Review

The Role of Cryptography in Blockchain: Ensuring Immutability, Transparency and Security

Janaka Ishan Senarathna *

Posted Date: 22 April 2025

doi: 10.20944/preprints202504.1814.v1

Keywords: blockchain; cryptography; hashing algorithms; asymmetric cryptography; digital signatures; distributed ledger technology; security; privacy

Review

The Role of Cryptography in Blockchain: Ensuring Immutability, Transparency and Security

Janaka Ishan Senarathna

Department of Computer and Data Science, NSBM Green University, Mahenwatta, Pitipana, Homagama, Sri Lanka; janakaishansenarathna0169@gmail.com or djisenarathna@students.nsbm.ac.lk

Abstract: This review paper explores the fundamental relationship between blockchain technology and cryptography, highlighting how cryptographic methods are essential for the security, integrity, and functionality of blockchain systems [2]. Blockchain, a decentralized and distributed ledger technology, relies on cryptography to ensure tamper-proof records of transactions. This paper delves into the core cryptographic pillars of blockchain, including hashing algorithms, asymmetric cryptography (public and private keys), and digital signatures, explaining their roles in maintaining the blockchain's immutability, transparency, and security against double-spending and data manipulation. The paper also discusses real- world applications of blockchain in supply chain management and healthcare, illustrating the practical significance of its cryptographic underpinnings [3]. Furthermore, it critically analyzes the strengths and limitations of relying on cryptography in blockchain, including challenges such as key management and the potential threat of quantum computing.

Keywords: blockchain; cryptography; hashing algorithms; asymmetric cryptography; digital signatures; distributed ledger technology; security; privacy

1. Introduction

Blockchain technology has emerged as a groundbreaking innovation in the realm of distributed ledger systems, capturing widespread attention across diverse industries. Its promise of heightened security, enhanced transparency, and improved efficiency in digital transactions has positioned it as a transformative force [1]. At its core, a blockchain operates as a continuously expanding chain of data blocks, with each block containing a collection of transactions that are bundled together and cryptographically linked to the preceding block [5]. This chronological and linear structure ensures a tamper- evident and immutable record of all transactions within the network [1]. A defining characteristic of blockchain technology is its decentralized architecture, which fundamentally shifts away from traditional centralized authorities by distributing the ledger across a network of computers. This decentralization enables peer-to-peer transactions and interactions without the need for intermediaries such as banks or clearinghouses [6].

The security, integrity, and overall functionality of blockchain technology are inextricably linked to the application of robust cryptographic methods [7]. Cryptography provides the essential toolkit for securing data within the blockchain, ensuring the authenticity of transactions, and maintaining the integrity of the distributed ledger [8]. Without these cryptographic underpinnings, blockchain systems would be inherently vulnerable to a myriad of security threats, including the risk of double-spending digital assets and the potential for malicious data manipulation [9]. This review paper aims to conduct a [10]. comprehensive analysis of blockchain technology, with a particular focus on its profound reliance on various cryptographic methods [11]. It will delve into the fundamental principles of both blockchain and cryptography, exploring their intricate interplay and the synergistic relationship that underpins the technology's core features [12]. Furthermore, this paper will examine the diverse applications of blockchain across different sectors, highlighting the critical role of

 doi:10.20944/preprints202504.1814.v1

cryptography in enabling these use cases. A critical analysis of the strengths and limitations of the technology, particularly in relation to its cryptographic foundations, will also be presented, alongside a discussion of potential future directions and advancements in this rapidly evolving field. To provide a practical understanding of the concepts discussed, real-world examples and a mini implementation of a basic blockchain system will be included.

The initial research suggests a strong consensus within the academic literature regarding the fundamental and indispensable role of cryptography in blockchain technology. Multiple sources, ranging from introductory overviews to more technical analyses, consistently highlight the decentralized nature and cryptographic security as defining characteristics of blockchain. This repeated emphasis underscores the foundational principle that cryptography is not merely an add-on but rather an integral component that enables the very essence of blockchain. Moreover, the identification of double-spending and data manipulation as specific vulnerabilities that cryptographic techniques effectively mitigate further illustrates the direct security benefits derived from these methods within the context of blockchain's decentralized framework. Decentralization, while offering numerous advantages, inherently introduces challenges related to ensuring the trustworthiness and immutability of records without a central controlling entity. Cryptography provides the necessary tools, such as hashing and digital signatures, to address these specific threats and establish a secure and reliable distributed ledger system.

2. The Cryptographic Pillars of Blockchain Technology

Blockchain technology's robust framework is built upon several core cryptographic concepts that work in concert to ensure its security, integrity, and functionality. These fundamental cryptographic pillars include hashing algorithms, asymmetric cryptography (involving public and private keys), digital signatures, and, to a lesser extent, symmetric cryptography.

2.1. Hashing Algorithms

At the heart of blockchain's architecture lies the concept of cryptographic hash functions. These algorithms take an input of arbitrary size and produce a fixed-size output, commonly referred to as a hash or message digest. This output acts as a unique digital fingerprint of the input data [1]. Several key properties of cryptographic hash functions are particularly relevant to their application in blockchain:

- **Preimage resistance:** Given a hash value, it should be computationally infeasible to find the original input that produced that hash [4]. This property ensures that one cannot easily reverse the hashing process to obtain the original data.
- **Second preimage resistance:** For a given input, it should be computationally infeasible to find a different input that produces the same hash value [4]. This prevents malicious actors from substituting one piece of data for another while maintaining the same hash.
- **Collision resistance:** It should be computationally infeasible to find two distinct inputs that produce the same hash value [3]. While theoretically collisions might exist due to the fixed-size output for a variable-size input, a strong cryptographic hash function makes finding such collisions computationally prohibitive.

Several widely used hashing algorithms have found application in blockchain technology. SHA-256 (Secure Hash Algorithm 256-bit) is prominently used in Bitcoin [1]. Ethereum, on the other hand, employs a modified version of SHA-3 known as Keccak-256 [6]. BLAKE3 is a more recent hashing algorithm that has garnered attention for its potential speed and security advantages [6].

Hashing plays a crucial role in linking blocks together within a blockchain. Each block's header, with the exception of the very first block (the genesis block),

contains a cryptographic hash of the previous block's header [1]. This inclusion of the previous block's hash creates a chain of blocks, where each block is inextricably linked to its predecessor. Any

 doi:10.20944/preprints202504.1814.v1

alteration to the data in a previous block would result in a different hash for that block, thereby breaking the chain and making the tampering easily detectable [1].

Furthermore, hashing is also employed in the construction of Merkle trees, which are often used in blockchain to efficiently summarize and verify the integrity of a large number of transactions within a single block [4]. A Merkle tree is a tree-like data structure where each leaf node represents the hash of a transaction, and each non-leaf node represents the hash of its child nodes. The root of the tree, known as the Merkle root, provides a single cryptographic hash that represents all the transactions in the block. This allows for efficient verification of whether a specific transaction is included in a block without needing to download the entire block [4].

2.2. Asymmetric Cryptography (Public and Private Keys)

Asymmetric cryptography, also known as public-key cryptography, is another cornerstone of blockchain security. This cryptographic approach utilizes a pair of mathematically related keys for each participant: a public key and a private key [2]. The public key is designed to be shared openly and can be used for encryption and verifying digital signatures. Conversely, the private key is kept secret by its owner and is used for decryption and creating digital signatures [2]. While the public and private keys are mathematically linked, it is computationally infeasible to derive the private key from the public key [4].

In the context of blockchain, public keys often serve as user identifiers or addresses for receiving digital assets. When someone wants to send cryptocurrency to another user, they typically use the recipient's public key as the destination address. The corresponding private key is then used by the recipient to authorize transactions, such as spending the received cryptocurrency [1].

RSA (Rivest-Shamir-Adleman) and Elliptic Curve Cryptography (ECC) are common asymmetric cryptography algorithms employed in blockchain technology [3]. ECC is particularly popular for digital signatures in cryptocurrencies like Bitcoin and Ethereum due to its strong security profile and relatively short key lengths.

2.3. Digital Signatures

Digital signatures are a critical application of asymmetric cryptography in blockchain, providing a mechanism for authentication and non-repudiation of transactions [1]. When a user initiates a transaction on a blockchain network, they typically use their private key to create a digital signature for that transaction. This signature is essentially a cryptographic hash of the transaction data that has been encrypted using the sender's private key [1].

Anyone with access to the sender's corresponding public key can then verify the digital signature [1]. The verification process involves decrypting the digital signature using the public key and comparing the resulting hash with a newly computed hash of the original transaction data. If the hashes match, it cryptographically proves that the transaction was indeed signed by the owner of the private key associated with the public key used for verification, and that the transaction data has not been altered since it was signed [1]. This mechanism ensures both the authenticity of the sender and the integrity of the transaction, providing non-repudiation as the sender cannot easily deny having authorized the transaction [4]. Digital signatures play a vital role in securing various blockchain applications, including cryptocurrency transactions, ensuring the integrity of supply chains, enabling secure electronic voting systems, and facilitating the execution of smart contracts [4].

2.4. Symmetric Cryptography

Symmetric cryptography utilizes a single secret key for both the encryption and decryption of data [4]. While asymmetric cryptography is fundamental for authentication and digital signatures in blockchain, symmetric cryptography is generally less commonly used for core blockchain operations like transaction signing due to the challenge of securely distributing the shared secret key among all participants in a permissionless network [4]. However, symmetric encryption can be employed for

 doi:10.20944/preprints202504.1814.v1

specific purposes within blockchain systems, such as encrypting the content of transactions in permissioned blockchain networks [4]. Algorithms like AES (Advanced Encryption Standard) are examples of widely used symmetric ciphers [4].

The interplay of these cryptographic methods forms a robust and secure foundation for blockchain technology. Hashing ensures the integrity and chaining of blocks, asymmetric cryptography provides secure identity management and transaction authorization, and digital signatures guarantee the authenticity and non-repudiation of actions on the blockchain.

Table 1. Summary of Cryptographic Methods in Blockchain.

Cryptographic Method	**Core Concepts**	**Key Algorithms/Techniques**	**Role in Blockchain**
Hashing Algorithms	Fixed-size output (hash) for any input; preimage, second preimage, collision resistance	SHA-256, Keccak-256, BLAKE3	Linking blocks, ensuring data integrity, Merkle trees for efficient transaction verification
Asymmetric Cryptography	Public key (encryption/verification), private key (decryption/signing)	RSA, ECC	User identification, secure communication, generating and verifying digital signatures, controlling access to digital assets
Digital Signatures	Private key signing of data hash; public key verification of authenticity	RSA signatures, ECDSA	Authenticating transactions, ensuring non-repudiation, verifying the integrity of data, securing smart contracts, supply chains, and voting systems
Symmetric Cryptography	Single secret key for encryption and decryption	AES	Encrypting transaction content (especially in permissioned blockchains), secure communication channels within specific network configurations

The research indicates that the efficiency of hash functions is a significant consideration in blockchain technology, particularly concerning the speed of transaction processing and block generation [3]. This highlights an ongoing trade-off between the need for strong security, as provided

 doi:10.20944/preprints202504.1814.v1

by collision-resistant hash functions, and the demand for high performance in blockchain systems. Researchers are actively exploring new and optimized hashing algorithms to strike a better balance between these competing requirements [3]. Furthermore, the use of Merkle trees within blockchain demonstrates a multi-layered approach to security. Data integrity is not only ensured at the chain level through the linking of block hashes but also within individual blocks through the cryptographic summarization provided by Merkle trees [4]. The variety of asymmetric algorithms employed in blockchain, each with its own strengths and weaknesses, suggests that the selection of a specific cryptographic algorithm is often tailored to the particular security needs and performance characteristics of the blockchain application [1]. For example, ECC is favored for digital signatures in many cryptocurrencies due to its strong security profile and relatively short key lengths, which contribute to efficiency [1].

3. Strengths and Limitations of Cryptography in Blockchain

The integration of cryptographic methods into blockchain technology bestows a multitude of significant advantages, contributing to its reputation as a secure and trustworthy system. However, it is equally important to acknowledge the inherent limitations and potential vulnerabilities associated with this reliance on cryptography.

3.1. Strengths of Cryptography in Blockchain

One of the most prominent strengths of cryptography in blockchain is the immutability it provides [4]. Through the use of cryptographic hashing and the chaining mechanism, once a transaction is recorded on the blockchain and becomes part of a block, it is exceptionally difficult to alter or tamper with it [4]. Changing the data in a past block would necessitate recalculating its hash, which would then invalidate the hash of the subsequent block, and so on, effectively breaking the chain and making the alteration immediately apparent to all network participants [4].

Cryptography also enables a high degree of transparency within blockchain networks. While user identities are often represented by pseudonymous public keys, all transactions recorded on a public blockchain are typically visible to anyone with access to the network [1]. This transparency fosters trust and allows for public auditing of the ledger, although it's important to note that the link between a public key and a real-world identity might still be possible to establish in some cases.

Cryptography plays a crucial role in ensuring security against double-spending, a significant concern in digital currencies [4]. Digital signatures guarantee that only the legitimate owner of the private key associated with a particular digital asset can authorize a transaction to spend those assets [4]. This prevents malicious actors from fraudulently spending the same digital currency multiple times.

Furthermore, digital signatures provide strong authentication and non-repudiation [4]. By verifying a transaction's digital signature using the sender's public key, recipients can be confident in the identity of the sender [4]. The non-repudiation aspect ensures that once a transaction is signed and added to the blockchain, the sender cannot easily deny having initiated it [4].

Finally, cryptography, particularly through hashing algorithms, ensures data integrity within each block of the blockchain [4]. Any unauthorized modification to the data within a block would result in a different hash value for that block, which would be immediately detectable by other network participants [4].

3.2. Limitations of Cryptography in Blockchain

Despite its numerous strengths, the reliance of blockchain on cryptography also presents certain limitations and potential vulnerabilities. The security of cryptographic methods is inherently tied to the complexity of the underlying mathematical problems. While current cryptographic algorithms are considered robust against classical computing attacks, advancements in computing power could potentially render some of these algorithms vulnerable in the future [4].

 doi:10.20944/preprints202504.1814.v1

While the cryptographic integrity of the blockchain is strong, the system is not entirely immune to attacks. For instance, a 51% attack, where a single entity or group gains control of a majority of the network's hashing power, could theoretically allow the attacker to manipulate the blockchain by reversing transactions or preventing new transactions from being confirmed [1]. However, such attacks are often economically prohibitive and difficult to execute on large, well- established blockchain networks. Additionally, vulnerabilities in smart contracts, which are self- executing contracts written in code and stored on the blockchain, can be exploited if the code contains errors or logic flaws, even if the underlying blockchain and cryptographic mechanisms are sound [1].

A significant limitation lies in the challenges associated with key management [4]. The security of a user's digital assets is entirely dependent on the security of their private key. If a user loses their private key or if it is stolen, they can irreversibly lose access to their funds [4]. Securely generating, storing, and recovering private keys remains a significant challenge for many users, and the complexity of key management can be a barrier to wider adoption.

Perhaps the most significant long-term challenge to blockchain cryptography comes from the emergence of quantum computing. Quantum computers possess the potential to perform certain types of calculations exponentially faster than classical computers, which could have profound implications for the security of currently used asymmetric cryptographic algorithms, including RSA and ECC, which are fundamental to blockchain. Quantum algorithms, such as Shor's algorithm, could theoretically break the security of public-key cryptography, potentially allowing unauthorized access to wallets and transactions and undermining the integrity of digital signatures. While practical, large-scale quantum computers capable of breaking these algorithms are not yet a reality, the threat is considered significant enough that researchers are actively working on developing post-quantum cryptography algorithms that are resistant to both classical and quantum attacks.

While cryptography forms a robust security foundation for blockchain, it is crucial to recognize that it is not the sole determinant of the system's overall security. Other aspects, such as the network's consensus mechanisms and the security of smart contract code, also play vital roles. Furthermore, the responsibility for maintaining the security of digital assets within a blockchain system often rests with the individual user, particularly in terms of secure key management. The potential threat posed by quantum computing necessitates ongoing research and development of quantum-resistant cryptographic methods to ensure the long-term security and viability of blockchain technology in the face of future technological advancements.

4. Real-World Applications and Use Cases

Blockchain technology, underpinned by its robust cryptographic methods, is finding diverse applications across various industries, demonstrating its transformative potential beyond its initial association with cryptocurrencies. Two compelling real-world examples that highlight the integral role of cryptography are in supply chain management and healthcare.

4.1. Supply Chain Management

Supply chain management is a critical area where blockchain technology is being increasingly implemented to enhance transparency, security, and overall efficiency. Traditional supply chains often suffer from a lack of visibility, inefficiencies, and vulnerabilities to fraud and counterfeiting. Blockchain offers a solution by providing a shared, immutable, and tamper-proof record of the movement of goods and related transactions at every stage of the supply chain.

Cryptographic hashing plays a fundamental role in ensuring the integrity and immutability of these records [4]. Each event or transaction in the supply chain, such as the sourcing of raw materials, manufacturing processes, shipping details, and delivery confirmations, can be recorded as a transaction on the blockchain. The cryptographic hash of each block containing these transactions is linked to the hash of the previous block, creating a secure and auditable chain of custody. Any

 doi:10.20944/preprints202504.1814.v1

attempt to tamper with the recorded information would alter the hash of the affected block, breaking the chain and immediately signaling the discrepancy to all participants in the network [4].

Digital signatures are also crucial in supply chain applications of blockchain. They can be used to authenticate the identity of various participants involved in the supply chain, such as manufacturers, distributors, and retailers [4]. For instance, when a shipment of goods changes hands, the receiving party can verify the digital signature of the sending party, ensuring that the information about the transfer is legitimate and originates from an authorized source. This use of digital signatures helps to build trust and accountability among the different entities involved in the complex supply chain ecosystem.

A prominent example of blockchain in supply chain management is IBM Food Trust [4]. This blockchain- based platform allows food producers, distributors, and retailers to track food products from farm to table. Every step in the journey of a food item, including its origin, processing, storage, and transportation, is recorded on the blockchain as an immutable transaction secured by cryptographic hashing. Participants can use their private keys to digitally sign the information they add to the blockchain, and others can verify the authenticity of this information using their public keys. This enhanced traceability helps to improve food safety, reduce waste, and build consumer trust by providing transparency about the origin and journey of the food they consume. Similarly, the Aura Consortium, which includes luxury brands like Louis Vuitton and Prada, utilizes blockchain to prove the authenticity of luxury goods [4]. Each product is given a unique digital identity on the blockchain, and its entire history, from manufacturing to purchase, is recorded and secured using cryptographic methods, helping to combat the proliferation of counterfeit products.

4.2. Healthcare

The healthcare sector is another area where blockchain technology, enabled by cryptography, offers significant potential for improving data security, patient privacy, and interoperability among different healthcare providers. The fragmented nature of healthcare data management, coupled with increasing concerns about data breaches and patient privacy, makes blockchain an attractive solution for creating a more secure and patient-centric system for managing electronic health records (EHRs).

Cryptographic hashing is essential for ensuring the integrity of medical records stored on a blockchain [4]. When a new medical record or update is added to the blockchain, it is stored in a block, and the hash of that block is linked to the previous block in the chain. This cryptographic linking makes it extremely difficult to tamper with past medical records without detection. Any unauthorized alteration would change the hash of the block, breaking the chain and alerting authorized users to the potential data breach [4].

Asymmetric cryptography and digital signatures are critical for controlling access to sensitive patient data and ensuring privacy. In a blockchain-based healthcare system, each patient can have a unique public-private key pair. Their medical records can be encrypted using their public key, ensuring that only those holding the corresponding private key can decrypt and access the information. Healthcare providers, such as doctors and hospitals, can be granted access to a patient's records using digital signatures. The patient can use their private key to sign a permission request, allowing a specific provider to access their records for a defined period or purpose. The provider's identity can be verified using their own public key, ensuring that only authorized individuals can access the patient's sensitive information.

MedRec, a blockchain platform developed at MIT, is a prime example of how cryptography is used in healthcare. MedRec operates as a decentralized record management system that allows patients to control access to their medical data. Patient records are stored on the blockchain, and cryptographic techniques are employed to ensure that only authorized healthcare professionals, who have been granted permission by the patient through digital signatures, can access the data. This patient-centric approach enhances data security and privacy while still enabling seamless and

 doi:10.20944/preprints202504.1814.v1

secure sharing of medical information among authorized providers. Estonia has also implemented a national-level blockchain-based system to secure its entire health records system [4]. This system utilizes blockchain's decentralized and cryptographic features to ensure the integrity and confidentiality of patient data, providing a secure and efficient infrastructure for managing healthcare information across the country.

Table 2. Cryptographic Methods in Real-World Blockchain Applications.

Application Area	**Specific Example**	**Key Cryptographic Methods Used**	**How Cryptography Ensures Security/Functionality**
Supply Chain Management	IBM Food Trust	SHA-256 hashing, Digital Signatures (likely ECDSA or RSA)	Ensures tamper-proof tracking of food products, authenticates participants in the supply chain, verifies the integrity of information added to the blockchain.
Luxury Goods Tracking	Aura Consortium	Hashing (likely SHA-256), Asymmetric Cryptography (unspecified)	Creates unique digital identities for products, records their history immutably, allows verification of authenticity, preventing counterfeiting.
Healthcare	MedRec	Encryption (likely AES or similar), Digital Signatures (unspecified)	Encrypts patient medical records, controls access to data based on patient consent via digital signatures, ensures only authorized professionals can view sensitive information.
National EHR System	Estonia's EHR System	Decentralized blockchain, Cryptographic security (unspecified)	Provides a secure and tamper-proof infrastructure for managing national health records, ensuring data integrity and confidentiality.

 doi:10.20944/preprints202504.1814.v1

The application of blockchain in supply chain management demonstrates how cryptography can establish trust and transparency in complex ecosystems involving multiple stakeholders. By ensuring the integrity and authenticity of data recorded on the blockchain, cryptography underpins the ability of the technology to serve as a single, reliable source of truth across the supply chain. In the healthcare sector, the use of blockchain highlights the critical role of cryptography in safeguarding highly sensitive personal medical information and adhering to stringent privacy regulations. Cryptographic techniques such as encryption and access control mechanisms are essential for enabling the secure and private management of health data on a decentralized platform.

5. Future Directions and Potential Advancements

The field of blockchain technology and its underlying cryptographic methods is constantly evolving, with ongoing research and development focused on addressing current limitations and exploring new possibilities. Several key areas are receiving significant attention, including post-quantum cryptography, enhanced privacy-preserving techniques, advancements in consensus mechanisms, and the integration of blockchain with other emerging technologies.

5.1. Post-Quantum Cryptography

Recognizing the potential threat posed by quantum computers to current cryptographic standards, a significant area of research is dedicated to developing post-quantum cryptography (PQC). These are cryptographic algorithms that are believed to be secure against attacks by both classical and quantum computers. Researchers are investigating various mathematical approaches to construct these quantum- resistant algorithms, with the goal of finding suitable replacements for vulnerable algorithms like RSA and ECC. The development and standardization of robust PQC algorithms are crucial for ensuring the long-term security and viability of blockchain technology in the future.

5.2. Enhanced Privacy-Preserving Techniques

While blockchain inherently offers a degree of pseudonymity, there is a growing demand for more advanced privacy-preserving techniques to be integrated into blockchain systems [5]. One promising area is the development and application of zero- knowledge proofs (ZKPs), such as zk-SNARKs (Zero- Knowledge Succinct Non-Interactive Argument of Knowledge) and zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge) [4]. These cryptographic techniques allow one party to prove the validity of a statement to another party without revealing any information beyond the fact that the statement is true. ZKPs have the potential to enable confidential transactions and private smart contract execution on blockchain networks [4]. Another significant area of research is homomorphic encryption, which would allow computations to be performed on encrypted data without the need for decryption first [4]. This could revolutionize privacy in blockchain applications by enabling data processing and analysis while maintaining confidentiality. Other privacy-focused cryptographic algorithms, such as confidential transactions (e.g., using Bulletproofs) and secure multi-party computation (SMPC), are also being explored for their potential to enhance privacy within blockchain systems [4].

5.3. Advancements in Consensus Mechanisms

Consensus mechanisms are the protocols that allow participants in a blockchain network to agree on the validity of transactions and the state of the ledger [4]. Ongoing research is focused on developing alternative consensus mechanisms that aim to improve upon the scalability, energy efficiency, and security characteristics of traditional Proof-of-Work (PoW) and Proof-of-Stake (PoS) protocols [4]. Cryptography plays a vital role in ensuring the security and fairness of these evolving consensus protocols [4].

 doi:10.20944/preprints202504.1814.v1

5.4. Integration with Other Technologies

The future of blockchain technology is also likely to involve its increasing integration with other emerging technologies, such as the Internet of Things (IoT) and Artificial Intelligence (AI) [4]. In IoT applications, blockchain can provide a secure and transparent platform for managing data generated by connected devices. Cryptographic methods will be crucial for securing communication between IoT devices and the blockchain, as well as for ensuring the integrity and authenticity of the data being recorded [4]. Similarly, the integration of AI with blockchain could lead to more intelligent and automated blockchain systems. Cryptography will play a key role in securing AI models and ensuring the trustworthiness of AI-driven decisions within the context of blockchain applications [4].

The ongoing research and development efforts in post- quantum cryptography demonstrate a proactive approach within the blockchain community to address the future security challenges posed by quantum computing, highlighting a commitment to long-term resilience. The exploration of advanced privacy- preserving techniques signifies a growing awareness of the limitations in current blockchain implementations regarding confidentiality and a strong drive towards creating more user-centric systems where data privacy is paramount [5]. The continuous innovation in consensus mechanisms indicates an ongoing effort to overcome the scalability and efficiency hurdles associated with earlier blockchain designs, paving the way for broader adoption across various industries [4]. The potential integration of blockchain with other transformative technologies like IoT and AI underscores the versatility of blockchain and the crucial role of cryptography in securing these interconnected and intelligent systems of the future [4].

6. Conclusion

This review has explored the fundamental and multifaceted reliance of blockchain technology on cryptographic methods. From the very architecture of the blockchain as a chain of cryptographically linked blocks to the mechanisms that secure transactions and ensure the integrity of the distributed ledger, cryptography forms the bedrock upon which blockchain technology is built [1]. Hashing algorithms provide the means for linking blocks and verifying data integrity, asymmetric cryptography enables secure identity management and transaction authorization through public and private keys, and digital signatures guarantee the authenticity and non-repudiation of actions within the network [1].

Cryptography is not merely an enabling technology for blockchain; it is an intrinsic and indispensable component that underpins its core value propositions of security, transparency, and trust [1]. The strengths offered by cryptographic methods in blockchain, such as immutability, security against double-spending, and data integrity, have been instrumental in its widespread adoption and exploration across diverse industries [4]. However, it is also crucial to acknowledge the limitations and ongoing challenges, including key management complexities and the looming threat of quantum computing.

The landscape of both blockchain technology and cryptography is in constant flux, with continuous research and development pushing the boundaries of what is possible [4]. Future research is actively focused on addressing current limitations through the development of post-quantum cryptography to ensure long-term security, the advancement of privacy- preserving techniques to enhance confidentiality, and the exploration of more efficient and scalable consensus mechanisms [4]. As blockchain technology continues to mature and integrate with other emerging technologies, the role of cryptography will remain central to its security, functionality, and widespread adoption [4].

7. Recommendations for Future Research

Based on the analysis presented in this review, several potential avenues for future research warrant further exploration:

 doi:10.20944/preprints202504.1814.v1

- **Post-Quantum Cryptography for Blockchain:** Continued research and standardization efforts are needed to identify and implement robust post-quantum cryptographic algorithms that are specifically tailored to the requirements and constraints of blockchain environments.
- **Practical Privacy-Preserving Techniques:** Further development and optimization of advanced privacy-preserving cryptographic techniques, such as homomorphic encryption and zero-knowledge proofs, are essential to make them practical and efficient for real-world blockchain applications [5].
- **Security of Integrated Systems:** Research should focus on thoroughly investigating the security implications and potential vulnerabilities that may arise from the increasing integration of blockchain with other emerging technologies like the Internet of Things (IoT) and Artificial Intelligence (AI), with a particular emphasis on the role of cryptography in securing these integrated systems [4].
- **Scalable and Efficient Consensus Mechanisms:** Continued exploration of novel cryptographic approaches within the design of blockchain consensus mechanisms is crucial to enhance their scalability, energy efficiency, and overall performance while maintaining a high level of security [4].
- **Long-Term Security and Resilience:** Ongoing studies are needed to assess the long-term security and resilience of blockchain systems against evolving cryptographic threats, including the potential impact of future advancements in computing power.
- **User-Friendly Key Management Solutions:** Research should be directed towards developing more user-friendly and secure key management solutions to improve the accessibility and security of blockchain technology for a broader audience, addressing a significant barrier to wider adoption [4].

8. Proof of Concept

This section provides a basic implementation of a blockchain system in Python to illustrate the fundamental reliance on cryptographic hashing for linking blocks and ensuring data integrity.

8.1. Detailed Explanation of Steps

1. **Define the Block Structure:** A Block class is created to represent each block in the blockchain. Each block contains an index (its position in the chain), a timestamp (when the block was created), data (representing the transactions or information stored in the block), a previous_hash (the hash of the preceding block), and its own hash.
2. **Implement Hashing Function:** A function calculate_hash is implemented using the hashlib library in Python. This function takes a block as input and generates its SHA-256 hash based on its index, previous hash, timestamp, and data. This cryptographic hash acts as the digital fingerprint of the block.
3. **Create the Blockchain Class:** A Blockchain class is created to manage the chain of Block objects. It initializes with an empty list called chain.
4. **Create the Genesis Block:** A method create_genesis_block is implemented within the Blockchain class to create the very first block in the chain. This block has a fixed index of 0 and a previous_hash of "0".
5. **Add New Blocks:** A method add_block is implemented to add new blocks to the blockchain. When a new block is added, its previous_hash is set to the hash of the last block in the chain, establishing the cryptographic link. The new block's own hash is then calculated using the calculate_hash function.

8.2. Code and Relevant Details

The Python code for this basic blockchain implementation is provided in the Appendix. The code demonstrates how the SHA-256 hashing algorithm is used to generate a unique hash for each block based on its content and the hash of the preceding block. This cryptographic linking ensures the integrity of the blockchain, as any alteration to a block would change its hash and break the chain.

 doi:10.20944/preprints202504.1814.v1

8.3. Outputs

Output of the basic blockchain implementation in Python, demonstrating the creation of a genesis block and two subsequent blocks. The output shows the index, timestamp, data, previous hash, and hash for each block, illustrating the cryptographic linking between blocks.

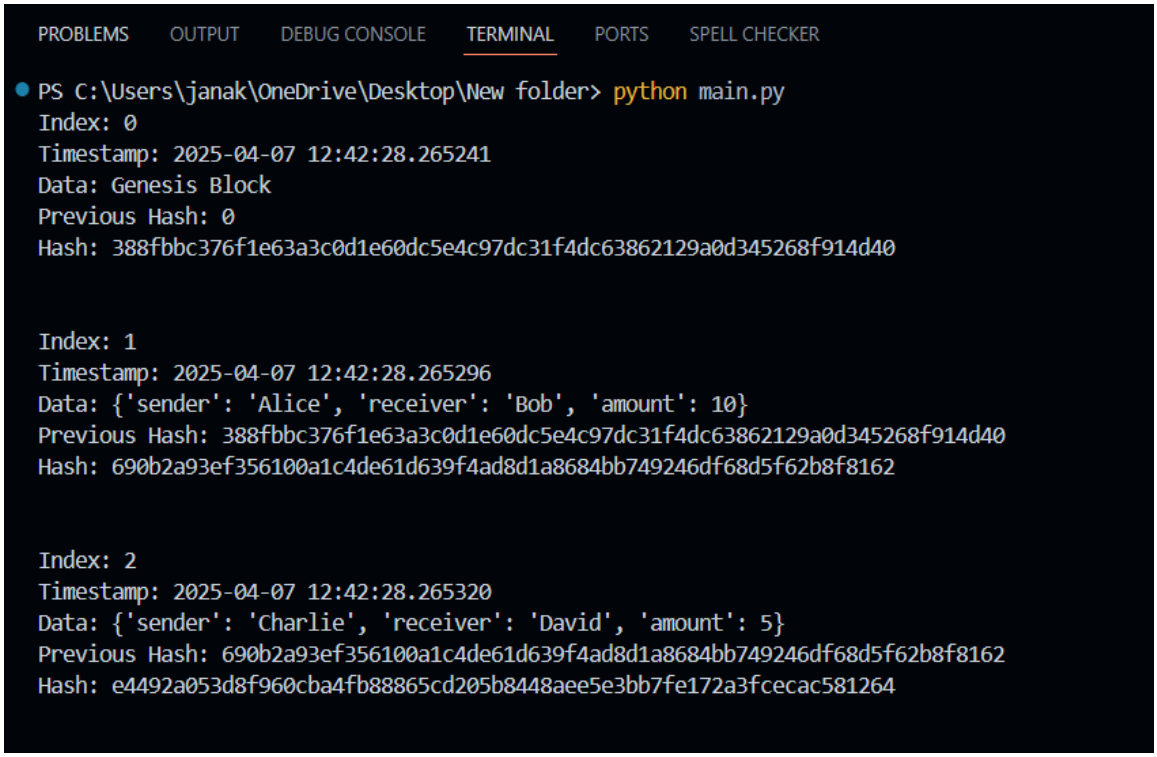

Figure 1. Output of the basic blockchain implementation in Python.

Appendix

This appendix provides a Python code implementation that illustrates key concepts discussed in the paper, specifically focusing on blockchain technology and cryptographic techniques. The code demonstrates a simplified blockchain system where blocks are linked using cryptographic hashing to ensure data integrity.

Purpose

The provided code implements a basic blockchain structure, showing how SHA-256 hashing connects each block to the previous one. This relates to the theoretical discussion in the paper about securing data in decentralized systems.

Overview

- Language: Python
- Key Components:
  - Block class: Defines a block with attributes like index, data, and a hash linking to the prior block.
  - calculate_hash function: Computes the SHA-256 hash for each block.
  - Blockchain class: Manages the chain, starting with a genesis block and adding subsequent blocks.
- Functionality: Creates a blockchain and demonstrates block chaining via hashing.

Prerequisites

Requires Python 3.x with standard libraries hashlib and datetime (no external dependencies).

 doi:10.20944/preprints202504.1814.v1

Note

Review the code below for a practical view of the concepts. It complements the paper's theoretical insights with a hands-on example.

```
import hashlib
import datetime

class Block:
def __init__(self, index, timestamp, data, previous_hash):
self.index = index
self.timestamp = timestamp
self.data = data
self.previous_hash = previous_hash
self.hash = self.calculate_hash()

def calculate_hash(self):
block_string = str(self.index) + str(self.timestamp) + str(self.data) + str(self.previous_hash)
return hashlib.sha256(block_string.encode()).hexdigest()
class Blockchain:
def __init__(self):
self.chain = [self.create_genesis_block()].

def create_genesis_block(self):
return Block(0, datetime.datetime.now(), "Genesis Block", "0")

def get_last_block(self):
return self.chain[-1].

def add_block(self, new_block):
new_block.previous_hash = self.get_last_block().hash
new_block.hash = new_block.calculate_hash()
self.chain.append(new_block)

# Example Usage
my_blockchain = Blockchain()

# Add first block
first_block_data = {"sender": "Alice", "receiver": "Bob", "amount": 10}
first_block = Block(1, datetime.datetime.now(), first_block_data, my_blockchain.get_last_block().hash)
my_blockchain.add_block(first_block)

# Add second block
```

 doi:10.20944/preprints202504.1814.v1


```
second_block_data = {"sender": "Charlie", "receiver": "David", "amount": 5}
second_block = Block(2, datetime.datetime.now(), second_block_data, my_blockchain.get_last_block().hash)
my_blockchain.add_block(second_block)

# Print the blockchain
for block in my_blockchain.chain:
print("Index:", block.index)
print("Timestamp:", block.timestamp)
print("Data:", block.data)
print("Previous Hash:", block.previous_hash)
print("Hash:", block.hash)
print("\n")
```

References

1. F. Mohammad Saeidia, M. H. Zahedi, and E. Farahani, "A Secure and Reliable Model for Financial Documents Using Digital Signature and Blockchain Technology," *AI and Tech in Behavioral and Social Sciences*, vol. 3, no. 1, pp. 23–33, 2025.
2. National Institute of Standards and Technology, "Blockchain Technology Overview," *NIST Interagency Report 8202*, 2018.
3. J. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia, "Quark: A lightweight hash function," in *Cryptographic Hardware and Embedded Systems – CHES 2013*, R. Avanzi,L. Knudsen, and C. Paar, Eds. Berlin, Heidelberg: Springer, 2013, pp. 186–201.
4. S. W. Lo, Y. Wang, and D. K. C. Lee, "Cryptography and Blockchain Technology," in *Foundations for Fintech*, Singapore: World Scientific, 2021, pp. 1–30.
5. G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *University of Toronto*, 2014.
6. V. Buterin, "Ethereum: A secure decentralised generalised transaction ledger," *University of Toronto*, 2014.
7. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
8. Z. Zheng, S. Xie, H.-N. Dai, and X. Chen, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, 2017, pp. 557–564.
9. A. C. H. Chen, "Evaluation of Hash Algorithm Performance for Cryptocurrency Exchanges Based on Blockchain System," *arXiv preprint arXiv:2408.11950*, 2024.
10. M. Mohana, "An Adaptive Elliptical Curve Cryptography-Rivest-Shamir-Adleman- based Encryption for IoT Healthcare Security Model with Blockchain Technology," *Journal of Mechanics in Medicine and Biology*, vol. 23, no. 07, 2023.
11. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
12. A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT," *Sensors*, vol. 18, no. 8, p. 2284, 2018.