INTERNATIONAL JOURNAL OF
MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.521

Online Blockchain Based Certificate Generation and Validation System

Mr. S. Nishanth MCA, Mr. D. Prabhakaran, AP/MCA, Dr T. Geetha MCA, Ph.D.

PG Student, Department of Master of Computer Application, Gnanamani College of Technology, Namakkal,

Tamil Nadu, India

Assistant Professor, Department of Master of Computer Application, Gnanamani College of Technology, Namakkal,

Tamil Nadu, India

HOD, Department of Master of Computer Application, Gnanamani College of Technology, Namakkal,

Tamil Nadu, India

ABSTRACT: In the digital world, Advances in information technology, the wide availability of the Internet, and common usage of mobile devices have changed the lifestyle of human beings. In this project, I have identified the vulnerabilities and security themes required for document verification that seamlessly merges blockchain technology, cryptography, advanced verification mechanisms and innovative Capsule Siamese Network. Each block contains the hash value of its last counterpart for connection. All the blocks are connected and together they form a blockchain. Data are distributed among various nodes (the distributed data storage) and are thus decentralized. Consequently, the nodes maintain the database together. Under blockchain, a block becomes validated only once it has been verified by multiple. Blockchain features a decentralized and incorruptible database that has high potential for a diverse range of uses. Each and every thing are digitized in which the academic certificate is digitized in the educational institution and provided to the students. The increase in security breaches compromise user's privacy of academic digital certificate. The institution and organization find it very difficult to validate and verify the digital certificates. By using blockchain technology. we can provide a more secure and efficient digital certificate validation.

KEYWORDS: Blockchain, Digital certificate, SHA-256 Algorithm

I.INTRODUCTION

Advances in information technology, the wide availability of the Internet, and common usage of mobile devices have changed the lifestyle of human beings. Virtual currency, digital coins originally designed for use online, has begun to be extensively adopted in real life. Because of the convenience of the Internet, various virtual currencies are thriving, including the most popular Bitcoin, Ether, and Ripple are the value of which has surged recently. People are beginning to pay attention to blockchain, the backbone technology of these revolutionary currencies. Blockchain features a decentralized and incorruptible database that has high potential for a diverse range of uses.

Blockchain is a distributed database that is widely used for recording distinct transactions. Once a consensus is reached among different nodes, the transaction is added to a block that already holds records of several transactions. Each block contains the hash value of its last counterpart for connection. All the blocks are connected and together they form a blockchain. Data are distributed among various nodes (the distributed data storage) and are thus decentralized. Consequently, the nodes maintain the database together. Under blockchain, a block becomes validated only once it has been verified by multiple parties. Furthermore, the data in blocks cannot be modified arbitrarily. A blockchain-based smart contract, for example, creates a reliable system because it dispels doubts about information's veracity.

Because information technology has developed rapidly in recent years, data protection is more necessary than ever. Graduates, whether they choose to continue studying or start job hunting, require various certificates for interviews. However, they often find that they have lost their educational and commendation certificates. Reapplying for hard copies can be time-consuming because certificates are granted by different organizations and in-person application may be necessary. By contrast, applying for an e-copy can save paper and time. By providing information for identity verification, graduates are able to apply for any certificate easily. Nevertheless, because of this convenience, forged degree certificates, licenses, and certificates are prevalent. Consequently, schools and companies cannot instantly validate the documents

they receive. To solve this problem, a certificate system based on blockchain was designed in this study. Data are stored in different nodes, and anyone who wishes to modify a particular internal datum must request that other nodes modify it simultaneously. Thus, the system is highly reliable.

II.EXISTING SYSTEM

Employers evaluate applicants' education background to screen out applicants who have forged and or exaggerated their qualifications and to protect the company against scam, such as degrees purchased from and verified by illegal institutions. Verifications are done through direct contact with the school or through the aid of a third party such as trusted background screening companies. Job seekers provides information to background screening agencies and pay the stipulated amount accrued to such service. Manual record keeping like students receive these physical certificates and responsible for maintaining and storing them. This often involves creating personal files, folders, or storage system at home. Some pre-verification service provides a secured online cite where job seekers upload their education credentials to enable employers have access to view such verified information at any point in time. when verification Requests required for employment, further education, or other purposes, students may need to present physical copies of their certificate.

III. LITERATURE SURVEY

BLOCKCHAIN: The concept of blockchain was proposed by Satoshi Nakamoto in 2008. Blockchain is an online ledger that provides decentralized and transparent data sharing. With distributed recordings, all transaction data (stored in nodes) are compressed and added to different blocks. Data of various types are distributed in distinct blocks, enabling verifications to be made without the use of intermediaries. All the nodes then form a blockchain with timestamps. The data stored in each block can be verified simultaneously and become inalterable once entered. The whole process is open to the public, transparent, and secure. The emergence of Ethereum Smart Contracts in 2013 boosted blockchain technology, which became blockchain 2.0. As presented in blockchain 1.0 was mainly adopted by Bitcoin to solve problems concerning cryptocurrencies and decentralized payments. Blockchain 2.0 focused on decentralizing the entire market and is employed to transform assets through smart contracts, thereby creating value through the emergence of alternatives to Bitcoin.
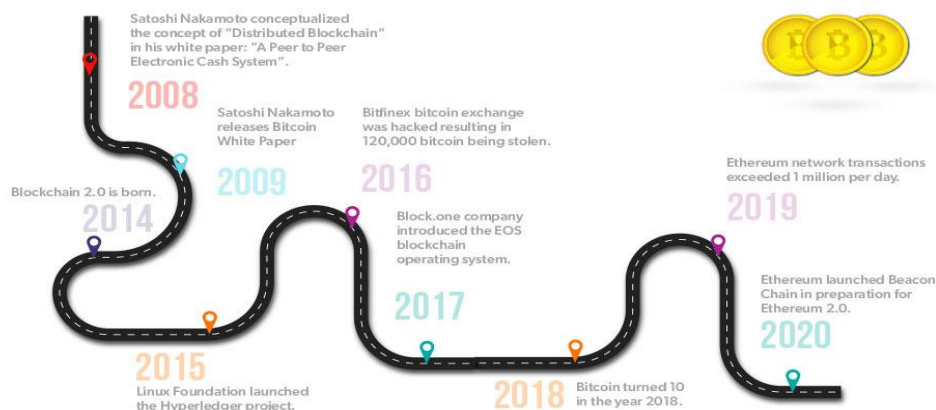
SMART CONTRACTS: Smart contracts were first proposed by Nick Szabo in the early 990s. He explained that a smart contract enabled computers to execute transaction clauses. As blockchain has become popular, smart contracts have received increased attention. Smart contracts are the main feature of Ethereum, a blockchain platform founded in 2015. A smart contract is "a digital contract that is written in source code and executed by computers, which integrates the tamper-proof mechanism of blockchain". Smart contracts can be created using the Ethereum blockchain. Developers are able, according to their needs, to specify any instruction in smart contracts; develop various types of applications, including those that interact with other contracts; store data; and transfer Ethers. Additionally, smart contracts that are deployed in blockchains are copied to each node to prevent contract tampering

IV.PROPOSED SYSTEM

Companies today are looking for the best and are recruiting only the 'cream of the crop'. Since certificate storage and its security is a matter of concern to the university, students, and employers, the proposed system provides a platform to store and verify the student credentials using blockchain technology. By adopting to Blockchain, colleges can now ensure their students are not only qualified and skilled, but also verified and are job-ready. It is imperative for any organization to hire genuine candidates with valid education and authentic degrees. Certificate Verification system closer analysis of the original copy of certificates provided by a student. Through blockchain to check the genuineness of the certificates and student. Each and everything are digitalized in which the certificate of SSLC, HSC, and academic certificate are digitalized in the educational institution and provided to the students. Then the certificates are store in blockchain. By using blockchain technology we can provide a more secure and efficient digital certificate validation. The proposed concept is based on decentralisation and an opensource strategy. There is no single entity that controls the system or the blockchain. The architecture consists of three essential parts:

BLOCKCHAIN AS A DATABASE

The database (blockchain) does not store any personal data; it only stores public keys, hashes10 and references to public institutions such as schools and universities. Because it operates multiple nodes, it is fail-safe and can withstand attacks. As envisaged by the authors of this white paper, the infrastructure would be operated by a consortium of municipal and public data centres. This would make it easier to secure and thus increase confidence in the system. The blockchain is private and access-protected. Certificate files are checked by certificate holders or users via the web service provided or interfaces that interact with one or more blockchain nodes. The system benefits from the known advantages of a blockchain (forgery protection, immutability, etc.) and at the same time avoids the disadvantages of completely public blockchain infrastructures (e.g., increased power consumption due to methods for building trust). The envisaged infrastructure does not offer crypto money that can be used speculatively. The costs for operating the blockchain are comparable to those of other distributed IT systems and also blockchain technology implement using SHA-256 algorithm.
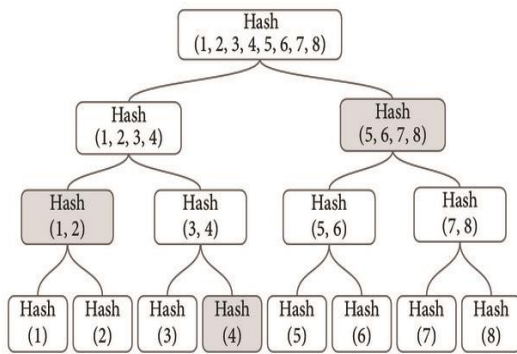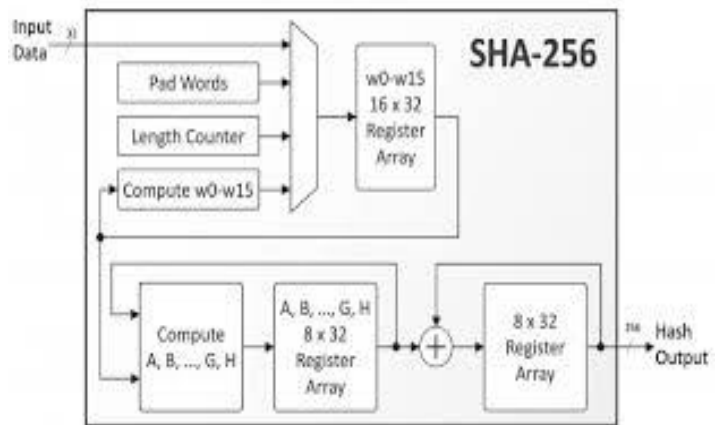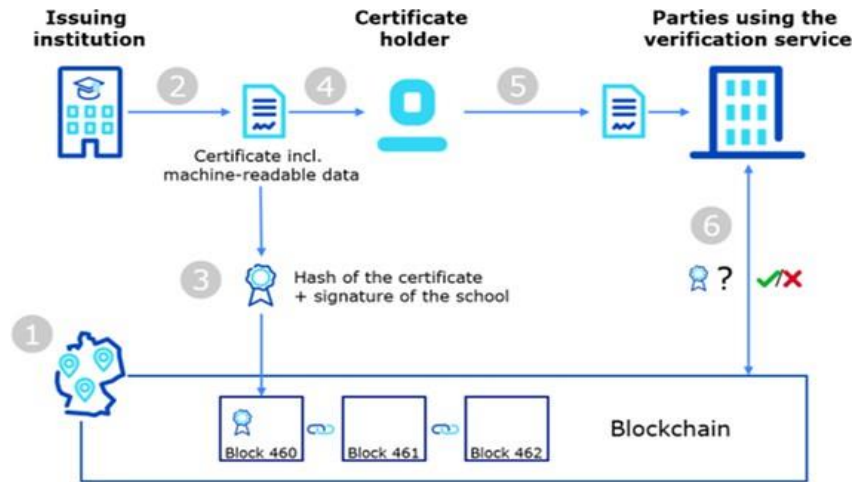

Fig 1: Hash value

Fig 2: SHA-256

WEB CLIENT FOR CREATING CERTIFICATES

Certificates are generated via a web service that can either run in the browser in the issuing institution or be integrated into an existing system via an interface. If required, the web service can be integrated into a client program.
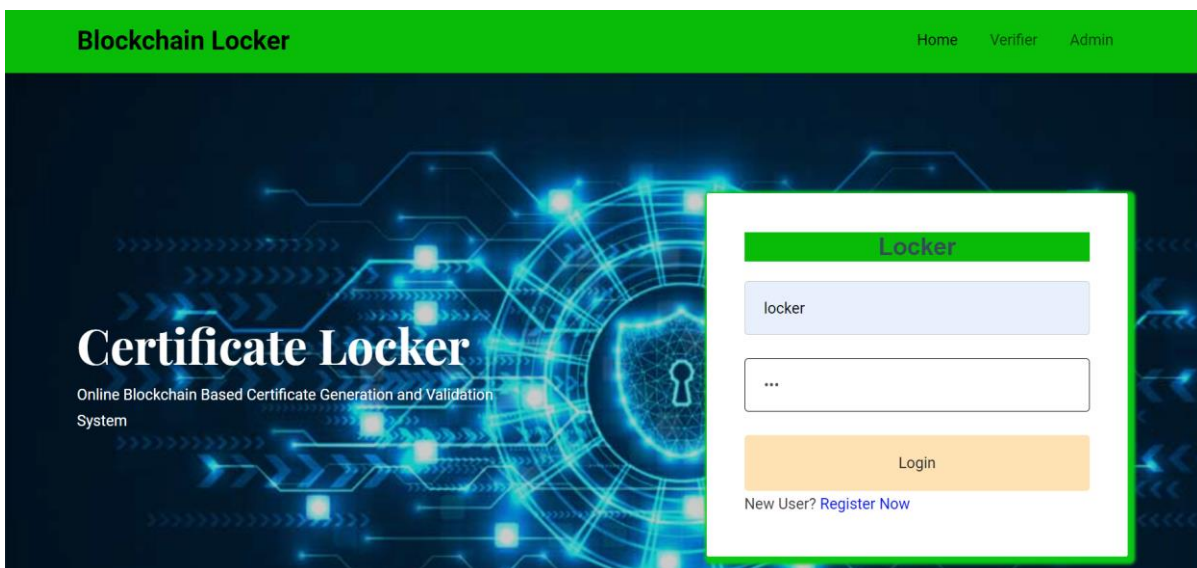
The web service can only be accessed by authorised institutions whose identity and authorisation to issue certificates has been confirmed by overarching authorities. The digital certificates created in this manner are transferred to the certificate holder securely. The current concept does not provide for the storage of the digital certificate file (either centrally or at the issuing institution). If, in the future, legislators impose requirements for the digital archiving of certificates, these can be easily implemented within the present concept.

WEB SERVICE FOR CHECKING CERTIFICATE

A publicly accessible web service shall be provided to verify the authenticity and integrity of certificate files. This web service can be used by anyone who has a certificate file, that is, by the certificate holder themselves and all third persons and institutions to whom the certificate holder submits their digital certificate file. By presenting the file, the hash value is calculated in the browser and checked for its presence in the blockchain. The certificate itself does not leave the browser. While there may be various causes for the result of the checking process to be negative (hash not written in the blockchain, file manipulation, etc.), a positive result confirms without doubt the document's authenticity and integrity as well as the issuing institution.

V.RESULT

SCREENSHOT:

OUTCOMES: To create the blockchain based unmodifiable certificates, initially the user needs to get registered. Any transaction can be sent through the wallet address of the Registered user mail. Only the owner of the smart contract has the authority to modify. Once added the user, will be able to access the system and can create Certificates with data fields. Each created certificate will be stored in the Inter planetary file system (IPFS). It will then return the unique hash generated using SHA-256 algorithm. This will serve as unique identity for each document his generated hash and detail of certificates will be stored in the blockchain and the student will be provided with the resultant transaction id. Anyone can use this transaction id to verify the certificate details and can view the original copy of certificate using IPFS hash stored along with data. And it is not using the same data. Hence with this we can solve the problem of certificate forgery.

VI.CONCLUSION

Data security is one of the major features of blockchain technology. Blockchain is a large and open-access online ledger in which each node saves and verifies the same data. Using the proposed blockchain-based system reduces the likelihood of certificate forgery. The process of certificate application and automated certificate granting are open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In conclusion, the system assures information accuracy and security. The project aims to address the inefficiencies and challenges present in traditional credential verification systems by leveraging blockchain technology to create a decentralized Student Certificate Verification platform.

REFERENCES

1. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture Consensus and Future Trends", 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557-564, 2017.
2. Dylan Yaga, Peter Mell, Nik Roby and Karen Scarfone, "Blockchain Technology Overview", 2019 National Institute of Standards and Technology Cryptography and Security.
3. A Alammary, S Alhazmi, M Almasri and S. Gillani, "Blockchain-Based Applications in Education: A Systematic Review", Applied Sciences, vol. 9, no. 12, pp. 2400, 2019, [online] Available: https://doi.org/10.3390/app9122400.
4. Q. Zheng, Y. Li, P. Chen and X. Dong, "An Innovative IPFS-Based Storage Model for Blockchain", 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), pp. 704-708, 2018.
5. M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform", IEEE Access, vol. 6, pp. 5112- 5127, 2018.
6. H. Li and D. Han, "EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme", IEEE Access, vol. 7, pp. 179273-179289, 2019.
7. Emanuel Estrela Bessa and Joberto Martins, "A Blockchain-based Educational Record Repository", 2019 CoRR abs 1904.00315.

8. Alkouz, A. HaiYasien, A. Alarabeyyat, K. Samara and M. Al-Saleh, "EPPR: Using Blockchain For Sharing Educational Records" in 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, pp. 234-239, 2019.

9. T. Kanan, A. T. Obaidat and M. Al-Lahham, "SmartCert BlockChain Imperative for Educational Certificates", 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 629-633, 2019.

10. Yaoqing Liu, Guchuan Sun and Stephanie. Schuckers, "Enabling Secure and PrivacyPreserving Identity Management via Smart Contract", pp. 1-8, 2019.

INTERNATIONAL JOURNAL OF

MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY