shorter key lengths. This makes it ideal for use in applications where there are limitations on computing resources, such as mobile devices or embedded systems. ECC is also highly resistant to attacks based on quantum computing, which makes it an attractive option for organizations seeking to future-proof their security infrastructure[1]. ECCs employ smaller keys to give great security while remaining fast.

ECC is used in a wide range of applications, including secure communications, digital signatures, and secure data storage. It is also used in many blockchain networks to provide a high level of security and integrity to transactions. Overall, ECC is a highly secure and efficient form of cryptography that is increasingly being adopted by organizations worldwide.

Elliptic Curve Cryptography (ECC) is a modern cryptographic system that was independently proposed by Neals Koblitz [9] and Victor Miller[13] in the late 1980s. Since its inception, ECC has gained widespread commercial recognition and has been endorsed by several standardization bodies such as ANSI, IEEE, ISO, and NIST. This cryptographic system has garnered much attention and popularity due to its ability to provide the same level of security as traditional public-key cryptographic systems but with much shorter key sizes. The equation defines an elliptic curve.

$$y^2 + xy = x^3 + ax + b \tag{1}$$

A fundamental feature of elliptic curves is their ability to facilitate the creation of a process for adding two points on the curve to produce a third point on the curve, which conforms to the standard addition characteristics. By applying this addition rule, a finite Abelian group is formed by the points on the curve, including a zero point (designated as 0), which does not satisfy the elliptic curve equation. This additional point is essential for ensuring that the addition operation is well-defined for any pair of points.

It should be noted that the value 0 is assumed to represent a point on the curve, and the number of unique points on the curve, including the zero point, determines the curve's order. This concept of the curve's order is an important characteristic, as it influences the overall security and effectiveness of the elliptic curve cryptography scheme.

The key advantage of Elliptic Curve Cryptography (ECC) over RSA lies in its core operation, which involves point addition. This operation is known to be computationally expensive, thereby enhancing the overall security of ECC. As a result, the likelihood of developing a comprehensive sub-exponential attack on

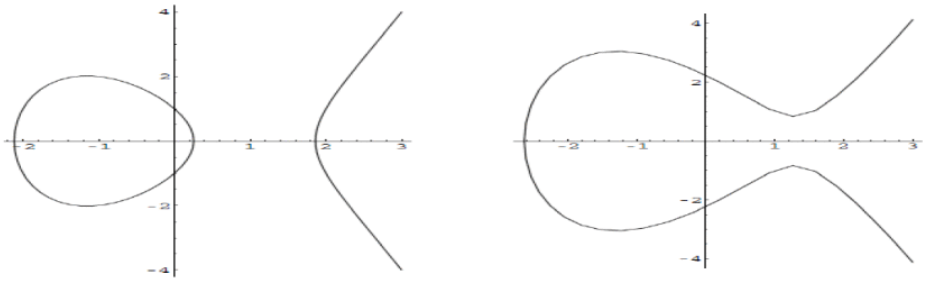

Fig. 5. ECC[1]

ECC in the near future is low, despite the existence of some attacks on specific types of curves. These types of curves can be readily identified and avoided to mitigate the risk of attacks.

As a result, in order to retain the same level of security, the number of bits required in the RSA-produced key pair will climb more quickly than in the ECC-generated key pair, as shown in Table 1. In order to provide sufficient security, a 1024-bit modulus must be employed in an RSA system, whereas a 160-bit modulus is enough for ECC.

ECC Key Size (bits)	RSA Key Size (bits)	Key Size ratio
160 bit	1024 bit	1:6
224 bit	2048 bit	1:9
256 bit	3072 bit	1:12
512 bit	15360 bit	1:30

4.2 Hashing

Hashing is a technique utilized to maintain the integrity of a message or file without the need for any type of key. The hash function is publicly available and generates a fixed-length output string when processing a message or file. The Secure Hash Algorithm-256 (SHA-256) is a widely used hashing technique that produces a 256-bit binary string when applied to a file. It has the property of producing significantly different hashes for very similar files in an unpredictable manner. This feature of SHA-256 is due to the fact that the hashes of distinct files are evenly and randomly distributed among the set of all possible 256 binary strings, which consists of approximately 10^{77} elements.

Each file has a unique hash or "fingerprint," and the same input always produces the same output. However, there is a possibility that two different files

could have the same hash, which is called a "collision." Nonetheless, collisions are highly improbable in practice. It is also important to note that hash functions are not reversible, meaning that a file cannot be retrieved from its hash.

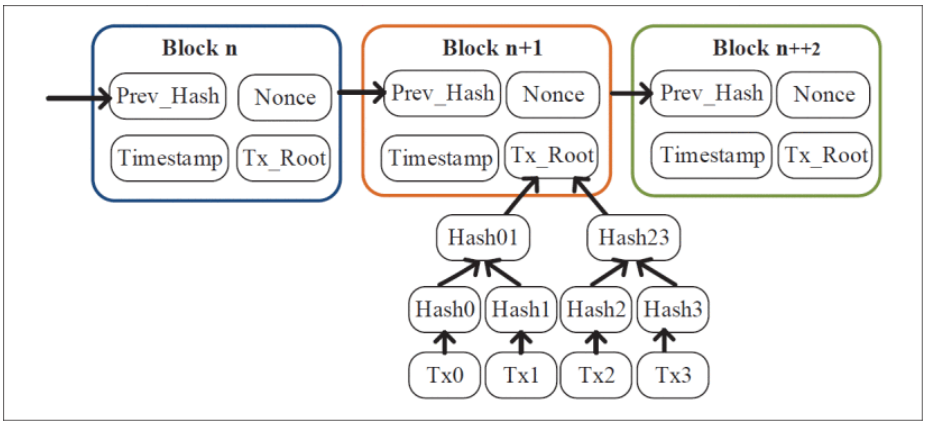

Fig. 6. Block Hashing[17]

Hash Function Applications

- **Document Checking**: Assume you sign a partnership agreement and subsequently have a disagreement. You and the other person both bring proof of the agreement to the judge, but your statements disagree. How will the judge know which is genuine? Assume the judge had access to a hash of the contract on the day it was signed. He may then compare it to hashes of the contracts you and your partner supplied to him. The real contract will generate the same hash, but any manipulated contract will generate something different.
- **Login Verification**: When a user attempts to log into a system, the system verifies the password provided by the user to the password stored in its files. The difficulty with this is that hackers might steal the passwords saved by the system. As a result, storing just hashes of user credentials is a solid security practice. Users continue to enter passwords, but the system generates a hash and compares it to the hashed password saved in its files. The hashed password will correspond to a previously saved hash if the password is accurate. It is useless if the hashed password file is taken from the machine. The hash does not reveal the password, and the system requires a proper plaintext password to enable access, not the hash.

4.3 Digital Signature

Digital signatures are an indispensable component of contemporary cryptography, serving to establish the authenticity, integrity, and non-repudiation of

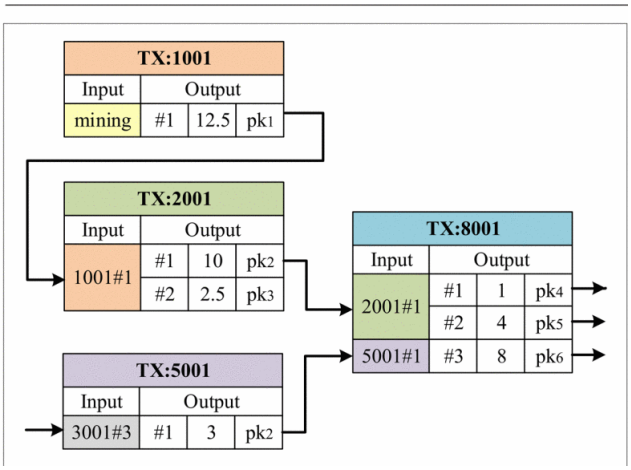

Fig. 7. Hash Minning

electronic documents and transactions. In the context of blockchain technology, digital signatures constitute a critical mechanism that enables users to authenticate the ownership and transfer of digital assets without relying on a trusted third-party intermediary.[14]

Blockchain represents a distributed ledger technology that relies heavily on cryptographic techniques to ensure the security and immutability of data stored on the network. In this context, digital signatures play a vital role in realizing these objectives by furnishing users with a means to prove ownership of their digital assets and authorize transactions in a decentralized fashion, with no reliance on centralized authorities.

To expand on the technical aspects of digital signatures, they are generated using asymmetric cryptography algorithms, which involve the use of a public and a private key. The private key is kept secret by the signer and is used to create the digital signature, while the public key is available to anyone who wishes to verify the authenticity of the signature.[5]

When a user creates a digital signature, the hash of the message or transaction is first generated, and then encrypted using the signer's private key. The resulting signature can then be verified using the signer's public key, which decrypts the signature and compares it to the original message hash. If the two values match, the signature is considered valid.

In a blockchain network, every node can independently verify the digital signature of a transaction, ensuring that the transaction has been signed by the correct user and has not been tampered with during transmission. This provides a high level of security and trust in the network, without the need for a centralized authority to oversee transactions.

Furthermore, recent advancements in post-quantum cryptography have led to the development of digital signature schemes that are resistant to attacks

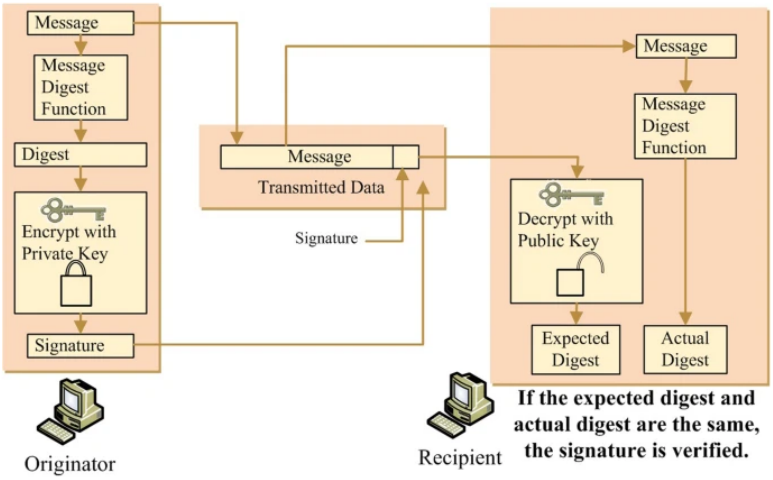

Fig. 8. Digital Signature

from quantum computers. This is an important consideration for the long-term security of blockchain networks as quantum computers become more powerful and capable of breaking traditional cryptographic algorithms.

Digital signatures are a critical component of blockchain technology, providing authentication, non-repudiation, and tamper evidence for transactions and digital assets. Ongoing research and development in digital signature schemes are necessary to improve their efficiency, security, and resilience to emerging threats.

Another paper [4] in which Bralic et al. discuss how blockchain technology can be used for digital archiving by ensuring the preservation of digital signature certification chains. The authors highlight the challenges of preserving digital archives, such as the risk of data loss, and explain how blockchain technology can help to mitigate these risks.

One potential solution for preserving digital signature certification chains is to utilize blockchain technology. This involves creating a digital signature certification chain that is stored on the blockchain network, providing a secure and tamper-proof record of all digital signatures and their associated certificates.

This blockchain-based approach ensures that all digital signatures and certificates are stored in a decentralized and distributed manner, preventing any single point of failure or potential tampering. Additionally, the immutability of the blockchain ensures that the integrity of the certification chain is maintained, with any attempts at modifying or altering the chain being immediately detected and rejected by the network.

By using blockchain technology [6] for digital signature certification chains, users can have increased confidence in the authenticity and integrity of their digital signatures, as well as the associated certificates. This can be particularly

beneficial in industries where compliance and regulatory requirements are strict, such as finance, healthcare, and legal industries.

4.4 Consensus in Blockchain Networks

In distributed systems, the challenge of keeping the blockchain state consistent across the peer-to-peer network can be viewed as a problem of fault-tolerant state-machine replication. Each node in the consensus maintains a local copy, or view, of the blockchain[16]. Despite treacherous or arbitrary failures, consensus nodes are expected to agree upon a single, unified view of the blockchain. In blockchain networks, treacherous failures can result in faulty nodes exhibiting a range of arbitrary behaviours, including malicious attacks or collusion (such as Sybil attacks and double-spending attacks), node errors (such as unexpected blockchain forks caused by software inconsistencies), and connection errors[15].

The sequence of blocks can be seen as the representation of the blockchain state, where the confirmation of a transaction triggers a transition in the blockchain state. As per the consensus algorithm in a treacherous environment, a blockchain updating protocol must ensure certain key properties are met. These include Validity, Agreement, Liveness, and Total order. The validity, also known as Correctness, means that if all honest nodes agree to expand the blockchain with the same block, any honest node that moves to a new local replica state must adopt the blockchain headed by that block. Consistency, also known as Agreement, is a critical property that ensures that if a valid block header is confirmed by an honest node, then any other honest node updating its local view of the blockchain must also update with that block header. Termination, or Liveness, guarantees that all transactions initiated by honest nodes will eventually be confirmed. Furthermore, Total Order demands that all honest nodes agree on the same order of transactions, as long as they are confirmed in their local blockchain views. These properties guarantee that the blockchain state remains consistent and secure, even in the face of failures caused by malicious attacks or arbitrary behaviours.

Permissionless blockchain networks lack explicit synchronization schemes or identity authentication, in contrast to permissioned networks. Therefore, the consensus protocol in these networks must be highly scalable and tolerant to pseudo identities and poor synchronization. In permissionless networks, any node can propose a state transition with its own candidate block for the blockchain header. Therefore, the primary objective of the consensus protocol in these networks is to ensure that every consensus node follows the "longest chain rule," where only the longest chain can be accepted as the canonical state of the blockchain when the blocks are organized in a linked list.

Since identity authentication is absent in permissionless networks, direct voting-based BFT protocols are unsuitable for these networks. Instead, incentive-based consensus schemes like the Nakamoto consensus protocol have gained widespread adoption. Such schemes reward nodes for performing specific tasks that promote the overall security and stability of the blockchain network, ensuring that the network remains decentralized, secure, and reliable.

4.5 Merkle Trees

Merkle Trees are a cryptographic data structure that provides an efficient method for verifying the integrity of large datasets. First introduced by Ralph Merkle in 1979 to secure data in a public key infrastructure, Merkle Trees have become a fundamental building block in various cryptographic applications.

A Merkle Tree is a binary tree where each leaf node represents a block of data, and each non-leaf node represents the hash of the concatenation of its child nodes. The root node of the tree represents the hash of the entire dataset[3]. The main advantage of Merkle Trees is their ability to efficiently verify large datasets. Instead of verifying the entire dataset, a party can simply verify the path from a leaf node to the root node, requiring only a logarithmic number of hash computations. This makes Merkle Trees particularly useful in applications such as blockchain and distributed systems.

Researchers have extensively studied Merkle Trees, focusing on their security properties, efficiency, and variations to address specific requirements. For instance, they have analyzed Merkle Trees' resistance to various attacks, including collision and preimage attacks, and proposed techniques to enhance their security. They have also examined Merkle Trees' performance on different platforms and developed optimizations to reduce their computational and storage requirements. Furthermore, researchers have proposed variations of Merkle Trees that cater to specific needs in various applications, such as using different hashing algorithms or allowing for more efficient updates to the dataset.

Overall, Merkle Trees provide a crucial tool for ensuring data integrity in cryptography. Their efficient verification properties make them a valuable data structure in many applications, and ongoing research continues to improve their security and efficiency in different settings.

4.6 Ring Signature

Ring signatures are a type of digital signature that allows a group of users to sign a message anonymously. In a ring signature scheme, a signer creates a signature by selecting a group of other users, called the ring, from a larger set of users. The signature is verified by anyone who knows the public keys of the users in the ring, but it is impossible to determine which user in the ring actually created the signature.

Ring signatures were first introduced by Rivest, Shamir, and Tauman in 2001 and have since been the subject of extensive research in cryptography. One of the main advantages of ring signatures is that they provide strong privacy guarantees, allowing signers to remain anonymous even if their public key is known. This makes them useful in various applications, such as anonymous voting, whistleblowing, and secure communication.[12]

In recent years, there has been significant research on improving the security and efficiency of ring signature schemes. For example, researchers have proposed new constructions of ring signatures based on various cryptographic assumptions, such as bilinear pairings, hash functions, and elliptic curves. These constructions

provide different trade-offs between security, efficiency, and anonymity. Furthermore, researchers have studied the security properties of ring signatures and have proposed attacks against various schemes. They have also studied the anonymity properties of ring signatures and have proposed metrics for measuring the level of anonymity provided by different schemes. Another area of research in ring signatures is the development of practical applications. For example, researchers have proposed using ring signatures for secure messaging and file sharing, as well as for anonymous authentication in decentralized systems such as blockchain networks.

Overall, research in ring signatures has led to the development of new and improved schemes, better understanding of their security and anonymity properties, and practical applications in various domains.

5 Conclusion

In conclusion, blockchain technology has enabled the development of secure and transparent systems through the use of cryptographic techniques. The techniques discussed in this analysis, including hash functions, public-key cryptography, elliptic curve cryptography, digital signatures, consensus algorithms, Merkle trees, zero-knowledge proofs, ring signatures, homomorphic encryption, threshold signatures, multi-party computation, and Schnorr signatures, provide a strong foundation for the security and integrity of blockchain-based systems.

As blockchain technology continues to evolve and be implemented in various industries, it is essential to understand the role that cryptographic techniques play in ensuring the safety and trustworthiness of these systems. The techniques discussed in this analysis are just a few examples of the many cryptographic tools available to blockchain developers and users, and there is still much to be explored and discovered in this exciting field. Overall, the use of blockchain-based cryptographic techniques has the potential to revolutionize the way we store and exchange information, providing greater security and transparency for individuals and organizations alike.

References

[1] Moncef Amara and Amar Siad. "Elliptic Curve Cryptography and its applications". In: *International Workshop on Systems, Signal Processing and their Applications, WOSSPA*. 2011, pp. 247–250. DOI: 10.1109/WOSSPA.2011.5931464.

[2] Samrah Arif et al. "Investigating smart home security: Is blockchain the answer?" In: *IEEE Access* 8 (2020), pp. 117802–117816.

[3] Georg Becker. "Merkle signature schemes, merkle trees and their cryptanalysis". In: *Ruhr-University Bochum, Tech. Rep* 12 (2008), p. 19.

[4] Vladimir Bralić, Hrvoje Stančić, and Mats Stengård. "A blockchain approach to digital archiving: digital signature certification chain preservation". In: *Records Management Journal* 30.3 (2020), pp. 345–362.

[5] Fangfang Dai et al. "From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues". In: *2017 4th International Conference on Systems and Informatics (ICSAI)*. 2017, pp. 975–979. DOI: 10.1109/ICSAI.2017.8248427.

[6] Weidong Fang et al. "Digital signature scheme for information non-repudiation in blockchain: a state of the art review". In: *EURASIP Journal on Wireless Communications and Networking* 2020.1 (2020), pp. 1–15.

[7] Hao Guo et al. "A Hybrid Blockchain-Edge Architecture for Electronic Health Record Management with Attribute-based Cryptographic Mechanisms". In: *IEEE Transactions on Network and Service Management* (2022).

[8] Laurie Hughes et al. "Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda". In: *International Journal of Information Management* 49 (2019), pp. 114–129. ISSN: 0268-4012. DOI: https://doi.org/10.1016/j.ijinfomgt.2019.02.005. URL: https://www.sciencedirect.com/science/article/pii/S0268401219302014.

[9] Neal Koblitz. "Elliptic curve cryptosystems". In: *Mathematics of computation* 48.177 (1987), pp. 203–209.

[10] R. Lakshmana Kumar et al. "Blockchain for securing aerial communications: Potentials, solutions, and research directions". In: *Physical Communication* 47 (2021), p. 101390. ISSN: 1874-4907. DOI: https://doi.org/10.1016/j.phycom.2021.101390. URL: https://www.sciencedirect.com/science/article/pii/S1874490721001270.

[11] Jiewu Leng et al. "Blockchain security: A survey of techniques and research directions". In: *IEEE Transactions on Services Computing* 15.4 (2020), pp. 2490–2510.

[12] Xiaofang Li et al. "A blockchain privacy protection scheme based on ring signature". In: *IEEE Access* 8 (2020), pp. 76765–76772.

[13] Victor S Miller. *Use of elliptic curves in cryptography*. Springer, 1986.

[14] Ahmed Afif Monrat, Olov Schelén, and Karl Andersson. "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities". In: *IEEE Access* 7 (2019), pp. 117134–117151. DOI: 10.1109/ACCESS.2019.2936094.

[15] Wenbo Wang et al. "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks". In: *IEEE Access* 7 (2019), pp. 22328–22370. DOI: 10.1109/ACCESS.2019.2896108.

[16] Wenbo Wang et al. "A survey on consensus mechanisms and mining strategy management in blockchain networks". In: *Ieee Access* 7 (2019), pp. 22328–22370.

[17] Yong Yu et al. "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things". In: *IEEE Wireless Communications* 25.6 (2018), pp. 12–18. DOI: 10.1109/MWC.2017.1800116.

[18] Shiwen Zhang et al. “A novel blockchain-based privacy-preserving framework for online social networks”. In: *Connection Science* 33.3 (2021), pp. 555–575.