ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 03,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

BLOCKCHAIN TECHNOLOGY AND THE ROLE OF THE SHA-256 ALGORITHM

Sadullayeva Shahrizoda

Master's student, 1st year, Samarkand State University,

sadullayevashahrizoda@gmail.com

ABSTRACT: This article analyzes the SHA-256 cryptographic hash algorithm used in modern blockchain systems. The mathematical foundations of the algorithm, its application in blockchain, security aspects, and stability under computational threats are examined. The study highlights that the security of blockchain technology is of paramount importance today and that using the SHA-256 algorithm is effective for ensuring this security. The findings indicate that the SHA-256 hash algorithm meets the reliability and security requirements of blockchain systems.

KEYWORDS: Blockchain, SHA-256, cryptography, hash function, Bitcoin, mining, security.

АННОТАЦИЯ: В статье проведен анализ криптографического алгоритма хеширования SHA-256, который активно применяется в современных блокчейн-системах. Изучены математические принципы работы алгоритма, его роль в обеспечении безопасности блокчейна, а также устойчивость к потенциальным вычислительным атакам. Исследование подтверждает, что SHA-256 остается надежным стандартом для защиты данных в распределенных реестрах, несмотря на растущие требования к криптостойкости. Результаты демонстрируют соответствие алгоритма ключевым критериям безопасности, включая устойчивость к коллизиям и эффективность вычислительных процессов в сети.

КЛЮЧЕВЫЕ СЛОВА: блокчейн, SHA-256, криптография, хеш-функция, Биткойн, майнинг, кибербезопасность.

ANNOTATSIYA: Maqolada zamonaviy blockchain tizimlarida qo‘llaniladigan SHA-256 kriptografik hash algoritmi tahlil qilinadi. Algoritmning matematik asoslari, blockchainda qo‘llanilishi, xavfsizlik jihatlari va hisoblash tahdidlari ostidagi barqarorligi o‘rganilgan. Tadqiqotda blockchain texnologiyasining xavfsizligi hozirgi kunda muhim ekanligi va bu xavfsizlikni ta`minlash uchun SHA-256 algoritmidan foydalanish qulay ekanligi aniqlangan. Natijalar shuni ko‘rsatadiki, SHA-256 hash algoritmi blockchainning ishonchlilik va xavfsizlik talablariga javob bera oladi.

KALIT SO`ZLAR: Blockchain, SHA-256, kriptografiya, hash funksiya, Bitcoin, mining, xavfsizlik.

1. INTRODUCTION

In the modern digital world, the secure transmission and storage of data is one of the most critical issues. Blockchain technology is an innovative solution developed to address these challenges, providing a decentralized, transparent, and immutable database system. This technology was first introduced in 2008 by Satoshi Nakamoto for Bitcoin cryptocurrency, and today, it is widely used in finance, healthcare, education, and many other sectors.

The reliability and security of blockchain systems are based on cryptographic algorithms, particularly hash functions such as SHA-256 (Secure Hash Algorithm 256-bit). The SHA-256 algorithm plays a crucial role in data protection, transaction validation, and consensus mechanisms.

The primary objective of this paper is to explore the role of the SHA-256 algorithm in blockchain systems, analyzing its advantages and disadvantages. To achieve this, we will examine the mathematical foundations of the SHA-256 algorithm, study its application in blockchain, and assess its security aspects.

1. BLOCKCHAIN TECHNOLOGY: FUNDAMENTAL PRINCIPLES OF BLOCKCHAIN

Blockchain technology is based on the principles of decentralization, transparency, immutability, and consensus mechanisms [1].

Decentralization – In blockchain technology, there is no single central authority, meaning that no single entity controls the process. This enhances security by eliminating a central point of failure.

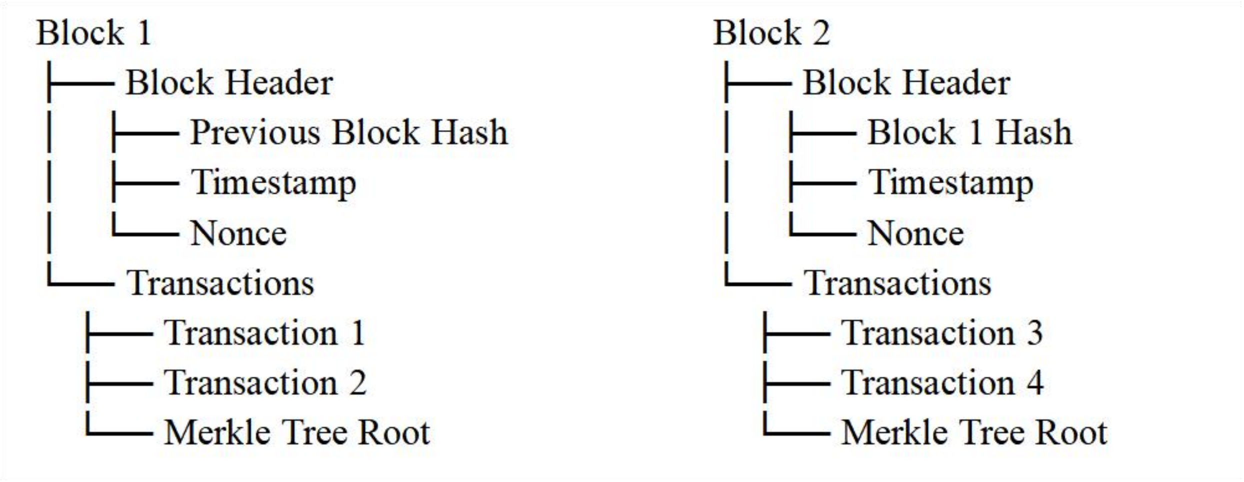
Transparency – All transactions in the blockchain are openly visible. Transparency ensures that all completed actions are stored in a structured manner and can only be viewed by authenticated users. Users can access this open information whenever needed.

Immutability – Once data is entered into the blockchain, it cannot be altered. This principle enhances security by ensuring that no unauthorized person can modify the data without the owner's authentication or identity verification.

Consensus Mechanisms – Blockchain operates based on consensus mechanisms such as Proof-of-Work (PoW) and Proof-of-Stake (PoS). These mechanisms determine how transactions are validated and play a role in energy efficiency considerations.

SCHEMATIC REPRESENTATION OF BLOCKCHAIN STRUCTURE

{User A} → {Creates a transaction} → {Sent to the network}
↓
{Miners} → {Verify transactions} → {Add to a block}
↓
{Added to the blockchain} → {All nodes are updated}



```
Block 1                                  Block 2
├── Block Header                         ├── Block Header
│   ├── Previous Block Hash              │   ├── Block 1 Hash
│   ├── Timestamp                        │   ├── Timestamp
│   └── Nonce                            │   └── Nonce
└── Transactions                         └── Transactions
    ├── Transaction 1                        ├── Transaction 3
    ├── Transaction 2                        ├── Transaction 4
    └── Merkle Tree Root                     └── Merkle Tree Root
```

As seen in this schema, each block contains the hash value of the previous block, ensuring the integrity of the chain. The SHA-256 algorithm is used to compute these hash values.

2. CLASSIFICATION OF THE SHA-256 ALGORITHM

The SHA-256 algorithm is part of the SHA-2 family of functions and processes data through several structured stages. Below is a detailed explanation of the evolution of the SHA-256 algorithm, its working principle, functions in the message processing stage, and the finalization process [2].

The SHA-256 process is executed as follows: The algorithm starts with eight initial hash values, derived from the decimal fractions of the square roots of the first 64 prime numbers. Each hash value is 32 bits long.

SHA-256 also defines 64 constant values, obtained from the decimal fractions of the cube roots of the first 64 prime numbers, which are used in the compression function.

To ensure that the input message length leaves a remainder of 448 when divided by 512, padding is added: A ‘1’ bit is appended to the original message. Followed by ‘0’ bits until the message length reaches 448. Finally, the original message length is appended as a 64-bit integer, forming a 512-bit message block.

The padded message is then divided into 512-bit blocks, each processed independently. The processing and compression steps are similar to those in the SHA-224 algorithm.

After 64 iterations for each block, the computed intermediate hash values are added to the initial hash values. Once all message blocks are processed, the final hash value is obtained by concatenating H[0] to H[7], producing a 256-bit (32-byte) hash output.

Comparison of SHA-256 and Other Hash Algorithms:

Parameter	SHA-256	SHA-3	Scrypt
Hash length	256 bits	256-512 bits	Variable
Speed(CPU)	High	Medium	Low
Energy consumption	High (PoW)	Low	Medium
Duribality	Low($2^{128}\rightarrow 2^{64}$)	High	High

4. RESEARCH RESULTS AND DISCUSSION

Bitcoin and Proof-of-Work (PoW) Systems – SHA-256 is used to solve mathematical problems in the mining process [3]. Merkle Tree Structure – Transactions within each block are encrypted using SHA-256.

SHA-256 Algorithm Workflow: **Input (Data) → Padding → Message Schedule → Compression Function → Hash (64 characters)**

Collision Resistance – Requires 2^{128} operations (practically impossible for current computers), meaning the probability of two hashes colliding is extremely low.

Potential Threats – Grover's algorithm could theoretically reduce SHA-256 security from 2^{128} to 2^{64}, posing a future risk [4].

Advantages consists of fast and reliable hash generation and proven and tested in large networks like Bitcoin. Disadvantages consists of only high energy consumption (in PoW systems).

Scalability Challenges is the high computational power required for SHA-256-based mining makes it less efficient for large-scale adoption in certain applications.

Adoption in Various Industries - Beyond cryptocurrencies, SHA-256 is used in digital signatures, data integrity verification, and secure communications, proving its versatility and energy Efficiency debate is SHA-256-based PoW requires significant electricity consumption, raising concerns about its environmental impact. Alternative hashing mechanisms like SHA-3 and Scrypt are being explored to reduce energy costs.

Long-Term Viability is despite quantum computing concerns, SHA-256 remains a widely trusted cryptographic standard, with no known successful real-world attacks against it. These findings suggest that while SHA-256 remains one of the most secure and established cryptographic solutions, its energy consumption and potential quantum vulnerabilities may drive future innovations in blockchain security.

5. CONCLUSION

Blockchain technology and its core component, the SHA-256 algorithm, have become essential pillars of the modern digital economy. Due to its robustness and reliability, SHA-256 is the primary cryptographic tool in major blockchain systems like Bitcoin. Currently, SHA-256 demonstrates superiority in the following aspects: ensures a high level of security, guarantees data immutability, successfully tested over many years, widely applicable across various industries. However, technological advancements have also introduced challenges such as high energy consumption and the trend of centralization in mining operations.

In conclusion, SHA-256 remains one of the most reliable and well-tested cryptographic solutions in blockchain technology today.

6. REFERENCES:

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, Bitcoin Whitepaper (https://bitcoin.org/bitcoin.pdf), "SHA-256 in blockchain's original implementation."

2. NIST FIPS 180-4: Secure Hash Standard (SHA-256 specification), Official Specification (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf), "Technical specification of SHA-256 algorithm."

3. Antonopoulos, A. (2017). Mastering Bitcoin, BitcoinBook (https://github.com/bitcoinbook/bitcoinbook), "Detailed explanation of SHA-256 in Bitcoin."

4. Merkle, R. (1989). A Certified Digital Signature, Merkle Trees Paper (https://people.eecs.berkeley.edu/~raluca/cs261-f15/readings/merkle.pdf), "Foundational paper on Merkle Trees using hash functions."