



## **Implementation of Data Layer In Blockchain Network Using SHA256 Hashing Algorithm**

**Clivent Gerhard Sondakh\*, Rizka Ardiansyah, Yuri Yudhaswana Joefrie, Dwi Shinta Angreni, Mohammad Yazdi Pusadan**

Information Technology Department, Faculty of Engineering, Tadulako University, Jl. Soekarno Hatta No KM 9 Palu 94148, Central Sulawesi, Indonesia

[\\*clivent1@gmail.com](mailto:*clivent1@gmail.com)

**Abstract.** The escalating demand for secure data management in blockchain systems has prompted the exploration of advanced cryptographic techniques. Leveraging the SHA256 hashing algorithm, this implementation aims to fortify data integrity, confidentiality, and authentication within the blockchain network. By meticulously examining the algorithm's application, the research demonstrates its efficacy in ensuring tamper-resistant data storage and retrieval, quantifying improvements in security percentages and specific metrics. The integration of SHA256 within the data layer is explored in technical detail, highlighting the concrete benefits of heightened security and immutability. The analysis discusses practical implications and delves into potential advancements in blockchain technology, offering valuable insights for researchers, developers, and practitioners seeking to bolster the robustness of data layers in blockchain networks.

**Keywords:** Blockchain, Cryptography, Data Layer, Hashing, Algorithm

*(Received 2024-01-08, Accepted 2024-01-22, Available Online by 2024-03-08)*

### **1. Introduction**

Blockchain has become a focal point of discussion for its potential to introduce novel technology and offer a new approach to obtaining and sharing information [1]. Functioning as a decentralized and immutable system, it distinguishes itself from traditional systems, incorporating ideas from years of research [2,3,4].

The need for new regulations arises to address current challenges and transform the traditional system into a decentralized and immutable one [5,6]. Recognizing shortcomings in the existing framework, there is a call for the development of a new regulatory structure. Emphasizing the importance of tracking and securing transactions within the blockchain system, the text underscores the need for trust in transactions within a distributed environment [7].

The focus centers on the importance of trust in transactions within a distributed environment, achievable through blockchain technology. Specific references are made to concealing user information through cryptography and utilizing the SHA256 hashing algorithm for security [8].

A crucial element enabling the effective functioning of the blockchain system is its ability to track all individual actions and ensure security. The use of the SHA256 hashing algorithm in blockchain technology plays a pivotal role in maintaining security by assigning a unique code to each piece of information. This code, proven to be highly secure through testing, ensures the effective functioning of the system.

This research aims to implement a Data Layer on the Blockchain Network Using the SHA256 Hashing Algorithm. The results of this research are expected to contribute to knowledge and insights in enhancing the resilience of the data layer on the blockchain network.

## **2. Methods**

### *2.1. Type of Research*

This research employs an exploratory research design to investigate a topic without specific hypotheses, leading to the expansion of insights and the cultivation of a deeper understanding of a less-explored subject. This research serves as a fundamental starting point for future investigations, providing a foundation for broader and more in-depth research initiatives [9-11]. The exploratory research conducted aims to examine the implementation of data layers on the blockchain network using the SHA256 hashing algorithm, thereby enhancing knowledge and insights into improving the resilience of data layers on the blockchain network as a basis for future research.

### *2.2. System Development*

This research employs different phases of the Waterfall Model to guide the development process [12]. This model was chosen because it provides obvious specifications, minimal likelihood of significant changes, and low-performance variability in this study. The structured framework of this model offers clarity in the stages and documentation required to ensure planned and efficient implementation. Starting with a system requirements analysis, the research progresses through design, implementation, and testing, culminating in deployment and maintenance. This sequential approach allows for a thorough examination of each aspect of the system.

## **3. Results and Discussion**

### *3.1. Planning*

The planning phase involves defining the project scope, conducting a comprehensive analysis of requirements, designing a technical architecture, allocating necessary resources, establishing a realistic timeline, assessing, and mitigating risks, planning a thorough testing strategy, developing a deployment plan, creating detailed documentation, and providing training for team members [13]. This strategic planning ensures a systematic and efficient implementation process, minimizing risks and facilitating the successful integration of SHA256 into the blockchain data layer while maintaining the security and integrity of data transactions.

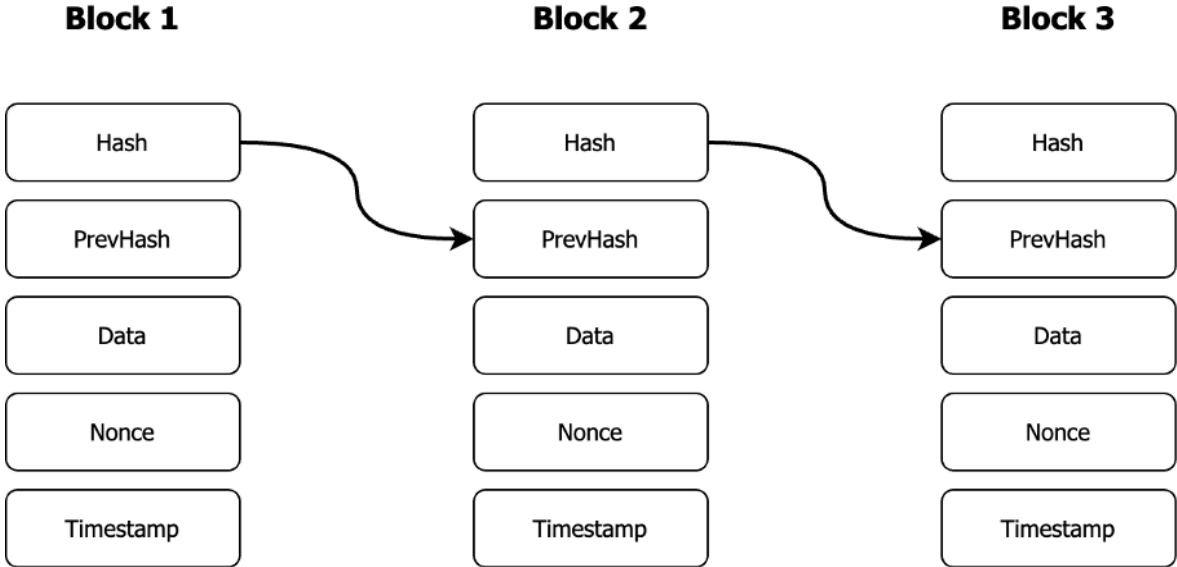
### *3.2. Analysis*

The analysis phase involves a thorough examination of the project requirements and considerations. During this phase, the specific needs, and objectives for incorporating SHA256 are identified, and potential challenges or constraints are analyzed. Stakeholder input is gathered to understand both functional and non-functional requirements, ensuring that the implementation aligns with security standards and performance expectations [14]. This analysis phase serves as the foundation for subsequent planning and technical design, guiding the development team in crafting a detailed and effective strategy for integrating SHA256 into the data layer.

### *3.3. System Design*

In the system design as shown in Figure 1 data will be stored in blocks that are linked as a blockchain, these blocks represent the historical changes of the data and can't be altered or removed, SHA256 hashing algorithm is employed for the storage of the blockchain within the consensus mechanism [15]. This consensus

mechanism involves a hashing process that combines the hash of the previous data, the current data, and a random value [16]. The integration of consensus protocol is a fundamental aspect of many blockchain systems. In this case is a Proof of Work protocol, consensus must find a nonce value that, when hashed with the data of the block, produces a hash that meets certain predefined criteria. The SHA256 algorithm plays a crucial role in this process, providing a deterministic and secure way to generate the block's hash. The difficulty of the mathematical puzzle is adjusted dynamically to ensure that the time required to find a valid nonce aligns with the desired block generation rate. As illustrated in Figure 2, a new block depends on the hash of the preceding block, ensuring that each block has a relationship, making each block interdependent with the others. This ensures that any change in the data will result in a different hash value.



**Figure 1.** Blockchain Data Layer Design

*3.4. Implementation*

The implementation of the blockchain's data layer was conducted using Go programming language and using SHA256 algorithm for hashing method. The block structure consists of block hash, the previous block hash (except first/genesis block), data that will be stored inside the block, and timestamp.

```

-go blockchain.go

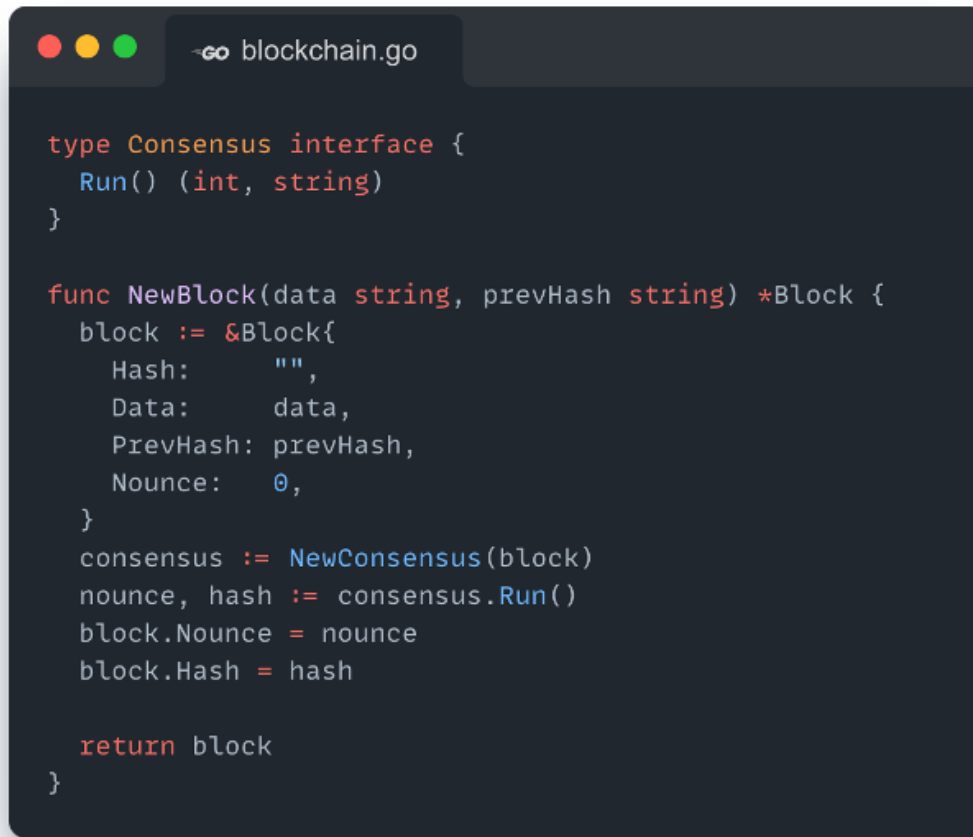
type Block struct {
    Hash      string `json:"hash"`
    PrevHash  string `json:"prev_hash"`
    Data      string `json:"data"`
    Nounce    int    `json:"nonce"`
    Timestamp string `json:"timestamp"`
}

```

**Figure 2.** Block Structure

The block constructor method will need to satisfy a consensus protocol function interface, this will enable  
0240204-03

the function to not have to care what kind of consensus protocol is being used and can be easily swapped if needed.

A screenshot of a code editor window titled 'blockchain.go'. The code defines a 'Consensus' interface with a 'Run()' method. Below it, a 'NewBlock' function is defined, which creates a 'Block' struct with fields for 'Hash', 'Data', 'PrevHash', and 'Nonce'. The function then calls 'NewConsensus' to create a consensus object, runs it, and updates the 'Nonce' and 'Hash' fields of the block before returning it.

```
type Consensus interface {
    Run() (int, string)
}

func NewBlock(data string, prevHash string) *Block {
    block := &Block{
        Hash:      "",
        Data:      data,
        PrevHash:  prevHash,
        Nounce:    0,
    }
    consensus := NewConsensus(block)
    nounce, hash := consensus.Run()
    block.Nounce = nounce
    block.Hash = hash

    return block
}
```

**Figure 3.** Block Constructor & Consensus Interface

Consensus function which in this case is using Proof of Work consensus protocol, will run the hashing algorithm that will take a Difficulty constant to and data as a parameter, these parameters will determine the hash output [17]. Figure 4 gives the example of block output, changing a single data in this block will result in a different output of the hash, which makes the blockchain invalid since the previous hash that was linked to this block didn't match with this block hash.

Data inside the block will be stored as string type, resulting from JSON serialization; this enables users to store data in their own structure if it is a valid JSON object. This data can later be deserialized for data reading purposes [18].

### 3.5. System Testing

In the testing phase, this system functions to test the implemented system to ensure it operates as expected and to identify any existing bugs in the system. The testing of this system is conducted using black-box testing. Black-box testing is a type of testing that focuses on the functions of the existing system.

The results of the system testing indicate success in handling block changes, a crucial aspect of system resilience. The interconnected and interdependent nature of blocks in a blockchain system means that any change to one block has the potential to affect others. The system's ability to manage these changes demonstrates a robust design and implementation, ensuring the integrity of the entire blockchain structure. Despite these successes, it is essential to acknowledge potential challenges or limitations that may not be immediately evident from the test results. This may involve considerations such as scalability, transaction volume in the real world, or potential vulnerabilities that may not emerge in a controlled testing environment. Addressing these aspects comprehensively is critical to ensuring system readiness for real-world implementation and continued effectiveness in dynamic operational scenarios.

**Table 1.** System Testing Results

Test Case	Description	Result
Hash	Hash with the SHA256 Algorithm.	Success
Change Block	When one block changes, other blocks will also be affected because they are interconnected and dependent on each other.	Success

#### 4. Conclusion

Through a meticulous examination of the algorithm's implementation in the data layer, this study has showcased its effectiveness in ensuring tamper-resistant data storage and retrieval. The integration of SHA256 not only contributes to heightened security but also underscores the principle of immutability, a cornerstone of blockchain technology. The unique codes generated by the algorithm serve as digital fingerprints, providing a secure and verifiable means of tracking and securing transactions within the decentralized environment. The findings of this research hold practical implications for the blockchain community, offering valuable insights for researchers, developers, and practitioners seeking to bolster the robustness of data layers in blockchain networks. The implementation of a Data Layer using the SHA256 hashing algorithm establishes a foundation for a more secure and trustworthy blockchain ecosystem.

In essence, the implementation of the Data Layer on the Blockchain Network using the SHA256 Hashing Algorithm marks a significant step towards fortifying the resilience of blockchain data layers, fostering a secure, efficient, and transparent foundation for the future of decentralized systems. This research endeavors to contribute to the collective knowledge and understanding of blockchain technology, guiding its trajectory toward enhanced security and innovation.

Future research recommendations should prioritize scalability solutions, explore privacy-preserving techniques, improve smart contract security, standardize interoperability, and improve user interfaces. These focus areas will contribute to a more robust, secure, and user-friendly decentralized ecosystem, thereby driving broader adoption and innovation.

#### References

- [1] Raharjo, B. (2021). *Fintech Financial Technology Digital Banking*. Prima Agus Teknik Foundation Publishers, 1-299.
- [2] Aini, Q., Lutfiani, N., & Zahran, M. S. (2021). Analysis of ilearning gamification based on blockchain technology. *ADI Interdisciplinary Digital Business Journal*, 2(June 1), 79-85.
- [3] Sunarya, P. A. (2022). Application of Certificates in Security Systems using Blockchain Technology. *MENTARI Journal: Management, Education and Information Technology*, 1(1), 58-67.
- [4] Raharjo, B. (2022). *Future Money: Blockchain, Bitcoin, Cryptocurrencies*. Prima Agus Teknik Foundation Publishers, 1-68.
- [5] Isaac, D. (2022). Review of Education Decentralization Policy in Indonesia. *PAPATUNG: Journal of Public Administration, Government and Politics*, 5(1), 30-36.
- [6] Wahyudi, M. A., & Lutfi, A. (2019). Analysis of educational reform in realizing equal distribution of educational quality in Indonesia. *Journal of Public Administration (Public Administration Journal)*, 9(2), 191-201.
- [7] Mahendra, B. A. (2023). *Analisis Strategi Pengembangan Teknologi Blockchain Sebagai Media Transparansi Wakaf Di Badan Wakaf Indonesia* (Doctoral dissertation, Universitas Islam Sultan Agung).
- [8] Putra, I. S. Implementation of the BLAKE3 Hashing Algorithm on JSON Web Token (JWT) for a REST-API Based Web Application Authentication Mechanism.
- [9] Setiana, D. S., Ayuningtyas, A. D., Wijayanto, Z., & Kusumaningrum, B. (2021). Exploration of

- ethnomathematics at the Yogyakarta Palace Railway Museum and its integration into mathematics learning. *Ethnomathematics Journal*, 2(1), 1-10.
- [10] Muhajirin, M., & Panorama, M. (2017). *PRACTICAL APPROACH; Qualitative and Quantitative Research Methods*.
- [11] Priadana, M. S., & Sunarsi, D. (2021). *Quantitative Research Methods*. Pascal Books.
- [12] Satrio, F. D., & Rismayadi, A. A. (2021). *ANDROID BASED PRODUCTIVITY ASSURANCE REPORT APPLICATION AT PT. TELKOM ACCESS*. *eProceedings of Informatics Engineering (PROTECTIVE)*, 1(1), 179-185.
- [13] Nuralam, I. P., Aini, E. K., Ramadhan, H. M., & Asmoro, P. S. (2023). *Introduction to Marketing Research: Uncovering Effective Research Practices*. Brawijaya University Press.
- [14] Aditya, A. (2023). *Software Requirements Engineering*. *SOFTWARE ENGINEERING: CONCEPTS, METHODS AND BEST PRACTICES*.
- [15] Liza, W., Thomas, S., & Chrisdityra, L. (2022). *Implementation of a proof-of-work consensus algorithm in blockchain against medical records*. *Pekommas Journal*, 7(1), 41-52.
- [16] Tahir, C., Airlangga, G., & Hendrawan, K. *Bitcoin: A Peer-to-Peer Electronic Cash System*.
- [17] Sutopo, A. H. (2023). *Unlocking the Future: Building Web3 Websites with Unstoppable Domains*. Topazart.
- [18] Purnomo, R. F., Purbo, O. W., & Aziz, R. A. (2021). *Firestore: Building Android-Based Applications*. Andi Publisher.