

BLOCKCHAIN BASED CERTIFICATE VALIDATION

¹Dr. A. Sudhir Babu, ²B. Gayatri Prasanna, ³G V S R Saranya, ⁴Ch. Sirisha, ⁵K. Sai Ram, ⁶V. Ravi Kumar

¹Professor, ^{2,3,4,5,6}Student
Dhanekula Institute of Engineering & Technology
Vijayawada, India.

Abstract- It aims to enhance the security of academic certificates by converting them into digital signatures and storing them securely on a Blockchain server. This server provides tamper-proof data storage, preventing any unauthorized access or alterations. Any attempt to alter the data will result in verification failure during subsequent block storage, alerting users to potential tampering. In Blockchain technology, identical transaction data is replicated across multiple servers and verified through hash codes. If any data alteration occurs on one server, it is detected by others due to differing hash codes. This ensures that stored data remains intact. Additionally, in Blockchain, data is stored by verifying previous hash codes, ensuring the originality and integrity of the information. New transaction data is added as new blocks, with all block hash codes verified each time to maintain security.

Key words: Blockchain, Digital Signature.

I. INTRODUCTION

Blockchain technology, introduced by Satoshi Nakamoto in 2008, revolutionizes data sharing with its decentralized and transparent nature. This project focuses on developing an Android application for secure certificate verification. Today, graduation certificates and transcripts are vulnerable to illegal tampering, necessitating a robust mechanism to safeguard their originality and reliability. Numerous systems have emerged to secure e-certificates for educational institutions, with Blockchain emerging as a pivotal tool. By integrating Blockchain with diverse hashing techniques, data can be safeguarded, reducing the need for constant certificate validation.

In Blockchain technology, identical transaction data is stored across multiple servers with hash code verification. If the data is altered on one server, it will be detected by the others because the hash code for the same data will differ. For instance, in Blockchain technology, data is replicated across multiple servers, so if a malicious user alters data on one server, the hash code changes on that server while remaining unchanged on others. This altered hash code is detected during verification, preventing future malicious alterations by users.

In Blockchain, data is stored by verifying previous hash codes. If the old hash codes remain unchanged, the data is deemed original and unaltered. Subsequently, new transaction data is added to the Blockchain as a new block. Each time new data is stored, the hash codes of all blocks are verified.

Existing system:

In the application the first page is admin login, the next page consists of add student and certificate and last verifier page. Administrators can access our application by logging in with the provided admin login credentials. Then the admin can add the student and their certificates by tap the add student and add certificate button. Next, the verifier can validate the certificate using the verifier login id and password. They provide the login id of the student and select the certificate type and tap the verify button. If the uploaded certificates are original then the result will be a success. Otherwise, the result will be error and modified.

Proposed system:

In the application the first page is admin login, the next page consists of add student and certificate and last verifier page. Administrators can access our application by logging in with the provided admin login credentials. Then the admin can add the student and their certificates by tap the add student and add certificate button. Next, the verifier can validate the certificate using the verifier login id and password. They provide the login id of the student and select the certificate type and tap the verify button. If the uploaded certificates are original then the result will be a success. Otherwise, the result will be error and modified.

II. LITERATURE SURVEY

Jin-chiou et al [1] developed software in order to avoid counterfeiting certificates. so, the decentralized application was designed based on ethereum blockchain technology. First, generate the digital certificate for the paper certificate then hash value created for the certificate is stored in the blockchain system. Even it used to verify the authenticity of the certificate it required another scanning app to scan the certificate. The system saves on paper, prevent document forgery. But the QR-Code must be scanned with a smartphone and an internet connection is required.

Ze Wang et al [2] designed a blockchain-based certificate transparency and revocation transparency system. In this system, the certificate authority (CA) signed the certificate and the revocation status information of the respected certificates are published by the subject (Certificate Authority). Public logs are used to monitor the CAs operation.

At the other end, if there are users looking for short term returns, then the prime focus will not be on distributed flow, but will be on other aspects pertaining to scalability, security, transparency etc. Also, an amalgamation of both public and private blockchains can be used to utilize the benefits of transparency and secure accessibility. However, a mechanism for the server to generate multiple unique addresses for each user performing an operation on the blockchain is essential to achieve better outcomes [6].

The ability to ensure trust across various nodes through consensus in coordination with authentic and secure access to the data stored is a challenging and desirable property. Particularly in Land registration system, the identity of the users is hidden and only the eligible and thoroughly verified land is put to sale. Also, the entire system is under the single controller in the current system. The scalability aspect is unproved which has wide impact on the overall performance of the entire distributed blockchain network [7].

In health field, medical history of each patient must be treated with utmost confidentiality. Blockchain technology is used as a distributed approach to provide security for the medical reports of patients. Security is implemented in a three phased manner which includes authentication, encryption[8].

III. METHODOLOGY

- a. Initially, students apply for an e-certificate through the online portal and upload all academic documents.
- b. The portal verifies the authenticity of these documents through a trusted third party, which validates records from universities, schools, and colleges.
- c. Upon successful verification by these educational institutions, the data is stored in the blockchain, and a unique certificate ID or QR code is generated and issued to the student simultaneously.
- d. Rather than presenting physical copies of documents, students provide the received QR code or certificate ID to the organization.

IV. ALGORITHM USED

SHA 512

SHA512 is secure hashing which converts text data into hash code. Hash code is stored in several blocks. It contains the large key compared to other algorithms. It has only encryption, there will be no decryption. Hash code can be used for verifying the integrity of data. It is essential for ensuring data security.

This algorithm is widely used in various applications today. It is known for its robustness and reliability in protecting sensitive information. However, some downsides may be present due to its complex nature. The implementation can be challenging at times, but once mastered, it proves to be an effective tool for data protection. The large key size ensures a high level of security, making it a popular choice among developers and security professionals alike.

Ethereum Blockchain

In the now-deprecated proof-of-work Ethereum system, each block included the block difficulty, represented by a numerical value such as 3,324,092,183,262,715.

Lastly, there was a nonce, which served as a unique number like "0xd4cc543c5db2e37c," used in the mining process to satisfy the difficulty requirement and add the block to the blockchain.

The Work in proof of work:

- a. In the proof-of-work protocol, Ethash, miners engaged in a competitive process of trial and error to discover the nonce required for a block. Only blocks containing a valid nonce could be appended to the blockchain.
- b. During the block creation race, miners iteratively applied a mathematical function to a dataset. This dataset could only be acquired by downloading and processing the entire blockchain, as done by miners. The goal was to produce a mixHash that fell below a target determined by the block's difficulty. Achieving this necessitated trial and error.
- c. The block difficulty established the hash target. A lower target resulted in a smaller pool of acceptable hashes. Once generated, verifying these hashes was straightforward for other miners and clients. Any alteration to a transaction would significantly alter the hash, promptly indicating potential fraud.
- d. Hashing provided a clear means of detecting fraud. Moreover, the proof-of-work mechanism served as a substantial deterrent against chain attacks.

Proof of work and Security:

Miners were motivated to participate in the main Ethereum chain as there was little incentive for a subgroup of miners to establish their own chain, which would undermine the integrity of the system. Blockchains rely on maintaining a single, authoritative state as the ultimate source of truth.

The primary goal of proof-of-work was to elongate the blockchain. The longest chain was considered the most trustworthy because it represented the accumulation of the most computational effort. Under Ethereum's PoW system, it was exceedingly difficult to forge new blocks to alter transactions, fabricate false transactions, or sustain an alternative chain. This difficulty stemmed from the requirement for a malicious miner to consistently outpace all others in solving block nonces.

To consistently generate malicious yet valid blocks, a malicious miner would need to possess over 51% of the network's mining power to surpass all others. Achieving such a significant portion of the network's computational power would demand substantial resources in terms of expensive hardware and energy consumption, potentially outweighing any gains from carrying out an attack.

1. Procedure SELECTHASH(transactions):
2. if sizeof(transactions) < h₁:
3. Hash ← SPONGENT
4. else if h₁ < sizeof(transactions) < h₂:
5. Hash ← PHOTON
6. else:
7. Hash ← QUARK
8. end if
9. End Procedure
10. Procedure MINING(transactions):
11. Initialize(B)
12. B.PreviousBlockHash ← PreviousBlockHash
13. B.HashHelper ← Hash
14. B.Nonce ← 0
15. while Hash(B) < difficulty:
16. B.Nonce++
17. end while
18. vBroadcastBVM(B)
19. if v = true:
20. PreviousBlockHash ← Hash(B)
21. return success
22. else:
23. return fail
24. end if
25. End Procedure

V. WORKING PROCESS:

The Certification.sol file consists of a struct Certificate that forms our data block structure. This gives a draft for the data to be saved on the ethereum block. It holds a byte32 ipfs_hash correlated with the produced document and will be used further for authenticating the uniqueness of the document. Others are the details that must be involved in the Certificate. These solidity files once written can be compiled on platforms like Remix IDEonline that comprehend how to compile Solidity. Here, Truffle compiles the solidity and alters the given solidity files to something termed abis; this includes the machine code of the solidity functions, and depending on the computation and space usage, the cost of the transaction is figured out. These files will generally, after compilation and execution, have a similar name as the solidity file name but with a JSON extension. This JSON file is then used to generate a web3 instance of executing solidity code on the ethereum blockchain. The next crucial part of the system is IPFS (Inter Planetary File System), utilized for uploading documents. Being distributed in nature and no single user storing the document, the uploaded documents are secured and can be accessed with the help of hash. Each node in the IPFS system will have a section of the file; thus, none can access a document at a time.

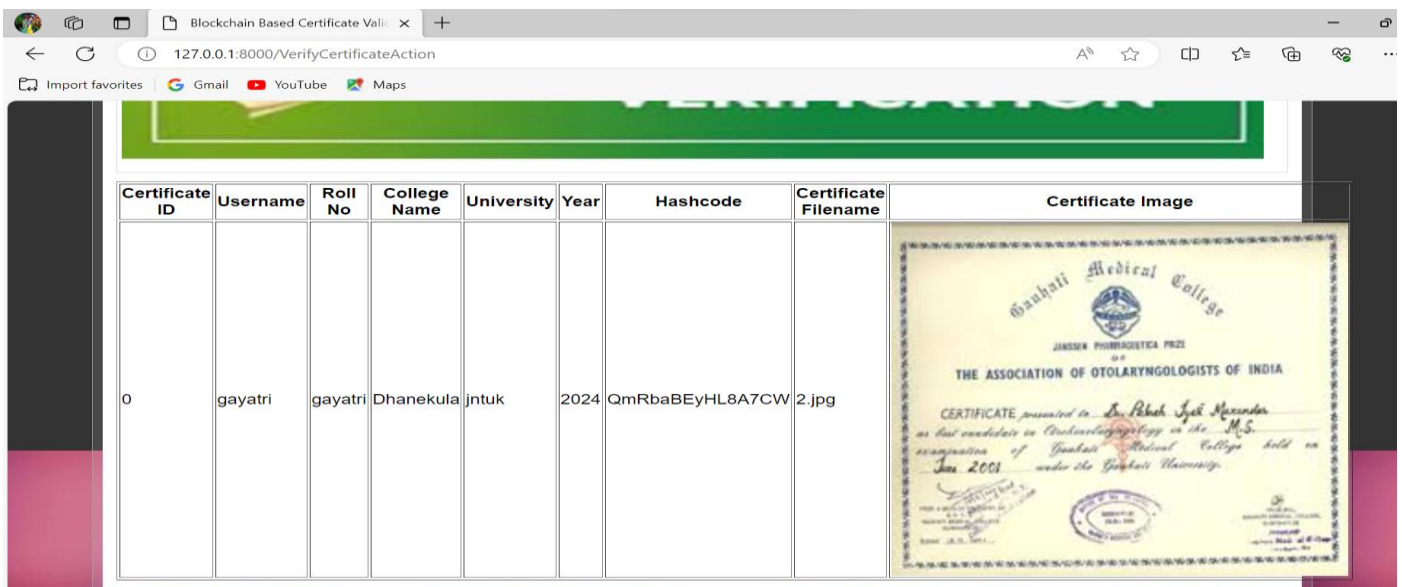
VI. MODELING & ANALYSIS

- Admin Login:** Administrators can access the system by logging in with the default username and password, which is 'admin'. Upon login, they have full access to all certificates stored in the Blockchain.
- New User Sign up:** New users can register with the application, and their signup details are securely saved in the Blockchain. These users can view the list of companies or universities that upload their students' certificates to the Blockchain.
- User Login:** Registered users can log in to the system using their credentials.
- Upload Certificate:** After logging in, users can upload certificates. The hash code address of the uploaded certificate is stored securely in the Blockchain, while the certificate image is saved in IPFS (Inter Planetary File System).
- Edit Certificate:** Users have the option to update existing certificates with new ones using this module.
- Verify Certificate:** Through this module, users can upload a certificate for verification. The Blockchain system verifies the uploaded certificate against all stored certificates. If a match is found, the certificate is successfully verified; otherwise, it fails verification.


VII. OUTPUT

It is the output after using blockchain a best fit and flask is used to create this web page and after upload the details the screen is shown like below:

In below screenshot 1 user can see all details of verified certificate and similarly can check verification for all certificates.



The screenshot shows a web browser window with the URL `127.0.0.1:8000/VerifyCertificateAction`. The page displays a table with the following data:

Certificate ID	Username	Roll No	College Name	University	Year	Hashcode	Certificate Filename	Certificate Image
0	gayatri	gayatri	Dhanekula	jntuk	2024	QmRbaBEyHL8A7CW	2.jpg	

Screenshot 1 : Certificate verified successful

In below screenshot 2 certificate verification failed and now click on 'Verify Certificate' link to verify with correct certificate.



Screenshot 2 : Certificate verification failed

VIII. CONCLUSION

The certificate application process and automated certificate issuance are transparent and accessible within the system. Companies or organizations can request information regarding any certification from the system. The assessment results offer convincing proof that the system is sufficiently secure to align with enterprise application standards. Subsequently, we performed a sequence of security assessments focusing on operational safety, data security, network security, and protocol security.

REFERENCES:

- [1]. J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere, and B. Stiller, "The Proposal of a Blockchain-based Architecture for Transparent Certificate Handling," in BIS2018: Business Information System Workshops, vol. 339 of Lecture Notes in Business Information Processing, Springer, pp. 185-196, 2018.
- [2]. A. Gayathri, J. Jayachitra, and S. Matilda presented a paper titled "Certificate validation using blockchain" at the 7th International Conference on Smart Structures and Systems (ICSSS) in 2020. The paper is associated with DOI: 10.1109/icsss49621.2020.9201988.
- [3]. Wang Z., Lin J., Cai Q., Wang Q., Jing J., and Zha D. discussed "Blockchain-Based Certificate Transparency and Revocation Transparency" in the proceedings of FC 2018 (Financial Cryptography and Data Security), published in Lecture Notes in Computer Science, volume 10958 by Springer, Berlin, Heidelberg, in 2019.
- [4]. J. Chang, S. N. Kadry, and S. Krishnamoorthy, "Review and synthesis of Big Data analytics and computing for smart sustainable cities," in IET Intelligent Transport Systems, 2020.
- [5]. Benyuan He, "An Empirical Study of Online Shopping Using Blockchain Technology", Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.
- [6]. Xiuping Lin, "Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the EthereumBlockchain", Department of Information Engineering, National Taiwan University, Taiwan, R.O.C., 2017.
- [7] Yong Shi, "Secure storage service of electronic ballot system based on block chain algorithm", Department of Computer Science, Tsing Hua University, Taiwan, R.O.C., 2017.
- [8] ZhenzhiQiu, "Digital certificate for a painting based on blockchain technology", Department of Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C., 2017.