Proceedings of the 3rd International Conference on Computing Innovation and Applied Physics
DOI: 10.54254/2753-8818/31/20240862

# Blockchain security and applications: A comprehensive analysis from hash functions to consensus algorithms

**Xuyang Wang**

Beijing Chaoyang Tongwen Foreign Language School, Beijing, 100020, China

631501010113@mails.cqjtu.edu.cn

**Abstract.** This article delves into the inherent security of blockchain technology by evaluating the sophisticated techniques it employs. Key among these are mathematical hash functions, elliptic curve cryptography, and zero-knowledge proofs. Mathematical hash functions ensure that data stored is immutable; any slight alteration to the information will lead to a drastically different hash output, making any tampering evident. Elliptic curve cryptography provides a robust encryption mechanism, ensuring that data transactions remain confidential and secure. Meanwhile, zero-knowledge proofs enable one party to prove to another that they possess specific knowledge without revealing the actual information, further bolstering privacy. Owing to these technological underpinnings, blockchain not only excels in safeguarding sensitive data but also facilitates operations like verifying information authenticity. Moreover, in sectors like supply chain management, it offers capabilities for precise logistics positioning and traceability. Such applications underline blockchain's potential as a tool for transparency and security in various industries. Through these features and mechanisms, blockchain stands as an exemplar of digital security in today's interconnected era.

**Keywords:** Hash function, Zero-knowledge, Proof, decentralization, Consensus Algorithm.

## 1. Introduction

Blockchain technology holds immense potential in safeguarding the legitimate rights and interests of traders. One of its defining features is the immutable nature of its data blocks, making unauthorized deletion or alteration virtually impossible. This characteristic stands as a formidable barrier against fraudulent market practices and promises a transparent and trustworthy system. Delving into the mechanism of blockchain provides insights into its intricate structure. At its core, a blockchain is a decentralized ledger of all transactions across a network. Once a transaction is added, it becomes a permanent record, ensuring transparency and traceability. This decentralized nature ensures that no single entity has control over the entire blockchain, which reduces the chances of manipulation or central point of failure. Furthermore, blockchain technology can revolutionize various industries by enhancing efficiency and problem-solving capabilities. For instance, in supply chain management, blockchain can offer real-time tracking and authentication of goods, reducing fraud and counterfeiting. Similarly, in the financial sector, instantaneous and transparent transactions can minimize delays and costs associated with intermediaries.

DOI: 10.54254/2753-8818/31/20240862

## 2. Relevant Theories

### *2.1. Definition of Blockchain*

Before its official formation, the concept of the blockchain was explored and experimented with by several scientists. In 1992, Eric Hughes developed and operated the Crypto Anonymous List Server. Its initial version merely obscured the sender's address and was vulnerable to single points of failure and potential malicious intervention by administrators [1]. By 1997, it evolved into the Cypherpunk's Distributed Remailer (CDR). This system utilized a multi-node list server in which nodes would replicate one another upon the receipt of new mail. This design ensured mail couldn't be lost due to the failure of individual nodes or malicious actions. In many ways, this system bore resemblances to the functioning of Bitcoin. In the same year, Haber and Stornetta introduced a protocol aimed at safeguarding digital files via timestamping. This system articulated the sequence of file creation using timestamps, and it was pivotal that these timestamps remained immutable post-creation [2]. This ensured that the associated file was protected against tampering. Early ventures into blockchain technology for virtual currencies were predominantly centralized. Consequently, as the companies championing these currencies faltered, the technological structures underpinning them also crumbled. It was Satoshi Nakamoto who introduced critical improvements, culminating in the invention of Bitcoin [3]. The blockchain landscape further transformed with the introduction of "Ethereum: the Next Generation of Smart Contracts and Decentralized Application Platforms" by a young Russian named Vitalik Buterin. His work ushered in the era of Blockchain 2.0, addressing concerns that the Bitcoin blockchain was relatively non-scalable and restricted to recording transactions exclusively [4]. With this innovation, blockchain technology found applications in an even broader array of fields.

### *2.2. Composition of blockchain system*

Lockchain systems are typically understood through six primary components: Data Layer: This is a distributed database characterized by its immutable properties. It holds all essential data information on the blockchain, encompassing hash values, timestamps, metadata orders [5], and both public and private keys. Thanks to asymmetric encryption and cryptographic hash algorithms, the data layer ensures the data's non-alterability and traceability. To guarantee consistency, the nodes of the blockchain deploy consensus algorithms, making sure the information in the data layer remains coherent. Network Layer: This layer facilitates the dissemination and exchange of data and information across the blockchain network. Consensus Layer: Often described as the backbone of governance in the blockchain system, the consensus layer [6] predominantly comprises consensus algorithm mechanisms, ensuring all nodes agree on a single version of the truth. Smart Contracts: These are self-executing contracts with the terms of agreement between parties directly written into lines of code. By embedding these codes into the system and establishing parameters, smart contracts allow for real-time operability. Application Layer: This pertains to the various applications and utilities developed on the blockchain. It represents how users and developers interact with the blockchain system, enabling them to harness its potential for various use cases. Incentive Layer: Often associated with mining incentives in the blockchain world, this layer offers rewards to miners for verifying transaction data. In doing so, it motivates continuous activity and the timely updating of the blockchain ledger. Additionally, the incentive layer can be equipped with mechanisms to penalize malicious nodes, ensuring the system's security and integrity.

### *2.3. Analyzing the core technology of blockchain*

*2.3.1. SHA-256 hash function algorithm.* Because hash functions are irreversible, attempting to reverse-engineer the output to retrieve the original input is futile, ensuring that the encrypted content remains secure from decryption by unauthorized parties. The SHA-256 algorithm is widely adopted in blockchain for encrypting blocks. The procedure begins by dividing the new dataset 'X' into 'n' blocks, each having a length of 512 [7]. Subsequently, each 512-length block is partitioned into 16 words, each 32 units long. In the following phase, the 17th word is derived from these initial 16 using a specific

DOI: 10.54254/2753-8818/31/20240862

mathematical formula. Likewise, the 18th word is produced based on prior words, continuing this pattern until the 64th word is generated. The fundamental principle is that for every unique input, there's a corresponding unique hash output. Thus, it's highly improbable for two distinct data blocks to yield the same hash value. Hash pointers link these values sequentially, giving rise to the blockchain structure. Should the data of any block be altered, its associated hash pointer becomes invalid. Subsequent blocks won't match the hash pointer of the tampered block, ensuring swift and accurate detection of any anomalies.

*2.3.2. Asymmetric Encryption Algorithm - ECC Encryption Algorithm.* The encryption technique used in blockchain is asymmetric encryption, which uses a "key pair" containing a public key and a key to decrypt the data. Among the asymmetric encryption algorithms [8], Elliptic Curve Cryptography, or ECC, is used to protect private data. For decryption, the Elliptic Curve Discrete Logarithm is used. The mathematical formula for Elliptic Curve Cryptography is Q=kP,where the point P is called the base point,k is the private key(K is an integer), and Q is the public key(Q is a point on the elliptic curve). given P and Q, it is very difficult to exhaustively find k. Further explanation is that the elliptic curve formula: quadratic of Y = the third power of X + aX + b function, the relationship between a and b exists such that the third power of 4a plus 27 times the second power of b does not equal 0.This qualification guarantees that the curve does not contain singularities, meaning that tangents exist at any point in the curve.It does not use the law of addition when performing addition operations, as exemplified by the elliptic curve in the figure 1 [9].

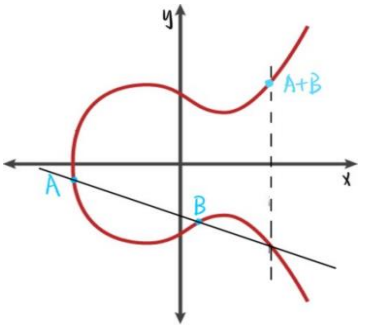


**Figure 1.** A + B calculation process (Photo/Picture credit: Original).

The second case is the calculation of A + A, you need to make a tangent line through the point A, this line and the elliptic curve to form an intersection [10], over the intersection point to make a straight line parallel to the Y-axis to intersect the curve at the point 2A, this point is the result of A + A (Figure 2).

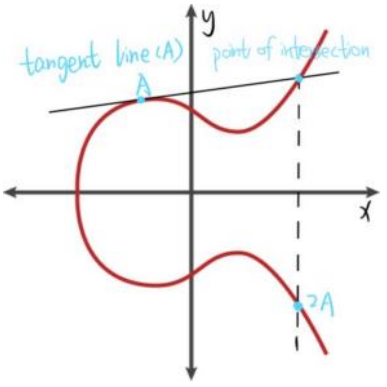


**Figure 2.** Calculation process of A+A (Photo/Picture credit: Original).

The process of accumulating these points is the process of multiplication between points.
Figure 3 shows the process of calculating 3A, which is the same elliptic curve addition pattern.

DOI: 10.54254/2753-8818/31/20240862

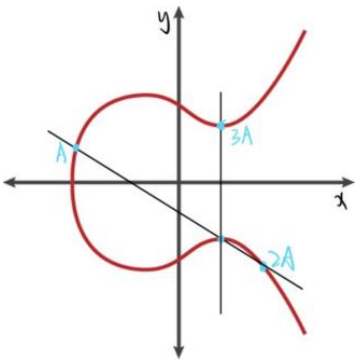


**Figure 3.** Calculation process of dot product (Photo/Picture credit: Original).

From the above three graphs, it can be noticed that the points in the computation are scattered all over the curve with no regularity. As the multiplicity of points to be calculated increases, the problem faced by the decryption will become more and more difficult. In the equation Q=kP, Q can be regarded as 3A, P can be regarded as A, and k is the coefficient of A. This is the root of the security of elliptic curve encryption algorithm. k is used as the private key. The encryption process of this technique is divided into four steps. In the first step, an elliptic curve Ep (a, b) is selected and a point on the elliptic curve is taken as the base point P. In the second step, a large number k is selected as the private key and the public key Q=kP is generated. in the third step, a random number r is selected and the message M is generated as the ciphertext C, the ciphertext is a point pair that is C= (rP, M+rQ). Here the random number is multiplied by P and the message and the value rQ are connected together to form a point pair to be passed to the decryptor.

*2.3.3. Zero Knowledge Proof.* Zero-knowledge proof is one of the important technical tools to protect blockchain privacy. The unique three properties of zero-knowledge proof are the key to protect blockchain privacy. In the famous three coloring problem. The first property is completeness, which means that the prover cannot deceive the verifier, what is true can't be false. If honest Alice has a If honest Alice has a definite coloring scheme, it will be 100% verified by honest Bob anyway. verified by honest Bob anyway. The second property is Soundness, which means that the verifier cannot deceive the prover. Alice will replace the colors again in a few rounds, and then cover all the nodes with envelopes. Bob picks another edge, and asks Alice to remove the envelopes to see what it looks Bob picks another edge, and asks Alice to remove the envelopes. Bob picks another edge, and asks Alice to remove the envelopes to see what it looks like, and if bob finds that the nodes at the ends of this edge are different colors and if bob finds that the nodes at the ends of this edge are different colors again, then bob is a little bit believing, and Bob wants to verify. Supposing that after n rounds, the probability of Alice cheating decreases so much that, if n is large enough, the cheating event is recognized as not occurring in statistics. The third property is Zero-knowledge, which means that the verifier does not have access to any additional knowledge, that the distribution of the partial coloring that Bob sees each time is the result of Alice's changes, and that no matter how many times Bob looks at it, he does not get a three-color answer. In fact, although Bob only gains a lot of information in the process, gaining this information does not allow Bob to compute In fact, although Bob only gains a lot of information in the process, gaining this information does not allow Bob to compute more results, (or the information is something that Bob would have been able to compute on his own) he does not gain any real knowledge.

*2.3.4. Decentralization.* The role of decentralization technology is to make the content of the blockchain load will not be dominated by one center, its central power is dispersed to multiple nodes with the same power, they exchange to verify the data with each other, so as to ensure that the information will not be switched. Decentralized technology features a blockchain that is maintained and managed by multiple nodes, which not only improves transparency but also reduces the risk of data being altered. Because

DOI: 10.54254/2753-8818/31/20240862

the data in the blockchain is distributed on different nodes without a centralized control body, this also avoids the problem of a single point of failure. That is, if one node has a problem, other nodes can still continue to operate.

*2.3.5. Consensus Algorithm – PoW.* Each node in the blockchain owns a complete copy of the ledger, and any changes to the information on the ledger need to be verified by consensus to ensure the consistency and reliability of the data. Bookkeeping in the blockchain is achieved through a consensus mechanism, and only transactions agreed upon by all nodes through an algorithm are recorded on the blockchain. Therefore there is no need for everyone to record every transaction. The bookkeepers in the blockchain are also known as miners, they will compete to get the bookkeeping rights, when they get the bookkeeping rights they need to complete certain computational tasks in order to complete the bookkeeping, this process is known as mining. Proof of workload is what works using a consensus algorithm, abbreviated as PoW. in PoW, different nodes compete with each other based on specific information, and ultimately have to prioritize proving that some computation is right, such as calculating the solution to an extremely difficult math problem, so that the next block can be created and be rewarded with virtual coins in the system. Upon validating the transactions in that block, this computed result is synchronized to each individual's current record. This triggers a healthy competition among the nodes, prompting them to solve the problem quickly and accurately. The consensus algorithm is also resistant to aggression. If miners misbehave on the proof-of-work mechanism, they will not be able to attempt to add new blocks. Attacks on this system also require a lot of money and computing power. For example, to create fraudulent transactions in this system of the blockchain, you need to control 51% of the network capacity. What's more, during the mining process, bookkeepers need to follow certain rules or else they will be rejected by other nodes and thus will not be rewarded. The reward mechanism controls the miners to a certain extent.

## 3. System Analysis and Application Research

### *3.1. Supply Chain Applications*

Enhancing inventory management is crucial for businesses to remain efficient and competitive. One key way to achieve this is by minimizing the time products spend in transit and shipping. Doing so not only helps in ensuring that goods arrive promptly to their intended destinations but also significantly reduces waste and associated costs. In the era of digital advancement, many businesses are adopting technologies that allow them to monitor the journey of their shipments in real-time. Through advanced tracking systems, they can instantly access crucial data like the status of customs documents or detailed cargo information sheets. Such transparency provides companies with an unprecedented level of control and oversight, enabling them to ensure that their products are handled correctly and delivered on time. Moreover, in scenarios where shipments go missing – an unfortunate reality for many businesses – these tools come to the rescue. Instead of grappling with uncertainty, lengthy wait times, or costly investigations, companies can swiftly pinpoint the exact location of the missing shipment. This rapid response not only mitigates potential financial losses but also enhances customer trust. When clients know that a business can handle discrepancies with such efficiency, they're more likely to maintain their loyalty and trust in that brand.

### *3.2. Agricultural Economy: "Step by Step Chicken" Program Launched by Zong'an Technology*

In 2017, Zhongan Technology announced the first domestic application of blockchain to the chicken industry, supporting domestic blockchain startup Lianmuo Technology to launch the "BBQ Chicken" project, which can provide consumers with more trustworthy food. The BBQ chicken farming industry integrates anti-counterfeiting technologies such as Internet of Things, blockchain and artificial intelligence, and each chicken wears a chicken tag, which is their Internet of Things ID card. Chicken tags are not replicable, one chicken, one tag, disassembly and destruction. Based on the blockchain is not tamperable, IoT devices automatically collect and other characteristics. This method of growing

DOI: 10.54254/2753-8818/31/20240862

chickens can accurately track each bird's development, allowing for traceability and the maximum amount of protection against dishonest dealers' counterfeiting. Every step of the process is documented on a safe blockchain database, which can guarantee the quality of chickens. Increased consumer trust and sales are made possible by this action. Blockchain's immutable records may significantly reduce information asymmetry, enhance the transparency of the whole industrial supply chain, and realize the value-added of the entire sector. As a result, blockchain technology is gaining popularity in the agriculture industry, where it offers limitless potential for the growth of agricultural production.

## 4. Challenges and problems

### *4.1. Storage and scalability issues*

As each node needs to verify and store a copy of the entire blockchain, the storage capacity of blockchain technology skyrockets as the number of problems solved by the blockchain increases. If one wants to keep applying the current blockchain technology, one needs infinitely more storage space to solve the problem. While applying the blockchain technology may face network congestion and the waiting time to deal with the problem will become longer.

### *4.2. Pollution to the environment*

Blockchain technology will have extremely high network energy consumption when applied. As the technology grows and more people get involved, the use of energy is increasing at a crazy rate. People are now working on more environmentally friendly proof of entitlement, but the technology is still immature.

### *4.3. Generating Fraud*

Blockchain technology has a strong ability to protect the privacy of the users, which can be exploited by unscrupulous people who use this feature for black market transactions. If the black market is not detected and banned in time, the non-compliant items will affect countless people, which will create an extremely strong security risk. Scams and other behaviors will also creep in with the help of blockchain technology.

## 5. Conclusion

Blockchain technology offers robust security through advanced encryption algorithms and cryptographic privacy schemes. In a digital world rife with uncertainty and cyber threats, this technology provides a beacon of trust. Its immutable nature ensures data integrity, leading to heightened efficiency in business operations and increased consumer confidence. The benefits trickle down to increased profitability for businesses.

From agriculture and medicine to finance, real estate, and education, blockchain is forging authentic connections and fostering trust between parties. This facilitates efficient and secure problem-solving across sectors. The horizons of its applications are expanding, and as the technology refines and advances, its potential advantages for humanity are boundless.

Given its immense promise, there's a pressing need to amplify focus on blockchain and raise its profile among the general populace. Accelerating its maturity will undoubtedly usher in benefits for a broader human audience. However, as an emergent technology, it has its share of teething problems. Many processes remain unrefined, and its nascent status can be a double-edged sword. While its promise is undeniable, so is its potential for misuse in the hands of the uninformed or malicious actors. For this reason, enhancing public understanding of blockchain is crucial. This not only aids in harnessing its advantages but also in safeguarding against deception due to its misinterpretation. Organizations venturing into the blockchain arena must be vigilant about its known technical limitations and vulnerabilities. A dedicated focus on studying its inherent weaknesses and devising appropriate countermeasures is imperative for leveraging its full potential in various professional arenas.

DOI: 10.54254/2753-8818/31/20240862

## References

[1] Portmann, E. (2018). Rezension „Blockchain: Blueprint for a New Economy" HMD Praxis Der Wirtschaftsinformatik, 55(6), 1362–1364. https://doi.org/10.1365/s40702-018-00468-4.

[2] Cocco, L., Pinna, A., & Marchesi, M. (2017). Banking on Blockchain: Costs Savings Thanks to the Blockchain Technology. Future Internet, 9(3), 25. https://doi.org/10.3390/fi9030025

[3] Challenges Potential and Future of Internet of Things Integrated with Blockchain. (2019). International Journal of Recent Technology and Engineering, 8(2S7), 530–536. https://doi. org/ 10.35940/ijrte.b1099.0782s719

[4] Rejeb, A., Keogh, J. G., & Treiblmaier, H. (2019). Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management. Future Internet, 11(7), 161. https:// doi.org/10.3390/fi11070161.

[5] Martino, R., & Cilardo, A. (2020). Designing a SHA-256 Processor for Blockchain-based IoT Applications. *Internet of Things*, 100254. https://doi.org/10.1016/j.iot.2020.100254.

[6] Goldreich, O., & Oren, Y. (1994). Definitions and properties of zero-knowledge proof systems. Journal of Cryptology, 7(1). https://doi.org/10.1007/bf00195207.

[7] Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. ACM Computing Surveys, 52(3), 1–34. https://doi.org/10.1145/3316481.

[8] Chum, C. S., & Zhang, X. (2012). Hash function-based secret sharing scheme designs. Security and Communication Networks, 6(5), 584–592. https://doi.org/10.1002/sec.576.

[9] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 100(1), 143–174. https://doi. org/ 10. 1016/j.rser.2018.10.014.

[10] Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2020). Addressing security and privacy issues of IoT using blockchain technology. IEEE Internet of Things Journal, 8(2), 881-888.