Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 03, March-2023

Performance Analysis of Various QoS Parameters of Different Hashing Algorithms in BlockchainTechnology

Dr. D S Waghole
Department of Computer Science
JSPM's JSCOE
Hadapsar, Pune-411028

Shyam Ramchandani
Department of Computer Science
JSPM's JSCOE
Hadapsar, Pune-411028

Mangesh Shinde
Department of Computer Science
JSPM's JSCOE
Hadapsar, Pune-411028

Intisar Sayyed
Department of Computer ScienceJSPM's JSCOE
Hadapsar, Pune-411028

Pruthvi Shetty
Department of Computer ScienceJSPM's JSCOE
Hadapsar, Pune-411028

***Abstract*—The blockchain technology presents an opportunity to introduce new business models in an integrated marketplace. One of the biggest challenges in the education sector is to utilize blockchain to securely store and verify student records. A reliable and valuable confirmation of these records can be achieved through the use of a secure, open blockchain. Choosing the right blockchain that is accessible, adaptable, and cost-effective is crucial in developing a successful business model. As clinical research records have increased, the need for accurate data and the elimination of measurement errors have become critical in confirming findings. Student records should be kept confidential and only accessible to authorized individuals. The blockchain era offers a solution to reduce fake certificates and ensure the legitimacy, privacy, and security of student records. However, using electronic signatures or marks as a form of authentication has a fundamental security flaw and does not fully address the issue. Simply having a marked document does not guarantee its authenticity and a false state of normality can occur if the system is compromised. Therefore, the marked document itself must be considered as an endorsement to ensure its security and validity.**

Keywords- Blockchain, Digital Certificate, Document Verification, SHA-256, Smart Contracts, Consensus Algorithm, Hashing, Authentication

I. Introduction

Blockchain technology was first introduced in 2008 by Satoshi Nakamoto as a decentralized and transparent ledger for data storage and manipulation [3]. By the means of this project, our goal is to design an web application for secure verification of certificates, specifically graduation certificates and transcripts [5]. Due to the ease of illegal tampering of information in these certificates and the need to keep it confidential, there is a high demand for a secure mechanism to ensure the authenticity of the information. Blockchain technology offers a solution to this problem [6]. The application uses the SHA processor to generate secure digests of different lengths using hash algorithms such as SHA512/224 and SHA-512/256. The initial hash values were generated using SHA-512 and the implementation was optimized for efficiency, using a 32-bit datapath. This ensures the secure and reliable verification of certificates and transcripts through the use of blockchain technology [7].

II. Literature Survey

The digital certificate system based on blockchain technology is proposed to solve the problem of counterfeit certificates in education. Schools input only the names of students and schools when issuing certificates and diplomas, leading to a lack of effective anti-forge measures. The unmodifiable property of blockchain technology allows for the creation of digital certificates that are anti-counterfeit and verifiable [2]. Blockchain technology is being used for cost savings and high security in various applications, including distributed systems and recording information about transactions without third-party verification. The issue of counterfeit certificates is a serious problem for education managers worldwide, and the proposed UniCert system, built on UniCoin, a digital currency based on blockchain, will solve this issue. The system can also be extended to address other issues such as anti-counterfeiting and copyright protection [3].

Previous blockchain contract protocols utilize centralized credible nodes for fairness and traceability, but they can compromise other nodes if credible nodes conclude to be dishonest. To address this, a secure method of digital certificate-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 03, March-2023

based verification in blockchains is developed. This solution uses blockchain and digital certificate in combination to design a secure system for privacy of data in blockchains without third-party verification. The proposed high-efficiency network forwarding protocol supports fair contract signing by multiple signers and protects the privacy of contracts used and identities of participants. Many experiments resulted into improved communication, storage overhead, and detection rate [4]. With the cost-effectiveness of 64-bit computing, a more efficient 256-bit hashing algorithm is proposed by using SHA- 512-bit algorithm and truncating its output to exact 256 bits, called SHA-512/256. Also a method to reduce the size of the SHA-512 constants table is provided to improve implementation efficiency [8].

III. Proposed System

A. Architecture

Our proposed architecture converts the soft copy of certificates to mathematical representations through encoding and quantization. These certificates are further processed using cryptographic principles to create a mathematical diploma and store it in blocks. The cryptographic hash function is used to create a mix of information. Each block contains a mix of information, hash pointing to the previous block and current timestamp. All adjacent blocks are linked to each other to form a blockchain. The organization records the graduate information by providing details such as name and email, which are stored in a table. The organization or authenticator can verify the authenticity by accessing the graduate information.

B. Digital Certificate Generation

This defines the process where, student certificates are transformed into the mathematical form using quantization and sampling. The academic and sports records of each organization are stored in a table. The certificates are transformed into a binary representations of 0's and 1's and represented as a 2-dimensional function. Each bit holds a specific value. An administrative login is used to access the platform and transfer the student's certificate into mathematical form. The platform allows adding new students and uploading new certificates. When a new student is added, their information is recorded, and when a new certificate is uploaded, it is stored.

C. Hash Code

A hash function is employed to create the hash for the certificates. The function takes arbitrary data as input to provide output result in an fixed format. The function needs to have a predefined plan, starting conditions, and boundaries. The verification process starts by following the same initial conditions and boundaries to develop the consistent output. Whenever the certificates are uploaded on the site, a hash code is generated for mathematical representation. Unlike SHA-1, these hash functions are collision free.

D. Digital guarantee confirmation

In this process, the validity of mathematical certificates is confirmed. The certificates shared on the websites are verified by comparing the generated hash code. The hash code generated for certificate is used to prevent any alterations. The organization and authenticator can sign-in to the platform and choose the type of certificate they wish to verify. If the provided certificates are authentic, it will result into a legitimate certificates and the process will proceed. If the certificate is tampered with or not from a legitimate source, it will result in an error stating altered certificates.

E. Working of Web portal

This platform consists of three pages: an admin login page, a student registration page, and a verification page. The admin can access the platform and transfer data using their login credentials. On the student registration page, the administrator can add a new student with his/her certificates by clicking the "add candidate" and "add certificate" buttons. The authenticator can verify the certificates through their credentials. Autenticator inputs the student ID and select the type of certificate, then choose the "confirm" option. If those uploaded certificates are genuine, the verification will be successful. If not, the verification will be unsuccessful.

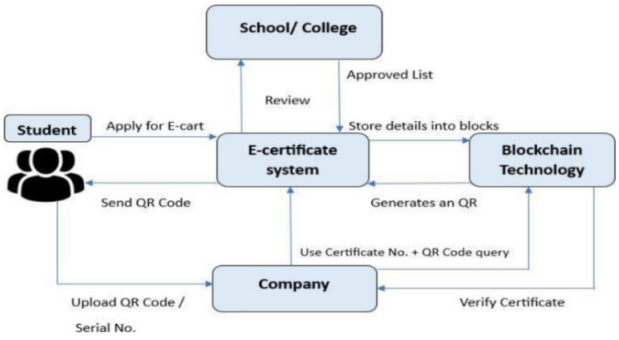

Fig. 1. Proposed System

IV. Implementation

Blockchain technology is known to be a decentralized and secure digital ledger system that facilitates easy and transparent sharing of information. It uses blocks to store data and eliminates the need for intermediaries to verify information. Each block contains a creation timestamp and provides a link to the previous block, forming a blockchain. The information stored in the blocks is verifiable, permanent, and accessible to everyone in the network. This makes the blockchain a transparent, secure, and public system.

V. PERFORMANCE EVALUATION

The most commonly used hash functions in real-time applications are MD5 and SHA-1. To achieve enhanced security,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 03, March-2023

the three new hash functions SHA-256, SHA-384, and SHA-512 (commonly referred to as SHA-2) are employed [9]. The hash size of MD5 is 128 bits, which is smaller than the hash size of SHA- 256, which is 256 bits. Additionally, MD5 is faster than SHA- 256. However, SHA-256 is more secure than MD5. To achieve maximum security with smaller size and high speed, we plan to merge these two algorithms to create an improved version called the Modified SHA-2 Algorithm. We have conducted 20 tests for both MD5 and SHA-256 to determine their security strength, as shown in the graph. By merging these two algorithms, we expect to achieve higher security with the Modified SHA-2 Algorithm. We believe that it will take intruders more time to crack passwords, making it nearly impossible. Thus, the Modified SHA-2 Algorithm is expected to be a better and improved version.

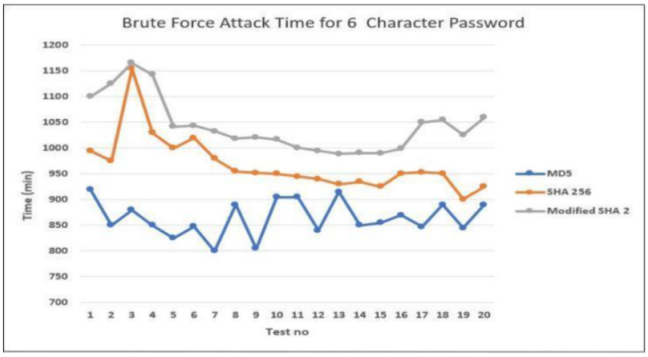

Fig. 2. Security Strength Comparison

VI. Conclusion

In this study, we propose a Blockchain-based approach to counter certificate forgery, which guarantees the protection and integrity of information. Additionally, we aim to shorten the prolonged verification time for certificates. All certificates are efficiently consolidated into a single QR code, making digital certificate management more convenient. Thus, we anticipate that the proposed Modified SHA 2 Algorithm will deliver a high level of security for the system's documents with enhanced speed.

Acknowledgment

We would like to thank all the staff at JSPM's Jayawantrao Sawant College of Engineering, for their generous help and companionship during our work. Likewise, we are extremely grateful to the scientists and distributors who provided their resources.

References

[1] A. Gayathiri, J. Jayachitra and S. Matilda, "Certificate validation using blockchain," 2020 7th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 2020, pp. 1-4, doi: 10.1109/ICSSS49621.2020.9201988.

[2] J. -C. Cheng, N. -Y. Lee, C. Chi and Y. -H. Chen, "Blockchain and smart contract for digital certificate," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, Japan, 2018, pp. 1046-1051, doi: 10.1109/ICASI.2018.8394455.

[3] T. T. Huynh, T. Tru Huynh, D. K. Pham and A. Khoa Ngo, "Is- suing and Verifying Digital Certificates with Blockchain," 2018 International Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, Vietnam, 2018, pp. 332-336, doi:10.1109/ATC.2018.8587428.

[4] B. Liu, L. Xiao, J. Long, M. Tang and O. Hosam, "Secure Digital Certificate-Based Data Access Control Scheme in Blockchain," in IEEE Access, vol. 8, pp. 91751-91760, 2020, doi: 10.1109/ACCESS.2020.2993921.

[5] Z. Wang, J. Lin, Q. Cai, Q. Wang, D. Zha and J. Jing, "Blockchain-Based Certificate Transparency and Revocation Transparency," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp.681-697, 1 Jan.-Feb. 2022, doi: 10.1109/TDSC.2020.2983022.

[6] J. Guo, H. Zhou, L. Yang and X. Chen, "Research on digital copyright blockchain technology," 2020 3rd International Conference on Smart BlockChain (SmartBlock), Zhengzhou, China, 2020, pp. 1-5, doi:10.1109/SmartBlock52591.2020.00028.

[7] S. -H. Lee and K. -W. Shin, "An efficient implementation of SHA processor including three hash algorithms (SHA-512, SHA-512/224, SHA-512/256)," 2018 International Conference on Electronics, Information, and Communication (ICEIC), Honolulu, HI, USA, 2018, pp. 1-4, doi:10.23919/ELINFOCOM.2018.8330578.

[8] S. Gueron, S. Johnson and J. Walker, "SHA-512/256," 2011 Eighth International Conference on Information Technology: New Generations, Las Vegas, NV, USA, 2011, pp. 354-358, doi: 10.1109/ITNG.2011.69.

[9] Jun-Cheol Jeon, Kang-Joong Seo, Kee-Won Kim, "Hardware complexity of SHA-1 and SHA-256 based on area and time analysis", 2012 International Conference on Information Networking (ICOIN 2012), pp. 557-561, doi: 10.1109/ICOIN.2012.6164439.

[10] Catia Khouri, Fabiola Greve, "A Generic Consensus Algorithm for Shared Memory", 2013 IEEE 19th Pacific Rim International Symposium on Dependable Computing (PRDC), doi: 10.1109/PRDC.2013.16.