STM JOURNALS

Journal of
Artificial Intelligence
Research & Advances

ISSN: 2395-6720
Volume 11, Issue 3, 2024
September–December
DOI Journal: 10.37591/JoAIRA

https://journals.stmjournals.com/joaira

Review JoAIRA

Blockchain from the Cryptographic Perspective of Privacy and Anonymization for Sustainability

Sharique Jamal[1,*], Sherin Zafar[2]

Abstract

This paper delves into the fascinating intersection of cryptography and blockchain technology. It explores the implementation of blockchain in cryptography, highlighting how cryptographic algorithms improve the security of blockchain systems. This paper looks at various issues such as why cryptographic methods in use with blockchain networks guarantee data security, confidentiality, and credibility. It also examines the relationship between consensus algorithms and cryptography, shedding light on how these elements work together to maintain the trust and reliability of blockchain systems. Furthermore, this paper explores the role of smart contracts in enhancing security within blockchain networks. It discusses how smart contracts can leverage cryptographic techniques to mitigate risks and vulnerabilities associated with transactions and data storage on the blockchain. In addition to examining the implementation of cryptography in blockchain technology, this paper conducts a comprehensive literature review. Analyzing existing research and studies on this subject matter aims to provide valuable insights into current advancements, challenges, and potential future directions for improving the security of blockchains through cryptographic algorithms. All in all, this study addresses important issues regarding risk management and improves overall blockchain security, making it a useful tool for scholars, practitioners, and enthusiasts interested in comprehending the complex relationship between cryptography and blockchain technology. Sustainability considerations are gaining significance in the rapidly advancing field of blockchain cryptography. Maintaining the security and environmental consciousness of the blockchain ecosystem requires balancing energy efficiency and cryptographic strength.

Keywords: Blockchain, cryptography algorithm, blockchain security, preferences, risk & security, smart contracts

INTRODUCTION

In the ever-evolving technology landscape, blockchain has emerged as a groundbreaking innovation with immense potential. In the blockchain, the data are maintained in a distributed manner. A crucial aspect that ensures the integrity and security of a blockchain is cryptography. The implementation of cryptography algorithms in blockchains plays a pivotal role in safeguarding sensitive information, securing transactions, and mitigating risks. This study delves into the intersection of cryptography and blockchain, exploring how cryptographic algorithms are utilized within this decentralized system. We delve into the inner workings of various consensus algorithms, smart contracts, and their relationship with cryptography. By examining the integration of these elements, we aim to shed light on how blockchain security can be enhanced using

***Author for Correspondence**
Sharique Jamal
E-mail: Shariquejamal248@gmail.com

[1]Student, Department of Computer Science Engineering, School of Engineering Science and Technology (SEST), Jamia Hamdard, New Delhi, India
[2]Assistant Professor, Department of Computer Science Engineering, School of Engineering Science and Technology (SEST), Jamia Hamdard, New Delhi, India

Received Date: May 18, 2024
Accepted Date: September 20, 2024
Published Date: October 07, 2024

Citation: Sharique Jamal, Sherin Zafar. Blockchain from the Cryptographic Perspective of Privacy and Anonymization for Sustainability. Journal of Artificial Intelligence Research & Advances. 2024; 11(3): 13–30p.

© STM Journals 2024. All Rights Reserved

robust cryptographic measures. Furthermore, this study seeks to identify vulnerabilities within existing cryptographic implementations of blockchain systems. Through an extensive literature review, we will analyze past research studies and advancements to gain insights into potential risks and explore strategies to address them effectively. By delving into the intricate connection between blockchain technology and cryptography algorithms, this study aims to contribute to a deeper understanding of how these components work together to enhance security within decentralized systems.

In a blockchain, data are stored in a distributed manner. Owing to the integrity and availability provided by blockchain technology, users can create, inspect, and validate transactions recorded in a distributed manner. However, it forbids deleting and changing transactions or other data stored in its blocks. The blockchain system is supported and protected by digital signatures, hash functions, and other cryptographic primitives and protocols [1]. In addition to offering integrity protection, authenticity verification, and non-repudiation to transactions recorded in the ledger, these primitives guarantee data secrecy. Furthermore, because blockchain technology is a distributed network, it requires a consensus protocol— a set of guidelines that each player must abide by—for all participants to agree on a single, globally unified view.

The advantageous features of blockchain technology, including decentralization, independence credibility, consistency, confirmation, tolerance for faults, privacy, auditability, and transparency, have received considerable attention from educational and commercial communities in recent years. These advanced features have made blockchains a focal point of interest in various fields. Cryptography, with its profound historical legacy, continues to adapt to and thrive in the modern age. Its roots can be found in 2000 B.C. when the Greeks and Egyptians used coded inscriptions and enigmatic hieroglyphics. The legendary Caesar cipher of ancient Rome also attests to its enduring significance [2]. Currently, billions of people worldwide employ cryptography daily to protect their data and are often unaware of its presence. Although cryptography has many uses, its security is questionable because of the possibility of a single programming error or specification flaw compromising the system [3]. Cryptographic algorithms, rooted in mathematical procedures, metamorphose plain-text data into an inscrutable entity known as ciphertext, rendering it indecipherable without the corresponding decryption key. These algorithms empower the secure transmission and storage of sensitive data, guaranteeing both confidentiality and the unaltered authenticity of information. A crucial role is played by text encryption, a popular use of cryptographic algorithms that can be achieved by less complex means such as the Caesar cipher or more complex ones like AES the Advanced Encryption Standard (AES) and RSA (Rivest-Shamir-Adleman). Scholars and practitioners in this field have always come up with new ideas to satisfy a variety of security needs. In the following sections, we examine the methodology, literature review, gaps in the field, and a detailed examination of the applications.

LITERATURE REVIEW

Within the discipline of computer science, networks, and computer security are dynamic and ever-changing areas of study. It continuously adjusts to the rapidly advancing technological landscape and the persistent threats from malevolent actors. The foundation of information protection is in algorithmic and mathematical components, such as hashing algorithms and encryption, which are the subjects of security courses in this ever-changing context.

Because hackers persistently seek to breach network systems, the need for up-to-date knowledge and expertise drives the creation of new courses that address the latest types of cyberattacks. However, these attacks have rapidly become obsolete as security software providers respond to timely countermeasures. Constant competition to outwit one another characterizes the relationship between security experts and hackers. In the middle of this never-ending tug-of-war, new terms and abilities in the field of security continue to develop. The cybersecurity landscape is constantly evolving, and factors such as businesses, network optimization, security design, and legal foundations have a significant influence. To remain competitive in this demanding setting, industry experts must adopt an attitude of constant learning and

© STM Journals 2024. All Rights Reserved

adjustment. In summary, network and computer security represent a constantly evolving discipline, in which the primary focus lies on encryption, hashing, and other key algorithms. It is a realm where practitioners and adversaries engage in a ceaseless battle, leading to a continuous stream of new courses and security practices. The ever-growing lexicon of security terminology and the emergence of innovative techniques contribute to the advancement and resilience of this critical field, safeguarding vital information and digital infrastructure from threats. In their study referenced in [4], Othman O. Khalifa and colleagues effectively elucidated the fundamental principles, attributes, and objectives of cryptography. Their work underscores the significance of privacy in the contemporary era, often referred to as the "age of information'." They underscored how communication, a pivotal driver of technological advancement, necessitates robust measures to ensure the confidentiality and security of data transmitted through various communication channels. Nitin Jirwan et al. [5] The world of data communication primarily revolves around digital transmission, where ensuring data security takes precedence through the utilization of encryption algorithms. The paramount goal is to safely deliver data to the intended recipients without compromising confidentiality. In this context, various cryptographic techniques, including symmetric and asymmetric methods, play a vital role in data transmission. These techniques are pivotal in safeguarding sensitive information from unauthorized access and potential threats and ensuring the integrity and privacy of the communicated data. Sandeep Tayal and colleagues [Tayal et al., 6] emphasized the significant data proliferation brought about by the growth of social networks and e-commerce applications in businesses throughout the world in a thorough analysis of network security and cryptography. Information security is of utmost importance because of the increase in data generation, particularly with regard to guaranteeing the safe transit of data via the Internet. As Internet user numbers continue to escalate, the importance of cryptography techniques becomes even more apparent [5]. This article offers a detailed overview of the myriad strategies employed within networks to bolster security, with particular emphasis on cryptography. Moreover, the historical foundations and significance of cryptography were discussed by Gupta et al. [Gupta et al., 7], providing insight into how information security has developed into a significant concern in the fields of computing and communications. This paper not only presents cryptography as a means of guaranteeing the identity, availability, integrity, authentication, and confidentiality of users and their data by offering security and privacy but also provides an extensive array of asymmetric algorithms that have given us the ability to protect and guarantee the security of our data. As we proceed with the objectives of cryptography, as outlined by Massey [8], the two main objectives of this secure communication technique are secrecy and authenticity. To guarantee the security and integrity of the sensitive data, these two objectives are essential.

Fraga-Lamas, P., and Fernandez-Carames (2020). This research addresses the security of blockchains in the future using quantum-resistant encryption. It addresses the need for novel cryptographic frameworks, including multivariate polynomial- and lattice-based encryption. This research focuses on securing blockchains in the post-quantum future because quantum computing poses a possible danger to blockchain technology as it develops [9].

Ferdous, M. S., Hoque, M. A., and Chowdhury, M. J. M. (2021). This review discusses the effects of modern consensus techniques, such as proof-of-stake (PoS), on public blockchain scalability and energy efficiency. Knowing the effects of newer consensus algorithms is essential for the longevity of the blockchain, as proof of work (PoW) is replaced with Proof-of-Stake (PoS) in Ethereum 2.0 [10].

Van Moorsel and Alharby (2019). The security, difficulties, and development of smart contracts, which are essential for decentralized applications, are the main topics of this study. Blockchain networks are increasingly integrating smart contracts, and developing blockchain technologies requires an understanding of the security issues and vulnerabilities they provide [11].

In 2020, Zhang, K., Wang, X., Cheng, X. Security, and privacy concerns with blockchain technology, including cryptographic techniques such as ring signatures and zero-knowledge proofs, were thoroughly

© STM Journals 2024. All Rights Reserved

examined in this review article. Including current security issues guarantees a thorough comprehension of the cryptographic security of blockchains in contemporary systems [12].

In 2019, Yaga, D., Roby, N., Mell, P., Scarfone, K. This study provides a technical overview of blockchain technology, which also covers cryptography techniques, consensus methods, and scalability concerns. It provides a governmental perspective on the prospects for blockchain technology and acts as a manual for regulatory compliance when using blockchain technology [13].

The goal of authenticity is to determine the reliability and provenance of data so that recipients can verify the integrity of the data and validate its source's legitimacy, guaranteeing that it does not change while being transmitted. By employing theoretical frameworks, such as Simmon's theory of theoretical authenticity, cryptography strives to build robust mechanisms that validate the authenticity of data, providing a solid foundation for secure communication and digital interactions. On the other hand, secrecy, a cornerstone of cryptography, aims to protect sensitive information from prying eyes and unauthorized access. The practical and theoretical aspects of security are closely intertwined in this pursuit, and Shannon's theory of theoretical secrecy is a fundamental concept. It lays the groundwork for developing encryption techniques that render data unintelligible to anyone lacking the proper decryption key, thwarting malicious attempts at eavesdropping and data compromise [14]. Convergence of authenticity and secrecy within cryptography is essential for fostering trust in the digital world. As we explore the intricacies of cryptographic algorithms and techniques, we uncover a landscape in which the protection of data integrity and confidentiality go hand in hand [15]. In this journey, we come to understand that cryptography is not merely a shield against potential threats but also a vital enabler for secure communication, authentication, and the preservation of sensitive information. Through a deeper understanding of these two core goals, we can unlock the full potential of cryptography and harness its power to fortify the security of an interconnected society.

METHODOLOGY TO BE UTILIZED

In cryptography, the primary objective is to ensure the confidentiality of information by transforming it into an unintelligible form, making it incomprehensible to unauthorized individuals. This is achieved through a process known as encryption, where the original information, termed "plaintext," is concealed and converted into "ciphertext." Encryption relies on specific rules and procedures known as "encryption algorithms," which operate on the plaintext and an "encryption key" provided as input.

Cryptography has widespread applications in two key scenarios. First, it facilitates the secure transmission of data through insecure channels, such as the Internet, safeguarding information from interception, and unauthorized access during transit. Second, it serves to prevent unauthorized individuals from comprehending the content of information, especially when they have illicitly gained access. To reverse the encryption process and retrieve the original information, the intended recipient employs a "decryption algorithm" along with the appropriate "decryption key." This process effectively transforms the ciphertext back into its original plaintext form, enabling the authorized party to access and interpret information securely. Through these encryption and decryption mechanisms, cryptography plays a crucial role in safeguarding sensitive data, enabling secure communication, and ensuring the integrity of digital transactions [16]. Post-quantum cryptography, which addresses the possible influence of quantum computers on existing encryption techniques, is an interesting and unexplored field of cryptography. Even though they are still in their infancy, quantum computers can crack many encryption schemes that protect digital communications today. Researchers are working hard to create new encryption algorithms in response to this threat and methods that should be safe even from highly potent quantum computers. These post-quantum cryptographic techniques investigate new mathematical frameworks including multivariate polynomial cryptography, lattice-based cryptography, and code-based encryption. The inclusion of a section on post-quantum cryptography in your review paper can add a unique and forward-looking perspective to the field. This highlights the ongoing efforts

© STM Journals 2024. All Rights Reserved

to adapt to emerging technological challenges and underscores the dynamic nature of the cryptography landscape. Many researchers have anticipated numerous security algorithms that can detect cryptographic attacks. In this case, there must be a new security system through steganography and cryptography. The complete cryptography process is illustrated in Figure 1.

Applications of Cryptography and Blockchain

Digital currencies, end-to-end encryption, electronic signatures, secure web browsing, and computer passwords. The analysis indicates that ECC is superior to RSA in several ways, including key size, speed, and attack resistance [17].

Applications for blockchain technology are numerous and span a number of sectors, including government, healthcare, and finance. The principal uses of blockchain technology are as follows.

Blockchain technology has revolutionized various industries and offers numerous benefits. One significant area is money transfer, where blockchain enables faster and cheaper transactions, particularly cross-border transfers. In addition, blockchain can be utilized to establish secure and tamper-proof identity management systems to ensure personal identity security. In the healthcare sector, blockchain applications can enhance payment processing, maintain electronic medical records, manage provider directories, and ensure data security. Similarly, in logistics, blockchains can track and manage supply chains, guaranteeing transparency and security throughout the process. Non-fungible tokens (NFTs) are becoming increasingly well-known as distinct digital assets that signify the ownership of goods or content. Governments can use blockchain technology to increase agency efficiency, simplify services, and strengthen voting processes. Media industries can leverage blockchain to track copyright and intellectual property rights, distribute content, and monetize content effectively. Blockchain can streamline lending processes, reduce the need for intermediaries, and improve efficiency. Blockchain technology can create transparent and secure insurance policies, manage claims, and prevent fraud in the insurance sector. Real estate transactions can benefit from blockchain technology by creating transparent and secure property records and streamlining the process. Blockchain also offers secure personal data storage by storing sensitive information in a decentralized network, thereby ensuring enhanced security and privacy [18]. Finally, in education, blockchain can create secure and transparent educational records while streamlining the accreditation process, as shown in Table 1.

Table 1. Blockchain architecture.

	Bitcoin	**Ethereum**	**Hyperledger**
Layer of applications	Trading Bitcoins	Trading Ethereum	Business blockchain
Layer of networks	P2P based on TCP	P2P based on TCP	P2P based on HTTP/2
Layer of contracts	Screenplay	Sturdiness/Script EVM	Java Docker/Go
Layer of consensus	PoW	PoW/PoS	SBFT/PBFT
Layer of data	Merkle tree	Merkle's patrician tree	Tree Merkle Bucket

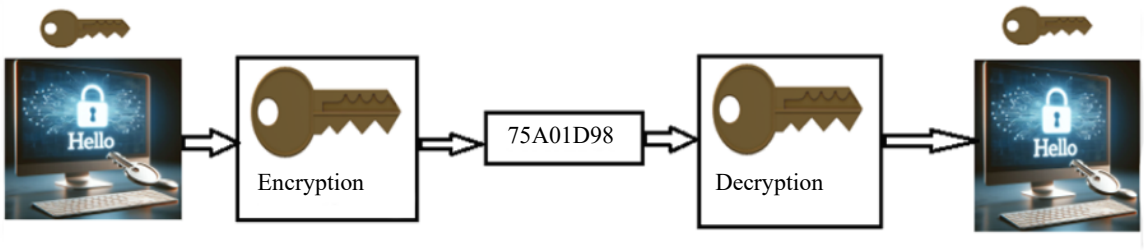

Figure 1. Cryptography concept.

© STM Journals 2024. All Rights Reserved

Block-based data structures are the principal tool used by the data layer to preserve the integrity of data storage. In this network, every node collects the data transactions it receives, groups them into time-stamped blocks, and links these blocks to the longest main blockchain for storage. Block storage, chain structures, hash algorithms, Merkle trees, timestamping, and other methods are used in this layer, as shown in Figure 2.

Gaps in Cryptographic Algorithm

In addition to the four fundamental elements of data security, several concerns impact the practical use of data. In any case, it can be difficult for a genuine client to access clearly jumbled, reliable, and meticulously labeled material during a crucial navigational phase. A computer system or network may be attacked by an attacker, making it unusable. High availability is one of the most crucial components of information security, which cryptography cannot ensure. Additional tactics are needed to defend against dangers, such as a denial-of-service attack or total information system collapse. In addition, selective access control is a basic criterion for information security that cryptography cannot provide. Administrative control and procedures must be followed. Vulnerabilities and threats against which encryption is powerless originate from ill-conceived systems, protocols, and procedures. A defensive infrastructure must be properly designed and built to address these issues. The implementation of public-key cryptography requires significant financial investment for the creation and maintenance of public-key infrastructure. The computational difficulty of numerical problems determines the security of cryptographic processes. Cryptography techniques could become vulnerable to any advancement in addressing numerical issues or increasing processor power.

Blockchain Preferences

The security and usefulness of blockchain preference have been largely shaped by cryptographic algorithms. Similarly, the Secure Hash Algorithm (SHA) hash function ensures that Merkle Trees have an immutable ledger, and hash functions are key components of both. Each transaction is digitally signed and forms the basis of transparency and integrity in the system. Through public-key cryptography, secure communication lines are established, thereby creating a network of security concerning confidentiality. Zero-knowledge proofs allow transaction verification while maintaining sufficient anonymity to protect privacy. Elliptic curve cryptography is highly efficient for cryptographic operations, where transactions require multiple signatures as an added control measure. AES secures data confidentiality, whereas Merkle Trees ensures efficiency in verifying large datasets. The algorithms do not work in isolation but rather entwine to create a complex but firm and reliable blockchain framework. They are critical in preventing tampering, and unauthorized access, and assuring that the ecosystem operates based on the principles of transparency and fairness, as shown in Figures 3-5.

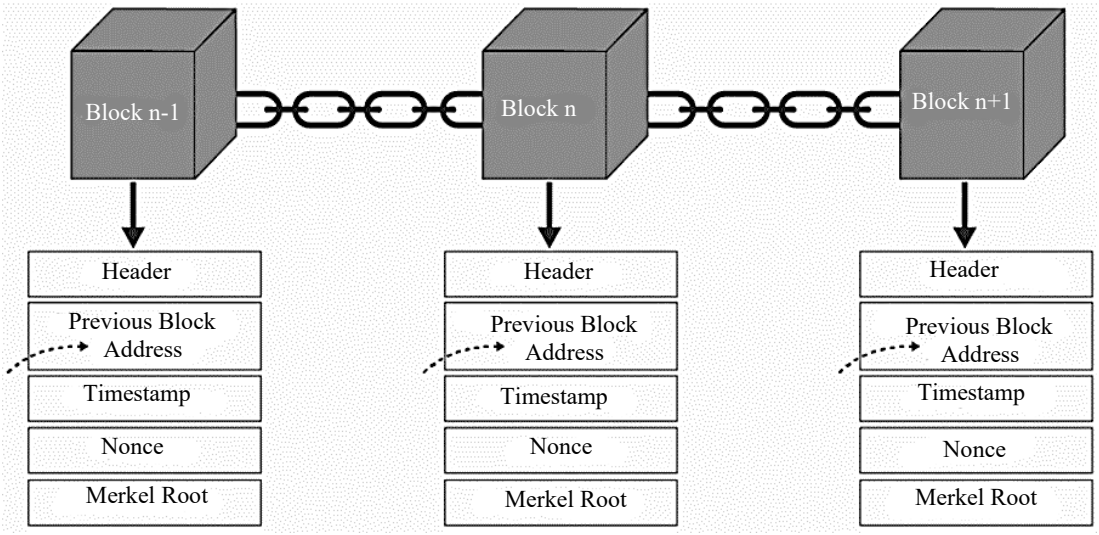

Figure 2. Structure Of Blockchain.

© STM Journals 2024. All Rights Reserved

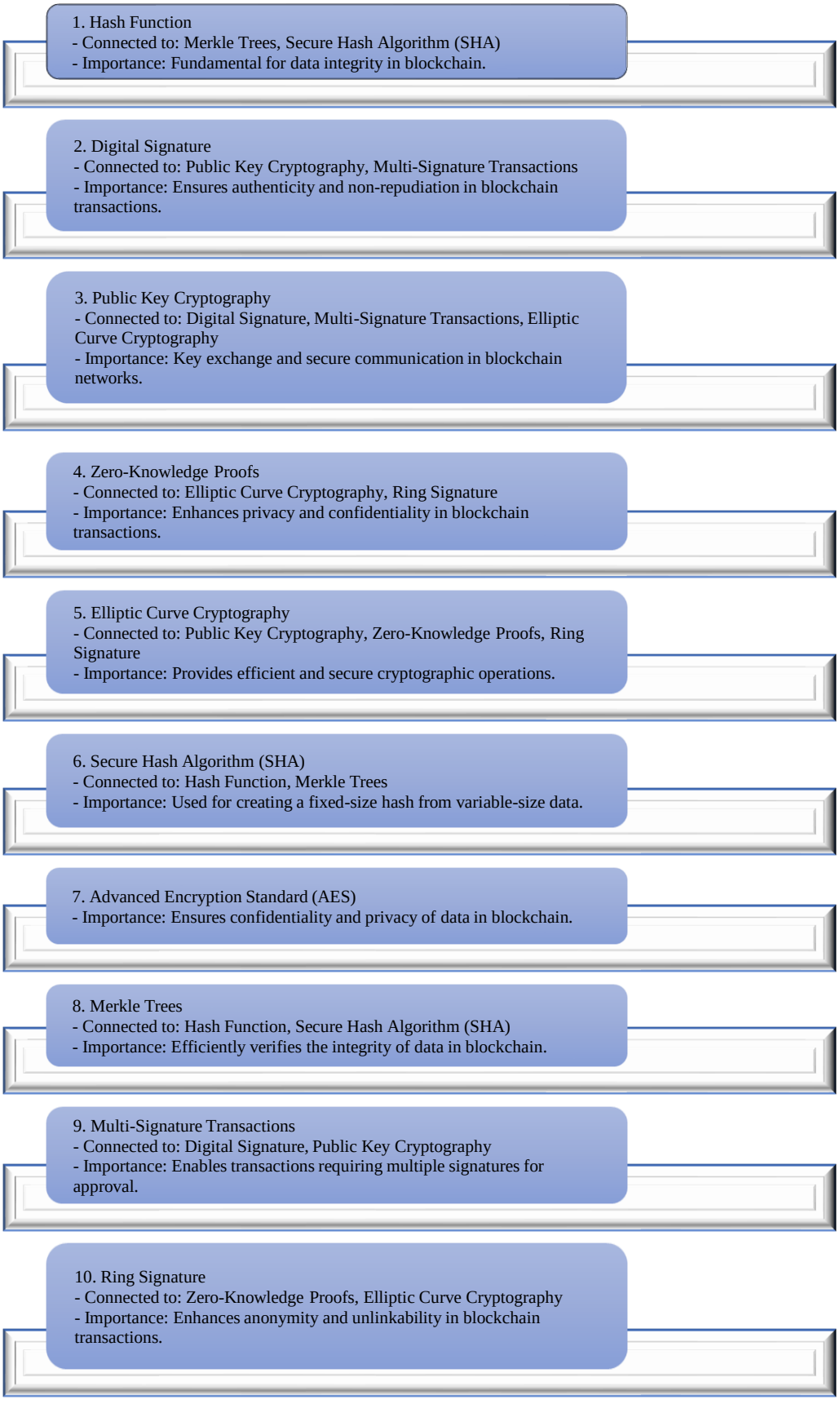

Figure 3. Interconnected Algorithms and Their Significance.

© STM Journals 2024. All Rights Reserved

Efficiency in Security

Measuring security with respect to cryptographic algorithms in the context of the blockchain is usually quite difficult, with such challenges depending on different facets, including, but not limited to, the implementation, key management, and peculiar use cases. However, a qualitative assessment is still possible, for example, through a histogram representing their relative strengths and uses. A conceptual breakdown is presented in Table 2.

Table 2. Analysis and Significance in Blockchain Security

Efficiency in Security and Implementation of the Following Algorithms			
Algorithm (Cryptography)	Security	Implementation	Use Cases
1. Hash Function	High	Moderate	Data Integrity
2. Digital Signature	High	High	Transaction Authentication
3. Public Key Cryptography	High	High	Secure Communication
4. Zero-Knowledge Proofs	High	Moderate	Privacy-Preserving Transactions
5. Elliptic Curve Cryptography	High	High	Efficient Cryptographic Operations
6. Secure Hash Algorithm (SHA)	High	High	Data Integrity and Hashing
7. Advanced Encryption Standard (AES)	High	High	Data Confidentiality
8. Markle Trees	High	High	Integrity Verification
9. Multi-Signature Transactions	High	High	Multi-Party Approval
10. Ring Signature	High	Moderate	Anonymity in Transactions

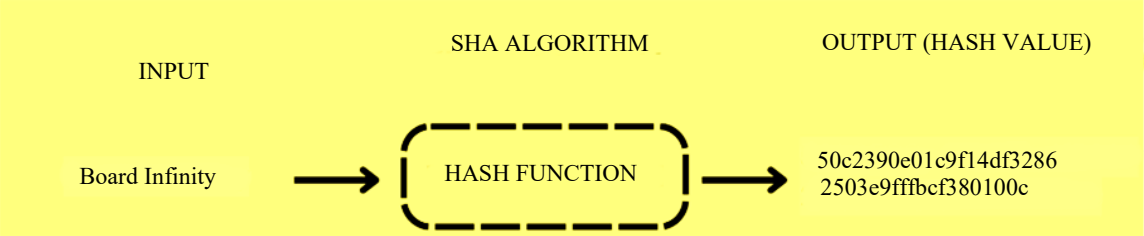

Figure 4. Structure of secure hash algorithms (sha).

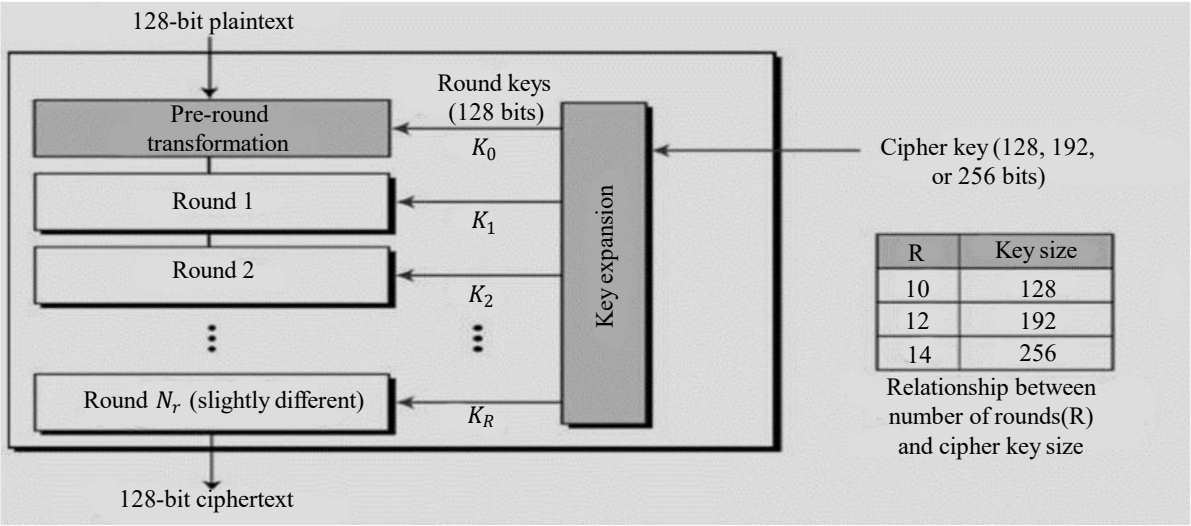

Figure 5. Structure of advanced encryption standard (AES).

© STM Journals 2024. All Rights Reserved

Cryptographic algorithms and their implementations and critical algorithms used in blockchain technology:

SHA-256 (Secure Hash Algorithm 256-bit)

- *Function on the Blockchain:* A fixed-size hash of any arbitrary data is created by Bitcoin using the SHA-256. The hash of the preceding block is included in the newly produced block, which connects the blocks and guarantees chain integrity.
- *Process:* This method employs a number of logical operations, such as XORs, shifts, and modular adds, to process an input. The result is a 32-byte, 256-bit hash that is almost difficult to reverse because it is one-way.
- *Implementation:* Proof of Work (PoW) systems commonly employ SHA-256. By modifying the block's nonce, miners attempt to discover a hash that satisfies the necessary difficulty during the mining process. This guarantees the immutability and security of the blockchain because altering any data would require recalculating all subsequent hashes.

Elliptic Curve Cryptography (ECC)

- *Use in Blockchain:* Digital signatures (ECDSA in Bitcoin and Ethereum, for example) and key creation in blockchains are handled by ECC. ECC is more efficient than RSA because it allows smaller keys with equivalent security.
- *Mathematics:* The algebraic structure of elliptic curves over finite fields serves as the foundation of ECC. An elliptic curve is often represented by the equation ($y^2 = x^3 + ax + b$), where the points of the curve are utilized for encryption and key creation.
- *Digital Signatures:* Public and private keys are generated via ECC in blockchain technology. A user's public key is produced by multiplying its private key by the generator point on the curve. The private key was a random integer. Digital signatures can be verified using the public key without disclosing the private key, thereby ensuring the authenticity of transactions.

Zero-Knowledge Proofs (ZKPs)

- *Application:* Zcash and other privacy-focused blockchains employ Zero-Knowledge Proofs, particularly Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs). They withhold information regarding the value itself but let one party demonstrate to another that they are aware of it.
- *Structure:* A zk-SNARK comprises three parts: a statement, a verifier, and a prover. The verifier examines the proof without accessing the value, whereas the prover produces evidence that the prover is aware of the value and that it satisfies specific requirements (such as a legitimate transaction).
- *Benefits:* By enabling verification without disclosing sensitive information such as transaction amounts or user names, ZKPs enable privacy-preserving transactions. For blockchain applications, where privacy is a major concern, this is essential.

Merkle Trees

- Merkle trees are a type of tree data structure employed in blockchain technology to effectively verify the integrity of big datasets. Because this makes it possible to verify transactions efficiently and securely within a block, it is essential to blockchains.
- *Structure:* Every leaf node in a Merkle tree is a hash of a data block, and every non-leaf node is a hash of the nodes that comprise its children. The integrity of the entire block is guaranteed by the inclusion of the Merkle root (also known as the root of the Merkle tree) in the block header.
- *Efficiency:* A hash path from a transaction to the Merkle root is required to demonstrate the existence of a transaction within a block. This improved the computational efficiency of the verification process.

© STM Journals 2024. All Rights Reserved

Advanced Encryption Standard (AES)

- *Use in Blockchain:* To protect secrecy, sensitive data such as private keys are encrypted using AES, which is extensively utilized in blockchain systems.
- *Method:* The AES encryption technique uses symmetric keys, meaning that the same key is used for both encryption and decryption. It uses blocks of data (usually 128 bits) and performs several operations, including substitution, permutation, and mixing, to convert plaintext into ciphertext.
- *Modes of Operation:* Depending on whether integrity and/or secrecy are required, AES can be employed in a variety of modes, including Cipher Block Chaining (CBC) and Galois/Counter Mode (GCM).

Digital Signatures (ECDSA)

- *Role:* Digital signatures on blockchain, namely the elliptic curve digital signature algorithm (ECDSA), guarantee the authenticity of transactions and ownership of the private key pertaining to them.
- *Procedure:* The user's private key is utilized to generate a distinct digital signature for a transaction. The public key may then be used by the network to validate the signature without disclosing the private key, guaranteeing non-repudiation and authentication.
- *Security:* The complexity of the elliptic curve discrete logarithm problem makes it impossible to compute the private key from the public key, making the ECDSA safe.

Ring Signatures

- *Application:* Signers can sign a message on behalf of a group without disclosing their identity, thanks to Monero's usage of ring signatures.
- *Structure:* A ring signature is made up of a collection of potential signers; however, it is difficult to determine which signer contributed to the signature owing to cryptography.
- *Use Case:* This technique ensures privacy in blockchain transactions by maintaining anonymity while permitting transaction validity verification.

ANALYSIS

Therefore, cryptographic algorithms form the essential basis for ensuring safety, consistency, and privacy in distributed systems through the blockchain. Cryptographic algorithms are central to ensuring secure transactions and preserving the integrity of the distributed ledger. For instance, the hashing function used for the Merkle tree and secure hash algorithm helps to prove data authentication. The cryptographic toolbox has one item of particular importance, called digital signatures, which authenticates transactions. These are responsible for non-refunding, originality, and correctness of the data. Public key cryptography is the cornerstone of building secure communication and key exchange, which underpins the safe interaction between blocks within the chain. Furthermore, it employs more sophisticated cryptography, such as zero-knowledge proofs, which enable private validations devoid of private information disclosure. Elliptic curve cryptography and multi-signature transactions add additional layers of security to this security framework, ensuring that the system functions according to cryptographic requirements and allows transactions that require multiple approvals. In other words, the cryptographic algorithm in the blockchain secures not only malicious activities but also creates an open, secure, and trustworthy space for peer-to-peer trust, as shown in Table 3.

Strengths and Weaknesses

The strengths and weaknesses of the cryptographic algorithms are listed in Table 4. Collision attacks compromise the efficiency of the hash function and are an integral measure of information integrity, being both efficient and irreversible. Digital Signatures are great for authentication; however, they need strong key management to avoid weaknesses of non-repudiation and transaction integrity. Public Key Cryptography supports secure communication and digital signatures but faces key management issues and the likelihood of quantum attacks.

© STM Journals 2024. All Rights Reserved

Table 3. Analysis and significance in blockchain security.

Algorithms	Importance
Hash function	In the world of technology, hash functions like SHA 256 (used in Bitcoin) and Keccak 256 (used in Ethereum) are tools. They accept any length of input data. Convert it to a digest or fixed-length hash value. The blockchain system uses these hash methods for the following reasons: 1. Ensuring Data Integrity; Hashes are employed to ensure that the data remains intact. If any modifications are made to the input data it will result in a hash value thereby indicating that the data has been tampered with. 2. Verifying Blocks; In blockchain, blocks are interconnected using the block's hash often known as the Merkle root. This interlinking creates a tamper-resistant chain of blocks guaranteeing the reliability of the blockchain. 3. 3. Powering Proof of Work; Hash functions play a role in mining, where miners compete to discover a nonce (a number) that produces a hashed value below a predetermined target. This process is essential, for adding blocks to the blockchain while providing security and validating transactions.
Digital signature	Confirming the legitimacy and security of transactions is a crucial function of digital signature algorithms like EdDSA (Edwards-curve Digital Signature Algorithm) and ECDSA (Elliptic Curve Digital Signature Algorithm). They are vital for the following two reasons: 1. Proving Ownership: Digital signatures provide evidence that the person initiating a transaction is indeed the rightful owner of the private key associated with it. 2. 2. Securing Transactions: Using the sender's private key to sign transactions helps to ensure their security. This makes the process safe and dependable by guaranteeing that transactions may only be completed by the owner of the private key.
Public key cryptography	Blockchain systems use public key cryptography, which includes techniques such as Elliptic Curve Cryptography (ECC) and RSA. The creation of addresses and key pairs within the blockchain is handled by this cryptographic technique: 1. Address Generation: To create unique addresses on the blockchain, users' public keys undergo a process known as hashing. 2. Secure Communication: Ensuring safe communication and data sharing between users and the nodes that comprise the blockchain network is mostly dependent on public key cryptography.
Zero-knowledge proofs	Zero-knowledge proofs provide an approach to protect privacy without disclosing private information, such as zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge). They make possible two crucial features: Private Transactions: these allow users to prove they possess information, such as a legitimate transaction, without sharing the specifics. They also facilitate confidentiality by permitting smart contracts and private transactions.
Elliptic curve cryptography (ECC)	ECC, or Elliptic Curve Cryptography, stands as a specific form of public key cryptography adopted within blockchain technology for several critical purposes. It is employed to generate digital signatures, validate transactions, and safeguard communications. ECC is highly regarded for its effectiveness, particularly in situations with limited computational resources.
Secured hash algorithm(sha)	SHA, which stands for Secure Hash Algorithm, is a group of special math tools used in the world of digital signatures, transaction checks, and making sure that the blockchain stays safe and sound. People like using SHA in blockchain tech because it's super secure and gets the job done quickly and well.
Advanced encryption standard (AES)	AES, which stands for Advanced Encryption Standard, is a type of encryption method. It is employed in blockchain technology to keep information safe and to safeguard valuable data like private keys and seed phrases. AES ensures that data can be both protected and retrieved securely.
Merkle trees	The security of significant data collection is greatly enhanced using Merkle Trees, a particular type of tree structure. By ensuring that the blockchain is protected from illegal changes and confirming the legitimacy of transactions, blockchain technology is essential.
Multi-signature transections	Multi-signature transactions in blockchain need approval from multiple parties through their digital signatures before any transaction can take place. This extra step enhances security and helps prevent unauthorized or fake transactions.
Ring signature	With ring signatures, a unique type of digital signature, an individual can sign a message on behalf of a group of individuals without revealing who in the group signed it. Ring signatures are essential for maintaining transaction security and protecting anonymity in the blockchain world.

© STM Journals 2024. All Rights Reserved

Table 4. Strengths and vulnerabilities.

Algorithm	Strength	Vulnerabilities
Hash Function	Secures data integrity speeds up calculations, and transforms it irreversibly.	Collision attack prone such that similar inputs give the same hash.
Digital Signature	Maintains the authenticity, irreversibility, as well as the integrity of transactions.	Prone to key compromise attack (KCA) calls for caution in key management.
Public Key Cryptography	It provides secure communication, key exchange, and digital signatures.	Key management difficulties, vulnerability of today's algorithms to quantum attacks.
Zero-Knowledge Proofs	Proves knowledge without compromising the privacy of users and the associated information.	The complexity of implementation, and potential abuse.
Elliptic Curve Cryptography (ECC)	Offers robust security at much smaller key lengths and is well-suited for constrained devices.	Vulnerable to quantum assaults using the Shor algorithm.
Secured Hash Algorithm (SHA)	Commonly used for data integrity verifications since they generate fixed-size hashes.	Collision attacks apply to some scenarios.
Advanced Encryption Standard (AES)	Resistant to known attacks with efficient symmetric key encryption widely used all over the world.	Potential key management problems and possible side-channel adversaries.
Merkle trees	It is an efficient tool for ensuring the integrity of large databases.	Vulnerable to compromise when the fundamental hash function is compromised.
Multi-Signature Transections	Provides increased security through multi-approval transaction requirements.	Uses strong encryption keys, if one key is compromised, then security is jeopardized.
Ring Signature	Providing untraceable anonymity and privacy for transaction senders.	Complex implementation, potential for misuse.

The complex nature of Zero-Knowledge Proofs means that it is an excellent privacy-enhancing tool but needs serious consideration for implementation. Although Elliptic Curve Cryptography is efficient and safe, it is still exposed to quantum threats. The shade-tree Algorithm and Advanced Encryption Standard provide assurances of integrity and security but face problems of collision attacks and complicated key management. Merkle Trees facilitate efficient data verification but depend on the strength of the underlying hashing function. Secure multi-signature transactions based on approval by a group of people require secure key management. To conclude, Ring Signatures have anonymity; however, since they are complex, caution is required during use to prevent abuse and susceptibility. This brief review of these algorithms helps one interpret each of them against their role, strengths, and limitations in cryptography.

Protect and Improvement of Security

Strong cryptographic algorithms play a major role in protecting transaction data in the blockchain and guaranteeing the confidentiality, integrity, and legitimacy of the data transferred throughout the network. The security of transaction data is primarily dependent on cryptography and many other techniques. The foundation for the integrity verification procedure is, first and foremost, the unique, fixed-size representation of transactional data produced by the application of hash functions. Digital signatures play a crucial role in guaranteeing that only authorized parties can begin or approve transactions, validate the origin of the transaction, and offer non-repudiation. By creating secure communication channels, public-key cryptography enables parties to communicate data without running the danger of being intercepted or tampered with. Combining several sophisticated cryptographic algorithms is a common method for strengthening blockchain security through cryptography. Elliptic curve cryptography increases the security of digital signatures and key exchange, while also improving the performance of cryptographic operations. The ZKP provides an additional degree of secrecy by enabling transactions to be verified without disclosing private information. The approval of numerous private keys is necessary for multi-signature transactions, which lowers the possibility of a single point of failure and improves overall security.

© STM Journals 2024. All Rights Reserved

The essential components of blockchain networks and smart contracts also make substantial contributions to security. These self-executing contracts rely on cryptographic principles to operate and are encoded with predetermined rules and conditions. By automating and enforcing agreements, smart contracts lower the possibility of human mistakes and guarantee that transactions occur only when specific conditions are satisfied. Blockchain networks may achieve a better degree of security and trust by integrating cryptographic methods such as digital signatures for authentication within smart contracts. Because the execution and results of smart contracts are verifiable by all network participants, their transparency and immutability provide an extra degree of security. Essentially, the mutually beneficial association between blockchain technology and cryptography creates a strong defense against possible dangers, guaranteeing reliable and safe transfer of transaction information in decentralized networks. By serving as engines for pre-established regulations, smart contracts improve security and support the robustness and integrity of the blockchain ecosystem.

Concrete Examples or Simulations of Cryptographic Algorithms Integrated with Blockchain Systems

Bitcoin's Use of SHA-256

The SHA-256 hashing algorithm is used by Bitcoin to encrypt transactions and build new blocks in its network. The data in each block are hashed, and the next block uses this hash to ensure that no transaction in the chain can be tampered with without causing the sequence to break.

Example Simulation: Every block generated by SHA-256 results in a distinct 256-bit hash (digest). To ensure data integrity, the text field for "Transaction Data" may produce a hash such as {C0535E4B..}.

Ethereum's Use of Keccak-256

Ethereum signs and validates transactions using the Keccak-256 cryptographic hash algorithm. This algorithm, similar to Bitcoin, ensures that every transaction is safely hashed, which adds to the overall integrity of the Ethereum network.

Example Simulation: Cryptographic algorithms provide a hashed output for transactions, such as {D7322956...} in an Ethereum smart contract. Data manipulation is impossible because this hash is irreversible.

Zero-Knowledge Proofs (zk-SNARKs)

Zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) are used in privacy-focused cryptocurrencies like Zcash to validate transactions without disclosing any underlying data (e.g., amount, sender, or receiver). This cryptographic technique preserves security while offering anonymity.

Example Simulation: To ensure privacy and secrecy, zk-SNARKs can be used to demonstrate the legitimacy of a transaction ({A → B}) without disclosing the precise amount transmitted.

Comparison with Recent Tools and Techniques:

Post-Quantum Cryptography

Post-quantum cryptography has surfaced in recent years to defend blockchain systems from quantum computer attacks that have the potential to destroy classic methods, such as RSA and Elliptic Curve Cryptography (ECC). Lattice-based cryptography and multivariate polynomial cryptography are two examples of algorithms under investigation.

Comparison: Most cryptographic algorithms used by current blockchain systems are classical (e.g., SHA-256 and Keccak-256). By creating new algorithms that are immune to quantum computing power, post-quantum cryptography seeks to protect existing systems against potential future quantum assaults.

© STM Journals 2024. All Rights Reserved

Multi-Signature Transactions

Multisignature (Multisig) protocols, which require several keys to authorize a transaction, are being integrated into advanced blockchain systems to improve security. For instance, three of the five authorized parties may need to sign a transaction.

In comparison, multi-signature setups provide increased security by spreading control across several parties, limiting unauthorized access or single-point failures, whereas traditional systems rely on single-key signatures.

Elliptic Curve Cryptography (ECC)

Because ECC can provide the same level of security with lower key sizes as more traditional techniques, such as RSA, it is quickly emerging as the industry standard in cryptography. Ethereum uses transaction signing (ECDSA).

Comparatively speaking, ECC is significantly more effective than RSA in terms of security and processing power, which is why current blockchain systems prefer ECC.

CASE STUDIES

Empirical data and case studies can be used in the following ways:

Case Study on Cryptocurrency Security

Bitcoin or Ethereum is used as a real-world example of blockchain technology and cryptography. For safe transactions, some cryptocurrencies use cryptographic algorithms (such as Bitcoin's SHA-256). Add certain figures, such as:

- Number of daily transactions on the network.
- Reduction in fraud cases due to cryptographic security.
- Hash rate performance as a measure of security robustness.

Number of Daily Transactions

- *Bitcoin:* Between 350,000 and 400,000 transactions are processed every day as of mid-2024. The amount changes according to charge structure, network demand, and market activity.
- *Ethereum:* Because it is used for smart contracts and decentralized apps (dApps), it handles many more transactions. Every day, the Ethereum network processes about a million transactions; during periods of heavy network activity, such as NFT minting or decentralized finance (DeFi) events, this number frequently peaks.

Reduction in Fraud Cases

- Blockchain technology has drastically decreased the likelihood of fraud and double spending by guaranteeing transaction authenticity and immutability with cryptographic algorithms, such as Keccak-256 for Ethereum and SHA-256 for Bitcoin.
- *Fraud Reduction:* Blockchain's dependence on cryptographic hashing has significantly reduced instances of financial fraud, such as double spending and tampering with transaction history. Blockchain cryptography itself is safe from fraud; however, social engineering and exchange-level hacks continue to occur. Because cryptographic security prevents double spending, the fraud rate on Bitcoin is quite low.

Hash Rate Performance as a Measure of Security Robustness

- *Bitcoin Hash Rate:* The amount of processing power required to process transactions and safeguard the network is measured by the hash rate. By 2024, the hash rate of Bitcoin will surpass 350 exahashes per second (EH/s). An increased hash rate makes the network more secure because it makes it more difficult for bad actors to attack or tamper with the blockchain.

© STM Journals 2024. All Rights Reserved

- *Ethereum Hash Rate:* Ethereum's hash rate peaked at over 900 terahashes per second (TH/s) prior to the platform's shift to the Proof of Stake (in 2022, with the release of Ethereum 2.0). Although hashing is no longer a component of Ethereum's consensus process, this hash rate protects the network during the Proof of Work stage.

Supply Chain Transparency

Walmart is a prime illustration of how blockchain technology guarantees accountability and transparency at every level of the food supply chain. Thus, using blockchain in the real world improves food security and safety.

Cutting Down Fraud and Increasing Accountability

- *Fraud Reduction:* A product's entire route from the farm to the shop is tracked using blockchain technology. Because every transaction is permanently recorded on the blockchain, attempts to modify, or fabricate data can be quickly detected. The likelihood of fraud, such as misleading labeling or misrepresentation of the origin of items, is reduced by this degree of openness.
- *Accountability:* Farmers, processors, distributors, and retailers are held responsible for their portion of the process, as is every other business in the supply chain. Information integrity is preserved because cryptographic hashing renders the data unchangeable and impenetrable to tampering. Because suppliers and customers can now believe that the data are real, the trust between them has increased.

Improving Response Time for Product Recalls

- *Food safety:* Blockchain makes it possible to trace items quickly and precisely. For example, in the case of a contamination epidemic (such as E. coli), the entire supply chain can be swiftly tracked back to the source. With blockchain, Walmart has been able to reduce the time it takes to find the provenance of a product from seven days to just 2.2 seconds. Quick action is essential to reduce health hazards and stop the spread of tainted items.

Cryptographic Hashing and Merkle Trees in Action

- *Cryptographic Hashing:* To ensure that data cannot be changed without being discovered, each transaction in the supply chain is hashed using cryptographic techniques. For example, to create a distinct fingerprint of the data, a hash function is applied to the data at every point of the supply chain (harvest, packing, shipping, etc.).
- *Merkle Trees:* These data structures make it possible to verify large datasets quickly and securely. Merkle Trees are employed in Walmart's blockchain to effectively arrange transaction data. This guarantees both security and efficiency because the system can check the integrity of the data without having to search the entire chain, even if only a small portion of the blockchain (such as a particular batch of items) must be verified.

These real-world applications demonstrate how blockchain technology, boosted by cryptographic methods, maintains data integrity in intricate supply networks.

Healthcare Case Study

See the use of blockchain in healthcare data management in programs, such as MediLedger, which monitors supply networks for pharmaceuticals. Encryption protects privacy and security, whereas cryptographic techniques stop unwanted data alteration. You might provide information about the following:

- Decline in illegal drugs.
- Better electronic medical record (EMR) data handling.

Management of the pharmaceutical supply chain and data security in medical records have greatly benefited from the application of blockchain technology in the healthcare industry, especially through resources such as MediLedger. This is an application of a blockchain.

© STM Journals 2024. All Rights Reserved

Reduction in Counterfeit Drugs

- *The Role of Blockchain:* MediLedger assists pharmaceutical businesses in monitoring pharmaceuticals at every stage of the supply chain, guaranteeing that only authentic products are sold. Every drug's path—from producer to distributor to pharmacy to patient—is safely documented using blockchain technology. Because blockchain is unchangeable, tampering is impossible, significantly lowering the possibility of fake medications infiltrating the system.
- *Impact:* Research indicates that between 10 and 30 percent of the medications in underdeveloped nations are fake. Pharmaceutical traceability is now extremely effective owing to blockchain, which has significantly decreased the number of fake medications. Blockchain-based technology from MediLedger has enhanced accountability and transparency, perhaps saved lives and guaranteeing that patients receive authentic medication.

Improved Data Management in Electronic Medical Records (EMRs)

- *Improved Security and Privacy:* Blockchain guarantees that patient data in EMRs are encrypted and only accessed by individuals with proper authorization. Public-key encryption is an example of cryptographic technology used to protect patient data against unwanted access or change. A tamper-proof audit trial is provided by the blockchain's immutable logging of access or alteration.
- *Efficient Data Sharing:* Blockchain decentralizes patient records, enabling healthcare practitioners to safely exchange EMRs among various organizations while protecting patient privacy. This lowers the number of medical history inaccuracies, improves data accessibility in the case of emergencies, and guarantees the security of private medical data. Additionally, it reduces the administrative load associated with upholding and safeguarding consolidated medical records.

MediLedger is an example of how cryptography is used in healthcare because its use of blockchain is revolutionizing the pharmaceutical sector by enhancing medication traceability and healthcare data security.

Non-Fungible Tokens (NFTs)

A major factor in the explosive growth of non-fungible tokens (NFTs) is the ownership and security assurances that the blockchain's cryptographic framework provides. NFTs use blockchain technology in the following manner.

Market Size Growth for NFTs

- *Quick growth:* Over the last several years, the NFT market has experienced exponential growth. The worldwide NFT market is estimated to be worth $41 billion in 2021, making it comparable to the fine art industry. According to predictions, the market size is expected to surpass $80 billion by mid-2024, with NFTs gaining popularity in the domains of virtual real estate, gaming, digital art, and collectibles.
- *Principal drivers:* The capacity to demonstrate digital ownership, the emergence of blockchain-based games (such as Axie Infinity and Decentraland), and the widespread acceptance of NFT by famous people and businesses are key drivers of the NFT adoption boom.

Number of Successful NFT Transactions

- *Volume of transactions:* Sales across many platforms, including OpenSea, Rarible, and Foundation, have reached over $25 billion in 2021, a significant increase in NFT transactions. The number of NFT transactions exceeded $50 billion by 2023, as more buyers and creators joined the ecosystem.
- *Ethereum dominance:* With tens of millions of NFT trades processed yearly, the Ethereum blockchain continues to be the most popular network for NFT transactions. Because they have lower costs and faster transaction times than other blockchain ecosystems such as Solana and Polygon, Layer 2 solutions are becoming increasingly popular as NFT transaction platforms.

© STM Journals 2024. All Rights Reserved

Security Concerns Addressed Through Cryptography

- *Ownership verification:* NFTs use cryptographic hashing to generate distinct tokens that signify digital ownership. Because every NFT is cryptographically connected to a particular asset, the ownership record on the blockchain is unchangeable and verifiable.
- *Preventing counterfeits:* The problem of counterfeit digital assets is addressed by the immutability of blockchain, which guarantees that once an NFT is coined, it cannot be changed or replicated. Every transfer, transaction, and resale are guaranteed to be transparent and safe using cryptographic methods.
- *Private key security:* An NFT owner is identified by its private key. NFT ownership cannot be changed or stolen as long as the private key is safe. Public-key cryptography was utilized to validate transactions and shield NFT holders from fraudulent activity.

The emergence of NFTs is evidence of how the cryptographic foundation of blockchain technology provides safe, open ownership and trade of digital assets. The uniqueness of each NFT is guaranteed by cryptographic procedures, giving buyers and creators peace of mind regarding the legitimacy and safety of their digital assets.

CONCLUSION AND FUTURE WORK

Cryptography is an essential cornerstone that is unmatched in its ability to protect core security goals such as secrecy, integrity, authentication, and non-repudiation. The creation and application of cryptographic algorithms are an effective means of achieving these vital objectives. In the realm of network and data security, cryptography assumes a momentous purpose, bestowing reliability, strength, and resilience on the protection of valuable information. This review paper presents the results of a thorough investigation of the dynamic field of cryptography, providing insight into the functioning of a wide range of algorithms used for different security objectives. The investigation delves into the depth of encryption methods, revealing their potential to protect financial, medical, personal, and e-commerce data while maintaining a respectable degree of anonymity. As we navigate the ever-evolving landscape of IT and business, the significance of cryptography will only burgeon further. With relentless dedication, it will continue to adapt and align itself with the growing demands of an interconnected world, providing steadfast security solutions to the ever-increasing array of digital challenges. In this enduring journey, cryptography remains steady, guarding the sanctity of sensitive information and fortifying the foundations of trust in the digital age.

This demonstrates that the digital encryption technology of the blockchain system is a key component. As this paper clarifies, research on cryptography is essential for the development of blockchain technology and offers a path for further study.

REFERENCES

1. Sharma N, Prabhjot, Kaur H. A review of information security using cryptography technique. Int J Adv Res Comput Sci. 2017;8(Special Issue):323–6.
2. Preneel B. Understanding Cryptography: A Textbook for Students and Practitioners. Berlin: Springer; 2010.
3. Katz J, Lindell Y. Introduction to Modern Cryptography. London: Taylor & Francis Group, LLC; 2008.
4. Khalifa OO, Islam MDR, Khan S, Shebani MS. Communications cryptography. 2004 RF and Microwave Conference (IEEE Cat. No.04EX924), Selangor, Malaysia, 2004, pp. 220-223. DOI: 10.1109/RFM.2004.1411111.
5. Jirwan N, Singh A, Vijay S. Review and analysis of cryptography techniques. Int J Sci Eng Res. 2013;3:1–6.
6. Tayal S, Gupta N, Gupta P, Goyal D, Goyal M. A Review paper on Network Security and Cryptography. Adv Comput Sci Technol. 2017;10:763–70.
7. Gupta A, Walia NK. Cryptography algorithms: a review. Int J Eng Dev Res. 2014;2:1667–72.

© STM Journals 2024. All Rights Reserved

8. Massey JL. Cryptography—A selective survey. Digital Commun. 1986;85:3–25.
9. Fernandez-Carames TM, Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access. 2020;8:21091–116. DOI: 10.1109/ACCESS.2020.2968985.
10. Ferdous MS, Chowdhury MJM, Hoque MA. A survey of consensus algorithms in public blockchain systems for crypto-currencies. J Netw Comput Appl. 2021;182:103035. DOI: 10.1016/j.jnca.2021.103035.
11. Alharby M, van Moorsel A. Blockchain-Based Smart Contracts: A Systematic Mapping Study. Comput Secur. 2019;88:101992.
12. Zhang K, Wang X, Cheng X. Security and Privacy on Blockchain. ACM Comput Surv. 2020;52:1–34.
13. Yaga D, Mell P, Roby N, Scarfone K. Blockchain technology overview. National Institute of Standards and Technology Internal Report. [Preprint]. arXiv preprint arXiv:1906.11078. DOI: 10.48550/arXiv.1906.11078.
14. Aumasson JP. Serious Cryptography: A Practical Introduction to Modern Encryption. San Francisco: No Starch Press, Inc.; 2018.
15. Dooley JF. A Brief History of Cryptology and Cryptographic Algorithms. New York: Springer; 2013.
16. Piper F, Murphy S. Cryptography: A Very Short Introduction. Oxford: Oxford University Press; 2002.
17. Goldreich O. Foundations of Cryptography: Basic Tools. Cambridge: Cambridge University Press; 2004.
18. Gennaro R. Randomness in cryptography. IEEE Secur Priv. 2006;4(2):64–7. DOI: 10.1109/MSP.2006.49.

© STM Journals 2024. All Rights Reserved