International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 Impact Factor: 8.176 ISSN: 2582-3930

CERTIFICATE VERIFICATION AND VALIDATION USING BLOCKCHAIN

G KAVYA REDDY
S BAL NARESH
Under the guidance of MR. **D. Rambabu**
Sreenidhi Institute of Science and Technology

KEYWORDS

Hash code, Blockchain, Certificate, Digital Signature

ABSTRACT

When the students have finished their studies, their numerous certificates of excellent performance, score transcripts, diplomas, etc., will be an important point of reference for entrance to other schools or positions. Only the names of the schools and the students are included when schools create different prizes or diplomas. Events that lead to the graduation certificate being forged are frequently discovered since there is no reliable anti-forge system. The blockchain-based digital certificate system would be suggested as a solution to the issue of certificate forgery. The blockchain's capacity to be modified makes it possible to create digital certificates with anti-counterfeit and verifiability. In this system, issuing digital certificates is done in the manner listed below. Create an electronic file of the paper certificate first, along with other pertinent data, and while doing so, determine the hash value of the file. The hash value should then be added to the block in the chain system. To be attached to the paper certificate, the system will generate a linked QR-code and an inquiry string code. The solution not only increases the legitimacy of diverse paper-based certificates, but also significantly lowers the chance of certificate loss because to the blockchain's changeable qualities.

INTRODUCTION

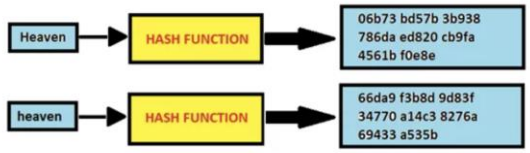
Blockchain was first introduced in 2008 under the pseudonym Satoshi Nakamoto although its inspiration goes back to 1982 by cryptographer David Chaum. Blockchain is a decentralised database that's frequently used to log various transactions. The transaction is added to a block that already contains records of numerous transactions after consensus among the various nodes has been obtained. The hash value of a block's most recent connection counterpart is included in each block. A blockchain is created when all the blocks are linked to one another. Data are decentralised because they are dispersed among several nodes (the distributed data storage). Consequently, the nodes maintain the database together. Under blockchain, a block becomes validated only once it has been verified by multiple.

With the use of hash code verification, the same transaction data is saved across many servers in blockchain technology. If data is altered on one server, it may be seen on the other server since the hash code will change. For example, in Blockchain technology data will be stored at multiple servers and if malicious users alter data at one of the servers then its hash code will get changed in one server and other servers left unchanged and this changed hash code will be detected at verification time and future malicious user changes can be prevented.

In Blockchain each data will be stored by verifying old hash codes and if old hash codes remain unchanged then data will be considered as original and unchanged and then A fresh block of transaction data will be added to the blockchain. Every new block of data storage will have its hash code validated.

SHA (Secure Hash Algorithm)

Secure Hashing Algorithm, or SHA. Data and certificates are hashed with SHA, a modified version of MD5. By using bitwise operations, modular additions, and compression functions, a hashing algorithm reduces the input data into a smaller form that is impossible to comprehend. Can hashing be cracked or decrypted, you may wonder? The main distinction between hashing and encryption is that hashing is one-way; once data has been hashed, the resultant hash digest cannot be decrypted unless a brute force assault is applied. See the illustration below to see how the SHA algorithm functions. SHA is designed to provide a different hash even if only one character in the message changes. Consider two example inputs to which hash keys are generated using a hash function



In the above figure, we can observe that the hash value generated for both words is different. This is known as the avalanche effect. This effect tells that a small change in the input message completely generates different outputs. As a result, attackers won't be able to decipher what the hash digest initially said or determine whether the message was altered while in route and inform the message's recipient.

PROPOSED SYSTEM

First, a block is created, attached to the blockchain, and disseminated throughout the network of nodes using the certificate data. The block data is then transformed into a PDF file and digitally signed using the certificates and signatures of the nodes. Then, these certificates are verified using an API that may be customized and includes a block explorer and invalidator. It is highly difficult to alter or amend a digital certificate on a distributed ledger due to the immutability of blockchain technology and digital signatures. It is also quite simple to confirm the authenticity of a digital certificate.

With the aid of distributed technologies like IPFS and Ethereum smart contracts, our suggested approach makes it simple to determine if a document is real or not as well as to check its integrity and originality. How people engage with smart contracts is depicted in the image over. The following players engage with our smart contract

• University/ College: College acts as a Certificate issuing authority. This reality can be any association that wants to issue a instrument. College or Certificate issuing authority only has the right to issue one or further instruments in the system. It'll also include a phase where the College will induce instruments after validating and authorizing the details.

• Pupil: scholars will be suitable to download and view digital documents. scholars also admit the hash regarding the document issued for him, which in the future can be used to pierce the document and corroborate it.

• Company: Company will be the stoner who'll have access to regarding originality, authenticity, and integrity of the documents with the help of the digital hand of the document.

METHODOLOGY

1. Block Creation and Hash Code Generation
2. Digital Certificate Creation
3. Broadcast the Generated Block
4. Digital Certificate Validation
5. Querying the Blockchain

Block Creation and Hash Code Generation

A block is a container data structure. The average size of a block seems to be 1MB (source). Here every certificates number will be created as a block. For every block an hash code will generate for security.

The Hash Code is generated by taking the details of the student then performing a Proof of Work algorithm using Secure Hash Algorithm 512 which is a hashing algorithm used to convert text of any length into a fixed-size string.

Digital Certificate Creation

Digital certificate is created with the details of the student. We have a HTML schema for the format of the certificate. Every certificate generated has a unique hash value which is hidden in the certificate.


Certificate of Completion

This certificate is presented to

KAVYA

with 19311A05E2 for passing

CSE

BTECH

awarded on 05/05/2023

Broadcast the Generated Block

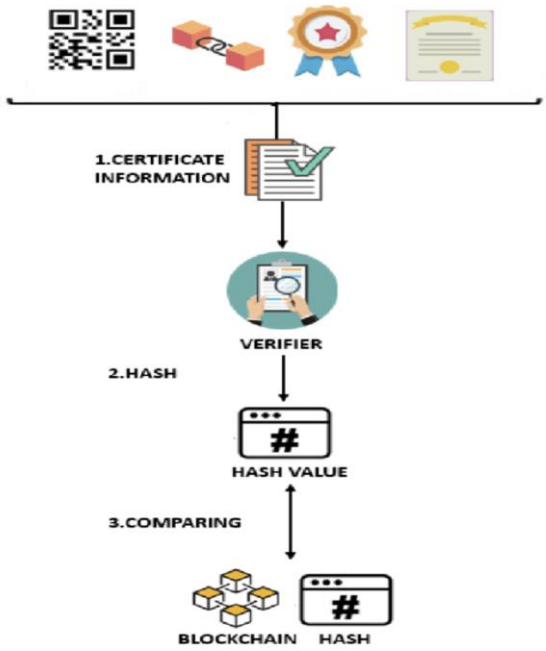
After the generation of the block and digitally signing the certificate document, we need to broadcast the generated block over the blockchain network so that all the participants in the network are aware of the new block and update the chain in their local storage so that the network is in sync.

Since, this step is very important because it is not possible to keep the data at one place which can lost at any time so every time the server generates the certificate it will broadcast to other servers so that though the data is lost at one server, we can still have the data at other servers. This helps in case of data lost.

Digital Certificate Validation

The digital certificate will be collected by a verifier, a company, or an administrator, who will then upload it to an application, convert it into a digital

signature, and check it against a blockchain database. If a match is found, the blockchain will retrieve all student information and display it to the verifier; if not, the certificate will be deemed fake or forged.



Querying the Blockchain

This is done in 2 ways:

1. By using hash value
2. By using the specific field's value in the block

By using Hash value

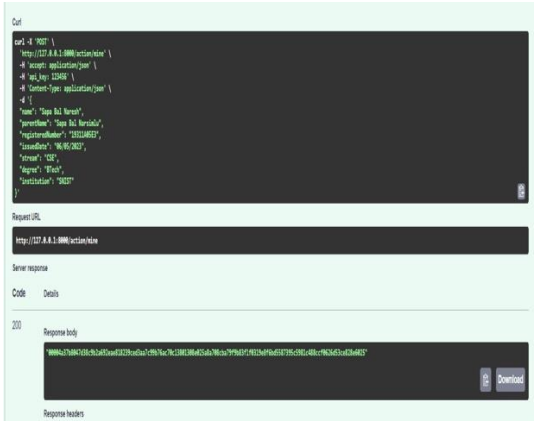
If the given hash value is found in the block then the respective block data will be given as output.

By using the specific field's value in the block

If the given field's value is found in any number of blocks generated then the respective blocks data will given as output

RESULT

Block Creation and Hash Code Generation



Digital Certificate Creation

Digital Certificate Validation

Querying the Blockchain

1. By using Hash value

2. By using the specific field's value in the block

CONCLUSION

One of the key characteristics of blockchain technology is data security. Each node in the blockchain stores and validates the same data, creating a massive and public online record. The possibility of certificate forgery is decreased by using the suggested blockchain-based system.Regarding the automatic certificate issuance and application processes, the system is open and transparent. As a result, groups or enterprises can query the system for information on any certificate. In conclusion, the system guarantees the security and accuracy of the information.

REFERENCES

1. Santosh Pandey, Gopal Ojha, Rohit Kumar, And Bikesh Shrestha BlockSIM: A practical simulation tool for optimal network design, stability and planning 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC).
2. Jiin-Chiou Chen, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen Blockchain and Smart Contract for Digital Certificate Proceedings of IEEE International Conference on Applied System

Innovation 2018 IEEE ICASI 2018- Meen, Prior & Lam(Eds).

3. Smart contractswhitepaper, https://github.com/OSE- Lab/learning-blockchain/blob/ master/ethereum/smart-contracts.md
4. Gong Chen, Development and Application of Smart Contracts, https://www.fisc.com.tw/Upload/b0499306-1905-4531-888a-2bc4c1ddb391/TC/9005.pdf
5. Weiwei He, Exempted from cumbersome auditing and issuance procedures, several national junior diplomas will debut next year.iThome, https://www.ithome.com.tw/news/119252
6. Xiuping Lin, "Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the Ethereum Blockchain", Department of Information Engineering, National Taiwan University, Taiwan, R.O.C., 2017.