The American Journal of Engineering and Technology
ISSN 2689-0984 | Open Access

TYPE Original Research
PAGE NO. 76-87
DOI 10.37547/tajet/Volume07Issue05-06

Check for updates

Cryptographic techniques in blockchain for enhanced digital asset security

Poltavskyi Dmytro
Team lead at Upland.me
Poland, Warsaw

OPEN ACCESS

SUBMITED 22 March 2025
ACCEPTED 27 April 2025
PUBLISHED 12 May 2025
VOLUME Vol.07 Issue 05 2025

CITATION

Poltavskyi Dmytro. (2025). Cryptographic techniques in blockchain for enhanced digital asset security. The American Journal of Engineering and Technology, 7(05), 76–87. https://doi.org/10.37547/tajet/Volume07Issue05-06

Abstract: This article examines the role cryptographic methods play in protecting digital assets through blockchain systems, with a particular focus on their adjustment to contemporary challenges and technological trends. An endeavor is undertaken to systematize major cryptographic algorithms, their effective appraisal in data protection, and development prospects under quantum computing threats. The study is relevant because centralized systems increasingly depend on cryptography due to greater regulatory pressures and, above all, a need for security through secrecy. The scientific novelty lies in the detailed comparative analysis of the said methodology (hashing, digital signatures, zero-knowledge proofs) for cases relating to major blockchain platforms (Bitcoin, Ethereum, Zcash), which hence demonstrate varied approaches towards security provision. The study's methodological foundation consists of analyzing 13 sources, merging a qualitative examination of algorithms and ECDSA with zk-SNARKs with a quantitative assessment of their effectiveness. Hash functions and Merkle trees ensure data integrity while reducing the computational costs of verification; asymmetric cryptography and Zero-Knowledge Proofs guarantee authenticity and confidentiality for the function of the transaction. Main findings support that cryptography is the cornerstone technology for blockchain security, but it has to be tailored to meet new challenges. Development in post-quantum algorithms and the infusion of homomorphic encryption will soon become imperative for quantum threats. This paper strongly advocates hybrid solutions

that would bring traditional ways merged with novelties, which will provide sustainability over time for digital assets. Thus, this article will be useful for Developers of Blockchain Systems, Cryptographers, Cybersecurity Experts, & Regulators willing to know how protection methods for digital assets evolve.

Keywords: blockchain, cryptographic methods, digital assets, data security, hash functions, digital signatures.

Introduction: Blockchain is essentially a decentralized ledger technology through which digital assets such as cryptocurrencies, tokens, and smart contracts can be securely managed [1]. While in the case of traditional centralized systems, data management falls into the hands of one control center, distribution among several nodes will make the system more resilient against both destructive attacks and simple failures in a blockchain-based structure. The new setting eliminates intermediaries and promotes transparency, but may also raise special demands for data protection that cannot generally be satisfied without specialized means. Cryptography will help provide security as well as confidentiality and integrity to the data on a blockchain. It helps address several key issues: integrity can be kept with hash functions like SHA-256 for Bitcoin or Keccak-256 for Ethereum that make any unauthorized modification easily detectable by the network; confidentiality is accomplished through methods like zero-knowledge proofs (e.g. Zk-SNARKs in Zcash, which hide details of transactions; Public cryptography and digital signatures act as authentication and authorization engines that ensure transaction legitimacy without revealing private keys. All these mechanisms put together form the trust base for the technology in its real application mode when centralized control is absent. Cryptography lays the foundation for security in blockchain, and its further evolution is highly desired to secure digital assets in the future. The more blockchain applications expand into fields as crucial as finance and healthcare, the higher the level of security demanded, and new risks are introduced that can potentially break current algorithms, one of them being quantum computing. Quantum-resistant solutions should gradually come into play, and advanced techniques such as homomorphic encryption should be proven to provide support for achieving technological sustainability. Thus, cryptography does not merely play a supporting role for existing functionality within the blockchain, but will dictate its very ability to evolve towards meeting the challenges of tomorrow.

Materials and Methodology

The study of cryptographic methods improving the security of digital assets through blockchain, carried out based on 13 sources, comprising academic papers, technical reports, conference proceedings, and web resources.

The source selection criteria were relevance, scientific importance, and practical application. The databases used for the search are IEEE Xplore, Scopus, and Google Scholar, which give access to peer-reviewed published works.

The search used these keywords: Cryptography in Blockchain, Digital Asset Security, Hash Function, Zero Knowledge Proofs, Post-Quantum Cryptography, Proof of Authority Consensus These were the terms used to try and find articles that cover the main parts of cryptographic security in blockchain systems.

Inclusion criteria for sources were: publications directly related to cryptographic methods for safeguarding digital assets in blockchain systems; articles published within the last 5 years; and materials that have undergone peer review. Works unrelated to the topic and non-peer-reviewed sources were excluded.

The formation of a theoretical basis upon reviews of modern cryptographic technologies such as the work of M. Tarawneh [1], which shall reveal the latest achievements in cryptography; and an upcoming study by A. Marlyn Rose and T. Prabu Vengatesh [12], which shall bring a complete review for the interaction between blockchain and various cryptographic protocols. Technical aspects regarding hash functions were reviewed here with examples SHA-256 [3] and hardware optimization for Keccak [13], to see their roles in block integrity as well as collision resistance. Methodologically, this work fused comparative algorithm analysis with systematic technology review. For example, ECDSA [5] and Zero Knowledge Proof [6] were compared, illustrating their advantages in transaction authentication and privacy protection. The structural usefulness of Merkle Trees [4] was illustrated

in data validation and computational load reduction. D.-S. Kim's work [8] on the Proof-of-Authority-and-Association consensus algorithm gives a basis for energy efficiency comparison with security requirements in IoT networks. A necessary review of quantum threats [10] and legal aspects of GDPR [11] leads to hybrid solutions combining post-quantum cryptography with compliance through regulatory standards. Also, a practice-oriented approach was applied: the case of electronic voting [5], Bitcoin energy consumption analysis [9], demonstrating how cryptographic methods get adapted to specific tasks. Startups in the blockchain industry may find S. Sharma's study [2] revealing barriers against implementing complex protocols. Data from sources [1, 7, 13] confirmed that digital signatures and hash functions, when optimized and hw-implemented respectively, affect the network's speed and reliability. Therefore, combining theoretical analysis with technology comparison and real case evaluation brings a comprehensive understanding of the role of cryptography in protecting digital assets.

Review and Analysis of Cryptographic Methods

Among the several mechanisms through which blockchain technology, or more appropriately, digital assets in a decentralized environment are secured, two major cryptographic methods stand out: hashing and public cryptography. These secure data integrity, authentication, and authorization controls over which central management is abolished in a blockchain system. While hashing guarantees that information cannot be modified, public cryptography ensures secure transmission and verification of transactions. Both guarantee reliable systems that cannot be changed by unauthorized users or attacked successfully [2]. The SHA-256 (Figure 1) function used by Bitcoin and the Keccak-256 (Figure 2) used by Ethereum are examples of hash functions; they convert input data of any length into fixed-length output data called a hash or digital fingerprint. For any given input data, this hash is established; it is also a characteristic that for every tiny variation in input, the output hash changes completely. In a blockchain, every block has the hash of its prior block appended to it, thereby creating a chain of linked blocks. This setup guarantees data integrity since any modification in the content of a block will necessitate the recalculation of hashes for all blocks that follow it; in a decentralized network, this becomes almost impracticable because of the spread-out computing resources. For instance, in Bitcoin, hashing serves double duty, linking blocks and providing distinct transaction identifiers that elevate counterfeiting safeguards.

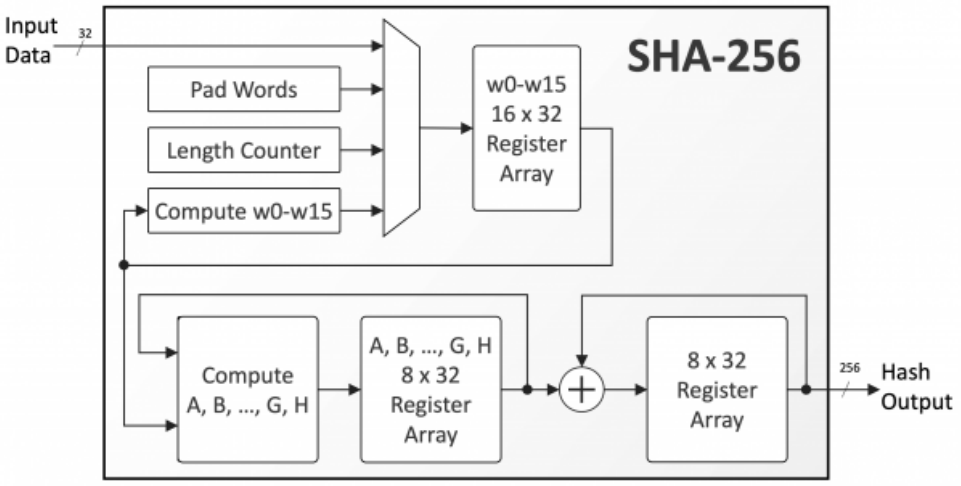

Fig. 1. 256-bit SHA Secure Hash Crypto Engine (compiled by author based on [3])

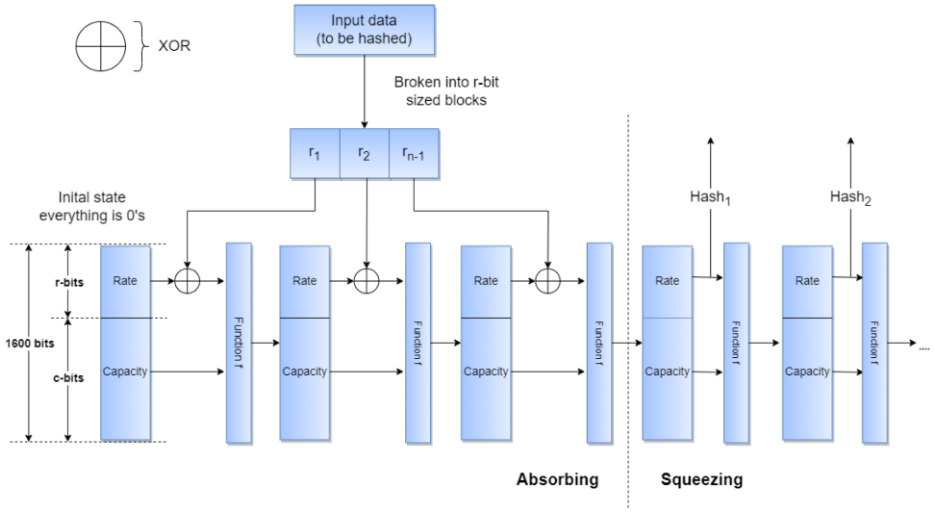

Fig. 2. Sponge construction of the Keccak algorithm [13]

Public cryptography, or asymmetric cryptography, works with a key pair comprising a public key available to all participants of the network and a private key that is known only to its owner. This mechanism in blockchain is used to create digital signatures and verify their authenticity. Whenever a user makes a transaction, it signs the transaction using its private key. The network verifies this signature using the corresponding public key, ensuring that this transaction was indeed authorized by the owner of the private key. In this way, unauthorized access can be mitigated, enabling the safe transfer of digital assets.

Cryptographic techniques include Merkle trees and digital signatures, which are the core of blockchain systems' security with efficient data verification and transaction protection [4]. Merkle trees, a binary data structure known as hash trees, with each leaf node holding a block's data hash, and each internal node created as a hash of the union of its child nodes' hashes. The example below illustrates how this can be compacted to represent a large data set where its root will give an identifier for all the leaves. This algorithm is illustrated in Figure 3. The major usage of Merkle trees within blockchain lies in rendering effective verifications possible for huge datasets; quick checking whether an element is part of a set can be done without going through all the information, thus saving computation time as well as network bandwidth.

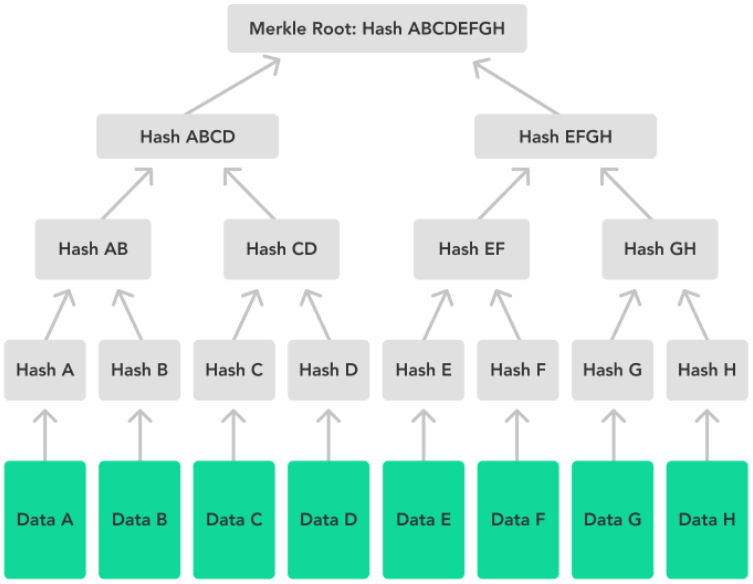

Fig. 3. Merkle Tree with Eight Leaves [4]

In Bitcoin, all transactions of a block are organized into a Merkle tree, and that root is put in the block header. This enables all network nodes, including light clients, to verify whether a specific transaction is included in a block without having to download the full data set, thus greatly speeding up verification time. In Ethereum use of Merkle trees goes beyond just transactions; they are used for storing account states as well as the results of smart contract executions.

Digital signatures will be the largest aspect of authentication and integrity through which the Blockchain operates. Digital signatures are based on public cryptography principles where a private key creates a signature and its corresponding public key allows verification by anyone in the network. Specifically, in Blockchain technology, every transaction has a sender's signature that not only verifies that only the owner of the private key could initiate this operation but also ensures that this transaction data cannot be changed once it is signed. Hence, this setup eliminates any possibility for forgery as well as unauthorized modifications to transactions, so that trust can be placed within a decentralized environment with no central governing body. ECDSA or Elliptic Curve Digital Signature Algorithm is one of the most popularly utilized digital signature algorithms within Blockchain. One of its major utilizations is found within Bitcoin, wherein ECDSA signs and certifies each transaction before its inclusion into a Block [5]. Another algorithm that is gaining popularity is EdDSA, which stands for Edwards-curve Digital Signature Algorithm [2]. This algorithm is widely used in the Cardano blockchain, where it signs transactions reliably with optimized computational costs. Both algorithms illustrate the evolution of cryptographic methods to improve security and performance within blockchain systems.

One of the major components in modern cryptographic techniques is Zero-Knowledge Proofs (ZKPs), which enable one party to convince another of the truth of a statement without revealing any other information[6]. There are many implementations of ZKPs, and among them, zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) and zk-STARKs(Zero-Knowledge Scalable Transparent Arguments of Knowledge) are considered to be the most prominent. The former is compact and very efficient, needing trusted setups for initial parameter generation, while the latter becomes more transparent and resistant to quantum attacks because such setups are not needed. For eexampleSTARKs prove less size-efficient compared to SNARKS proofs. For example, Zcash cryptocurrency uses zk-SNARKs to obscure sender, receiver, and transaction amount data while keeping verifiability possessed by network participants [7].

The fast growth of quantum technologies has caused worries about the safety of existing crypto systems. Quantum computers can solve the factoring problem and the discrete logarithm much more quickly, putting RSA and ECDSA at risk [14]. In answer to this, post-quantum schemes like CRYSTALS-Dilithium and Kyber were based on lattices, though CRYSTALS-Dilithium is seen to produce very small keys and work quickly. Similarly, Kyber, an Ephemeral Diffie-Hellman key exchange mechanism, provides a secure solution for the key exchange when there is a quantum threat. Even though they are theoretically secure, these algorithms are currently under standardization and should be further analyzed from the perspective of practical applicability.

The post-quantum algorithms are slowly being brought into the implementation of existing cryptographic infrastructures. Such systems as SSL/TLS, VPNs, and other security protocols work with RSA and ECDSA, not supporting next-generation algorithms [15]. Inclusion of these new algorithms would require great software as well as hardware changes. This again needs much time and resources to be put into practice, and thus challenges the compatibility with the legacy software and infrastructure. New algorithms further require upgrades in terms of cryptographic hardware, including HSMs and TPMs, thus making their integration into working systems more complex.

Despite the integration difficulties, quantum computing development goes on, with companies like Microsoft achieving success in the race to produce quantum processors. The Microsoft Quantum Development Kit and the Azure Quantum platform are meant for integrating quantum computing within real-life applications, such as cryptography [16]. The focus is on topological qubits, which, in contrast to conventional qubits, are believed to be more stable and have lower probabilities of errors. This greatly fast-

tracks the creation of workable quantum systems with improved computational abilities. Indeed, quantum computers can break existing cryptographic systems; hence, there is a need for post-quantum algorithms.

The stage of post-quantum cryptography is thus best described as transitional at present, with schemes like CRYSTALS-Dilithium and Kyber being strong and sound against quantum attack, though a lot of practical problems are making their lives difficult. Large computational overheads, incompatibility with existing systems, and the need for hardware upgrades are some of the most painful. Nevertheless, the quick change in quantum technologies and the rise of quantum processors illustrate that a change to post-quantum cryptographic methods is more than necessary. This will be the crucial time to advance, as over the next few years, the fast-approaching challenges need to be tackled to ensure data and digital assets in the post-quantum period.

Another significant method is homomorphic encryption. This guarantees that information remains private at all levels of processing, thus making it possible to create private smart contracts [7]. Such contracts can take encrypted input data and produce encrypted output results only accessible to authorized parties. Due to the high computational complexity, algorithms' optimization of algorithms leads to various new opportunities for this method's practical implementation.

Alongside this, distributed multi-signatures and threshold schemes dramatically boost blockchain security by unlocking cryptographic keys. While multi-signatures enable more than one independent signature for transaction authorization, thus drastically minimizing single key exposure risk and adding another layer of resistance against attacks on the system. The halves are keyed into many parts where a predefined minimum them must be gathered to execute an action are known as threshold schemes. These find general usability in enterprise blockchains that serve the purpose of protecting digital assets alongside managing critical operational access. For instance, in asset management systems, threshold schemes lend themselves to the instantiation of flexible organizational security policies.

Consensus algorithms form one more component of blockchain systems, ensuring data consistency in a decentralized environment as another function. Much of the strength behind securing digital assets lies in cryptography [8].

Proof of Work was first introduced in Bitcoin, and it employs hash-based cryptographic problems for validation of blocks. Here, miners competitively engage in solving complex computational puzzles that require input value guessing such that the output hash value meets certain criteria. As long as the network has more than 50% computing power controlled by an attacker, counterfeiting a block will become expensive, hence making a double-spending attack economically unfeasible as well. The problems' cryptographic difficulty level acts as a manipulation barrier, increasing digital assets' security. However, PoW faces serious energy efficiency issues: According to [9], Bitcoin's energy consumption will reach around 175.87 TWh in 2023.

Proof of Stake (PoS) presents an energy-efficient option where the picker of validators is based on the amount of assets frozen rather than computing resources. The cryptography in PoS helps make the random and fair choice of validators using primitives like digital signatures and hash functions, preventing attacks like Nothing-at-Stake in which a validator keeps conflicting branches of the blockchain against it. These ways ensure transaction integrity and boost digital asset security by removing manipulation chances without losing collateral.

Another set of algorithms apart from PoW and PoS is PBFT and DPoS, which leverage cryptography for achieving consensus in distributed systems. While PBFT is a component of private blockchains, it leverages cryptographic signatures to validate messages among nodes. Hence, it proves resilient against Byzantine faults, where up to one-third of the nodes may act maliciously. This method proves safe for digital assets in enterprise circumstances where great reliability is needed. However, the scalability is small because of high-intensity messaging. DPoS allows asset holders to rapidly engage in delegating their validation rights to elected representatives, which introduces additional efficiency into the network. Cryptography ensures that voting cannot be forged by whomsoever and that

delegation cannot be detected, thus enhancing security for assets on public blockchains. Both these algorithms illustrate how the methods of cryptography evolve under different circumstances, yet with one goal: maintaining consensus and safeguarding data.

The key management is the one that assures the safety of digital assets in the blockchain systems. Accessible assets and transaction-authorizing private keys require reliable protection methods. Among them are hardware wallets - physical devices that store keys in an isolated offline environment. These generate and store keys internally, mitigating leakage risk via network attacks. For transacting, the user connects it to a computer, signing it inside the device and sending data to the network, keeping the private key safe. Since phishing and viruses have no access, hardware wallets become trustworthy.

Multi-signature wallets improve security by sharing it with multiple signers. In an “m of n” arrangement, for example, “2 of 3”, where m is the number of required signers and n is the total number of signers, transactions can be authorized only when a sufficient number of signatures are provided. This way, if one key gets compromised, the risk of asset loss is mitigated as well as against fraud, ensuring collective responsibility. They are quite favored in enterprise blockchains and for large asset management. Platforms like Gnosis Safe for Ethereum illustrate how this methodology can work by combining cryptography with distributed control.

Hierarchical deterministic wallets (HD wallets) vastly simplify key management as they generate trees of addresses from a single master seed, which is the BIP32 standard [7]. New keys for each transaction can easily be generated, ensuring that their addresses are not linked to one another, hence providing greater privacy. Backing up just one seed minimizes the risk faced by users regarding loss of access. Current examples, such as Electrum, illustrate how HD wallets combine convenience with security by boosting the protection of digital assets at the user level. In 2025, new challenges and trends facing cryptographic methods in blockchain require adaptation to retain digital asset security; therefore, Post-quantum cryptography becomes imperative because existing algorithms like RSA and ECC will fall under attack by quantum computing [10]. Quantum computers will efficiently solve factorization and the discrete logarithm problem, compromising private keys and thus risking assets. In response, quantum-resistant algorithms are being developed—among them CRYSTALS-Dilithium, a finalist in the NIST Post-Quantum Cryptography (PQC) standardization competition.

The union of artificial intelligence and blockchain brings more opportunities for automating security management and risk controls. AI, strengthening the methods of cryptographic securities, shall analyze transactions in real-time, detecting anomalies and preventing fraud. For instance, machine learning algorithms based on historical data can predict attacks like double spending and also optimize key management. Thus, this merger not only helps in enhancing the security levels of digital assets but also makes the systems more adaptive to the present-day threats because they learn over time.

Regulatory aspects heavily drive the development of cryptographic standards over blockchain. Legislation on digital assets and data protection, like that of the EU GDPR, mandates platforms to have rigorous privacy and security provisions[11]. By 2025, more blockchain systems, including those related to smart contract auditing and key management standards, are likely to come under scrutiny. This will compel developers to again modify the cryptographic techniques due to the changed regulations, which might further impact the algorithm and system architecture choice. In this way, a blend of technical innovation with regulatory change carves out the future landscape for digital asset security, embedding key management within broader global trends and challenges. For instance, Bitcoin uses a hybrid SHA-256 hashing function, ECDSA digital signature algorithm, along with Proof of Work consensus mechanism for its security as one very well-known cryptocurrencies [8]. Unique hashes for both blocks and transactions are achieved using SHA-256, which means data integrity is ensured: any tampering with the information in a block will change its hash, an alteration that will be easily and quickly picked up by the network. ECDSA (Elliptic Curve Digital Signature Algorithm) provides authentication of transactions where users can sign transactions using a private key and verify them with a public key; this ensures no one else can carry out a transaction, thus protecting the asset from theft.

PoW (Proof of Work) requires cryptographic puzzle-solving by miners, thus making it economically impractical to attack the network, for instance, through double spending. Thus, Bitcoin illustrates how simple cryptographic techniques provide security for digital assets over a public blockchain. The other major blockchain technology, initially based on Proof of Work, has now transformed into Proof of Stake with the Ethereum 2.0 launch upgrade, which is a significant move towards energy efficiency and scalability. Bitcoin typically handles 7 TPS, whereas Ethereum, in its current form (Ethereum 1.0), manages about 30 TPS. With Ethereum 2.0's transition to Proof of Stake, it is expected to scale up to 100,000 TPS with sharding [12]. Ethereum uses the Keccak-256 hash function just as Bitcoin uses SHA-256, both ensuring data integrity and uniqueness. The change to PoS in Ethereum's framework modified consensus within this system: instead of being derived from computational work, validators are now based on assets that can be frozen, which reduces energy consumption as well as speeds up transaction processing. The cryptography in PoS ensures random and secure selection of validators using digital signatures and hash functions, thereby preventing such attacks as Nothing-at-Stake, where a validator would maintain multiple branches of the blockchain.

Monero applies advanced cryptography with ring signatures and stealth addresses to make its transactions anonymous. Ring signatures obfuscate the sender's identity by mingling their signature with the signatures of other users; therefore, it becomes impossible to ascertain the actual originator of the transaction. Stealth Addresses will obscure the receiver by creating a unique one-time address for every transaction so that transactions cannot be linked to any particular user. These techniques further increase digital asset privacy, making users untraceable and unanalysable on the blockchain. Monero has applied RandomX, which is ASIC-resistant and ensures decentralization and security across the network.

Another privacy-oriented cryptocurrency is Zcash, which also uses zk-SNARKs to guarantee transaction privacy. Zk-SNARKs stand for Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge, and they enable proving the possession of some information without revealing the information itself; for example, a balance sufficient to cover the transaction. This technology permits obfuscation of sender, receiver, and amount in a transaction while its validity can be checked. In Zcash, users have the option to choose between transparent and private transactions, thus reflecting the flexibility of cryptographic techniques based on the user's needs. The role of zk-SNARKs in Zcash also helps indicate how modern cryptography can enhance digital asset security by providing very high levels of privacy without system integrity loss. The case studies presented here thus indicate some varied roles that cryptographic techniques play within blockchain toward enhancing digital asset security. From simple hash functions and digital signatures in Bitcoin to complex privacy techniques in Monero and Zcash, cryptography is something that every platform tailors to its specific needs. Ethereum's transition to PoS also illustrates how cryptographic methods are changing to meet issues of scalability and energy efficiency. These examples, when viewed collectively, underscore the fact that cryptography lies at the heart of blockchain systems like those mentioned above, guarding digital assets within a decentralized setting. The comparison of different cryptographic methods is presented in Table 1.

Table 1. Comparison of different cryptographic methods (compiled by author based on [6, 7, 8, 10, 11, 12])

Cryptographic Method	Security Level	Computational Costs	Resource Consumption	Privacy Support	Quantum Threat Resistance	Key Trade-offs

Bitcoin (SHA-256, ECDSA, PoW)	High (based on PoW)	High (due to PoW mining)	High (energy-intensive)	Low (public transactions)	Low (vulnerable to quantum attacks)	Performance vs. Security: PoW ensures high security but is energy-hungry and slow. Transparent transactions make it secure but less private.
Ethereum (Keccak-256, ECDSA, PoS)	High (based on PoS)	Moderate (PoS more efficient)	Moderate (energy-efficient)	Medium (public by default, can use privacy-focused techniques)	Low (vulnerable to quantum attacks, transition to PoS increases some resilience)	Performance vs. Privacy: Public transactions by default, but allows privacy solutions like zk-SNARKs. PoS increases energy efficiency while maintaining security.
Monero (Ring Signatures, Stealth Addresses)	Very High (privacy-focused)	High (ring signatures increase complexity)	High (privacy mechanisms add overhead)	Very High (transaction details obfuscated)	Low (vulnerable to quantum attacks)	Performance vs. Privacy: Prioritizes privacy, but this comes at the cost of computational complexity and slower transaction speeds. More resource-intensive.

Zcash (zk-SNARKs)	Very High (privacy-focused, strong encryption)	High (zk-SNARKs are computationally expensive)	High (computational overhead)	Very High (fully anonymous transactions)	Low (vulnerable to quantum attacks, but zk-STARKs offer better post-quantum resistance)	Performance vs. Privacy: zk-SNARKs offer strong privacy, but are computationally expensive, impacting transaction speeds. High security, but less energy efficient.

Each method has its varying degree of security, computational efficiency, resource consumption, and support for privacy when it comes to combating quantum computing threats. This comparison illustrates how different platforms adopt diverse measures to ensure the security and privacy of digital assets as cryptographic techniques continue to evolve due not only to technological advances but also consistent pressure for more rigour from regulatory bodies.

Conclusion

The analysis conducted above proves strong cryptographic methods to be the core of the security systems based on the blockchain, ensuring secure digital assets under decentralization and conditionless trust among participants. The key algorithms include hash functions (SHA-256, Keccak-256), asymmetric cryptography (ECDSA, EdDSA), and data structures (Merkle trees) that provide transaction integrity, authenticity, and immutability. They not only prevent data forgery but also create the trust that is indispensable for working with cryptocurrencies, smart contracts, and decentralized applications. The true power of cryptography comes with illustrating its flexibility in fitting various requirements across different blockchain platforms. For instance, Bitcoin demonstrates basic method reliability, via PoW and ECDSA, in securing a public network; Monero and Zcash apply advanced techniques here for providing anonymity-ring signatures and zk-SNARKs, respectively. Ethereum's switch to PoS illustrates the change of cryptographic methods towards energy efficiency and width without giving up safety. These cases illustrate how cryptography balances openness, secrecy, and function, answering the details of each case.

One of the major threats still is the danger of quantum computing, which can ruin the strength of today's algorithms (RSA, ECC). Making new post-quantum standards like CRYSTALS-Dilithium becomes necessary for keeping assets safe over a long time. At the same time, the part of changes like homomorphic encryption that lets you work with coded data and multi-signatures that share control over assets is getting bigger. Adding AI brings in more chances, like predicting attacks and fixing key management, making proactive protection better.

Key management is critical to the security of any system. Hardware wallets, HD schemes, and threshold signatures help mitigate compromise risks most securely for corporate and regulatory scenarios. On the other hand, increasing pressure from new regulations like GDPR or MiCA pushes platforms against achieving a balance between anonymity and compliance, which eventually influences the choice of cryptographic methods. This means that cryptography for current security on the blockchain also determines its evolution towards future threats. Further development of quantum-resistant algorithms, in combination with AI

and flexible key management, will be a major part in digital asset sustainability. Case studies involving Bitcoin, Ethereum, and Zcash prove that proper utilization of cryptographic methodologies within blockchain architecture can forge dependable, expandable, and private systems that are going to be the bedrock of the digital economy moving forward.

REFERENCES

M. Tarawneh, "Perspective Chapter: Cryptography – Recent Advances and Research Perspectives," in *Biometrics and Cryptography*, BoD – Books on Demand, 2024.

H. Blake, H. Bullock, and N. Chouliara, "Enablers and Barriers to Mental Health Initiatives in Construction SMEs," *Occupational Medicine*, vol. 73, no. 6, Jul. 2023, doi: https://doi.org/10.1093/occmed/kqad075.

K. Raut, "Secure Message Hashing with SHA-256: Cryptographic Implementation," International Journal for Research in Applied Science and Engineering Technology, vol. 12, no. 11, pp. 1288–1294, Nov. 2024, doi: https://doi.org/10.22214/ijraset.2024.65078.

X. Wang *et al.*, "Integrating Merkle Trees with Transformer Networks for Secure Financial Computation," *Applied sciences*, vol. 14, no. 4, pp. 1386–1386, Feb. 2024, doi: https://doi.org/10.3390/app14041386.

C. Shekhar and R. K. Yadav, "An innovative and secured electronic voting system based on Elliptic Curve Signing Approach (ECDSA) and digital signatures," *International Journal of Information Technology*, Mar. 2025, doi: https://doi.org/10.1007/s41870-025-02405-3.

I. Aad, "Zero-Knowledge Proof," in *Trends in Data Protection and Encryption Technologies*, Springer, 2023.

G. Chen, "Optimizing Digital Signatures for Enhanced Privacy Protection in Blockchain Systems," *Applied and Computational Engineering*, vol. 110, no. 1, pp. 96–101, Nov. 2024, doi: https://doi.org/10.54254/2755-2721/110/2024melb0105.

D.-S. Kim, I. S. Igboanusi, L. A. Chijioke Ahakonye, and G. O. Anyanwu, "Proof-of-Authority-and-Association Consensus Algorithm for IoT Blockchain Networks," in *2025 IEEE International Conference on Consumer Electronics (ICCE)*, IEEE, Jan. 2025. doi: https://doi.org/10.1109/icce63647.2025.10930052.

"Bitcoin Energy Consumption Index - Digiconomist," *Digiconomist*, 2024. https://digiconomist.net/bitcoin-energy-consumption (accessed Mar. 21, 2025).

C. Gilbert and M. Gilbert, "Investigating the Challenges and Solutions in Cybersecurity Using Quantum Computing and Cryptography," *International Research Journal of Advanced Engineering and Science*, vol. 9, no. 4, pp. 291–315, Dec. 2024.

K. Paruchuru, Aneeshkumar Perukilakattunirappel Sundareswaran, and Akshun Chhapola, "The Impact of Data Privacy Laws, such as GDPR, on the Design and Operation of WMS," *International Journal of Research in Modern Engineering and Emerging Technology*, vol. 13, no. 3, pp. 183–203, Mar. 2025, doi: https://doi.org/10.63345/ijrmeet.org.v13.i3.11.

A. Marlyn Rose and T. Prabu Vengatesh, "Understanding Cryptocurrency and Blockchain Technology: a Comprehensive Overview," in *The International Conference on Fintech: Digital Transformation of Financial Services-ICF2023*, Sep. 2023.

A. Sideris, T. Sanida, and M. Dasygenis, "A Novel Hardware Architecture for Enhancing the Keccak Hash Function in FPGA Devices," *MDPI Information*, vol. 14, no. 9, p. 475, Sep. 2023, doi: https://doi.org/10.3390/info14090475.

H. Syed, A. Paul, M. Singh, and M. Rajan, "An Efficient Two-Party ECDSA Scheme for Cryptocurrencies," *Lecture notes in computer science*, pp. 411–430, Jan. 2023, doi: https://doi.org/10.1007/978-3-031-49099-6_25.

P. Jaya, None Sawaluddin, and Elviawaty Muiza Zamzami, "Comparison of ECDHE-ECDSA and ECDHE-RSA on SSL/TSL," in *2023 IEEE 7th International Conference on Information Technology, Information Systems and Electrical Engineering*, Nov. 2023. doi: https://doi.org/10.1109/icitisee58992.2023.10404441.

Mariia Mykhailova, "Teaching Quantum Computing Using Microsoft Quantum Development Kit and Azure

Quantum," in *2023 IEEE International Conference on Quantum Computing and Engineering (QCE)*, Sep. 2023. doi: https://doi.org/10.1109/qce57702.2023.20320.