JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURING DIGITAL CERTIFICATE BY BLOCKCHAIN TECHNOLOGY

[1]Sindiri Sameera, [2]Satish Chandra Palli, [3]Muddadam Sai Santhosh, [4] Bellala Sai Deexitha, [5]Jada Anitha, [6]Pandu Ranga Vital Terlapu

[1]Student, [2]Student, [3]Student, [4]Student, [5]Student, [6]Guide

[1] Department of Computer Science & Engineering,

[1] Aditya Institute of Technology and Management, Tekkali-532201, India

Abstract : Digital certificates serve as essential cryptographic tools in securing online transactions and communications by verifying the identities of parties involved. The main goal of this project is to make digital certificates more secure using blockchain technology. Digital certificates are important for verifying things like education degrees, medical records, and financial transactions. However, current methods can be vulnerable to fraud and tampering. We use blockchain technology, which is a decentralized and tamper-proof system. Digital certificates will be stored on the blockchain, making them impossible to alter. Smart contracts will automate the verification process, making it faster and more reliable. By using a decentralized approach, we can eliminate single points of failure and make the whole system more trustworthy. In the future, we'll expand the system to handle different types of certificates and work on making it compatible with existing systems. We'll also research ways to make the blockchain system work for large-scale use. Continuous improvements will be made to keep up with changes in technology and security threats.

Keywords **-** Digital Certificates, Blockchain technology, Verification, Vulnerable, Security, Trust, Tampering, Fraud.

I. INTRODUCTION

Digital certificates play a pivotal role in the modern digital landscape, serving as cryptographic instruments that verify the authenticity and integrity of online transactions, communications, and identities. These certificates, based on the principles of public key infrastructure (PKI), provide a mechanism for securely exchanging sensitive information over the internet by using asymmetric cryptography. However, dependent on centralized certification authorities (CAs) for issuing and validating digital certificates introduces inherent sensitivities to fraud, manipulation, and single points of failure.

Traditional methods of certificate verification involve trusting a hierarchical chain of CAs to verify the authenticity of digital certificates. While this approach has been widely adopted and standardized, recent high-profile incidents of CA agreement and certificate-related fraud have underscored its limitations. Centralized CAs are open to various threats, including insider attacks, external breaches, which can damage strongest matches of digital certificates and agreement of the security of online transactions.

In response to these challenges, researchers and industry experts have increasingly turned to blockchain technology as a potential solution to enhance the security and reliability of digital certificate verification. Blockchain, originally termed as the underlying technology behind cryptocurrencies like Bitcoin, offers a decentralized and immutable ledger for recording transactions. By distributing certificate-related data across a network of nodes and cryptographically linking each transaction in a sequential chain of blocks, blockchain provides a tamper-proof and transparent mechanism for managing digital certificates.

The integration of blockchain technology into certificate verification processes holds the promise of addressing several longstanding issues in PKI-based systems.

Blockchain's decentralized nature eliminates the need for centralized CAs, reducing the risk of single points of failure and enhancing the strength of certificate management infrastructure. Moreover, blockchain's immutable ledger ensures the integrity and transparency of certificate transactions, mitigating the risk of certificate tampering and fraud.

This paper aims to provide a comprehensive review and analysis of the application of blockchain technology in verifying and validating digital certificates. We explore the underlying principles of blockchain technology, its advantages in certificate verification, and the challenges associated with its implementation. Furthermore, we discuss various integration strategies and

frameworks for incorporating blockchain into certificate verification processes, highlighting existing approaches, case studies, and future research directions.

In summary, blockchain technology offers significant potential in the field of digital certificate verification by providing a decentralized, transparent, and tamper-proof infrastructure. By using the blockchain's unique features, organizations can enhance the security, trustworthiness, and efficiency of digital transactions and communications in an increasingly interconnected world.

II. LITRATURE SURVEY

Author Jiin-Chiou Cheng et al. suggested a model that is executed by the EVM and progrAMMED ON THE ETHEREUM PLATFORM. There are three different kinds of users in this concept. The first of these is a service provider who is in charge of system upkeep. A certification unit that issues certificates is the second one. Students who meet specified conditions make up the third group. Each pupil receives a QR code and a serial number from this GUI-based approach. All data is verified by the system before being added to the Blockchain[1].

Author A Gayathiri et al. suggested utilising a mobile application to validate certificates. The authors employed methods to create a digital image of certificate paper from an analogue one. After that, certificates are saved in the Blockchain and a hash value is generated. In this method, the mobile application that provides digital certificates hanDLES CERTIFICATE VALIDATION[2]. Author Padmavati E Gundgurti et al. explains how to validate secure certificates using a graphical user interface (GUI) and Remix, Solidity smart contracts, and metamask. Students must first log into the system to begin this process in order to request a certificate. After confirming all the information, the issuer approves the request. Users come in two varieties: administrators and students. The administrator is responsible for block-level data storage, certificate issuance, and hash transmission to students. Pupils have the option to request a certificate[3].

Jing Chen et al. have offered a strategy for an efficient blockchain-based certificate audit. To construct a certificate management system, the author designed a blockchain architecture consisting of four layers: the data layer, network layer, extension layer, and application layer.The main programmes are written in Javascript (node.js), HTML, CSS, PHP, and Ethereum.In the system model, there are four different kinds of entities: clients, domains, CAs, and bookkeepers[4]. The Author Fernando Richter Vidal et al . provides a revocation mechanism that enables certificates to be kept on the Blockchain. This system creates a trash area to verify the input state and stores revocation data on the Blockchain using Blockcerts Version 1.0. This creates a trash area and verifies the input status. Connecting a certificate hash to a JSON-formatted companion file in order to send a distributed resource, such as IPFS. The 32-length hash is generated by SHA-256. The two-time payment scheme for each revocation is the restrion of this technology, which makes Blockcert Version 1.0 extremely expensive[5].

Author Ze Wang et al. suggested a system prototype that is used with Nginx and Firefox. It records certificates and keeps track of their revocation status on the worldwide Blockchain. The bulk of P2P nodes in this paradigm measure certificate validity. However, this adds no official security proof, and that is the system's shortcoming[6].

Author SHIXION YAO et al. suggested a blockchain-based certificate status validation approach that primarily addresses two problems. One involves separating the control and storage planes of revoked certificates, and another involves creating a covert response to protect clients' privacy. The author maintained a Merkle hash tree and employed PKI to accomplish this type of task. It works incredibly well for security analysis and experimental evolution[7]. As a blockchain model for certification of completion certificate, the creation of a certification procedure was suggested. There will be less chance of certificate forgeries, and certificates will be more legitimate, secure, and secret[8].

Dasgupta et al. centred on security concerns using appropriate BC technology. The authors also provided future projects and advice regarding BC issues for researchers of the next generation, in addition to highlighting a few hacks in the susceptible system. This paper's primary focus is on the application of BC technology in the field of education. Therefore, the purpose of this article is to verify certification using BC. Numerous scholars used BC in the field of education, particularly with regard to certificate verification[9]. Chen et al. suggested a design for a BC-based public, effective certificate auditing system. They appropriately termed their superb data structure "CertOper," which aids in maintaining traceability and public audit in the BC. The first university to keep academic credentials on the Bitcoin BC was the University of Nicosia[10].

The literature reviewed underscores the transformative potential of blockchain technology in revolutionizing the verification and validation of digital certificates. The combination of decentralized trust, cryptographic security, and smart contract automation creates a robust framework that addresses the shortcomings of traditional systems. The upcoming project aligns with and extends the findings in this literature review, contributing to the ongoing discourse on securing digital credentials in the contemporary digital landscape.

2.1 Blockchain in Education System

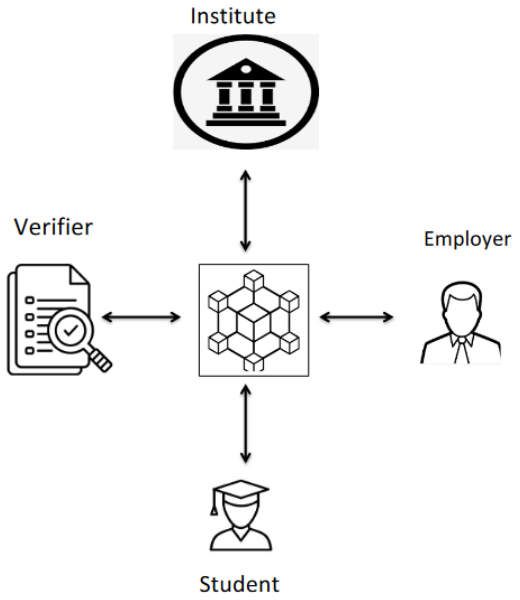

Fig.1 Blockchain in Education system

A blockchain can be used to store and distribute academic data, degrees, and certifications, in the context of education. Three people are in the diagram as part of a blockchain education system. Student is the owner of their educational data. An institute is responsible for issuing the certificates. An verifier is a person who can confirm the authenticity of academic qualifications. The student in the diagram has a record on the blockchain proving they were awarded a credential by the institution whereas the verifier can verify the authenticity of the credential using the blockchain.

2.2 Blockchain technology for certificate validation

Blockchain technology, originally conceived as the base structure for cryptocurrencies like Bitcoin, has garnered significant attention for its potential applications beyond digital currencies. At its core, a blockchain is a decentralized and immutable ledger that records transactions across a network of computers, or nodes, in a tamper-proof and transparent manner. Each transaction is cryptographically linked to the previous one, forming a chain of blocks that cannot be altered retroactively without consensus from the majority of the network.

In the context of certificate verification, blockchain offers several advantages over traditional PKI-based systems. One of the key benefits is decentralization, which eliminates the need for centralized certificate authorities (CAs) and reduces the risk of single points of failure. Instead of relying on a hierarchical chain of trust, blockchain distributes certificate-related data across a network of nodes, with each node maintaining a copy of the entire ledger. This distributed architecture enhances the resilience and security of certificate management infrastructure by eliminating the dependency on any single authority.

Immutability is another fundamental characteristic of blockchain that enhances the integrity and trustworthiness of certificate verification processes. Once a transaction is recorded on the blockchain, it becomes virtually impossible to alter or delete it without consensus from the majority of the network. This immutability feature ensures that certificate- related data remains tamper-proof and verifiable, mitigating the risk of certificate forgery or tampering.

Consensus mechanisms, such as proof of work (PoW) or proof of stake (PoS), ensure the integrity and security of the blockchain by validating and adding new transactions to the ledger through a process known as mining or forging. In the context of certificate verification, consensus mechanisms play a crucial role in ensuring that only valid certificate transactions are recorded on the blockchain, thereby preventing unauthorized modifications orfraudulent activities.

Integration of blockchain into certificate verification processes involves designing and implementing suitable architectures and protocols that leverage blockchain's unique features while ensuring compatibility with existing PKI infrastructure. Several approaches have been proposed, ranging from fully decentralized blockchain networks to hybrid models that combine blockchain with traditional PKI systems.

Overall, blockchain technology offers significant potential to revolutionize certificate verification by providing a decentralized, transparent, and tamper-proof infrastructure. By leveraging blockchain's unique features, organizations can enhance the security, trustworthiness, and efficiency of digital transactions and communications, paving the way for a more secure and resilient digital ecosystem.

III. METHODOLOGY

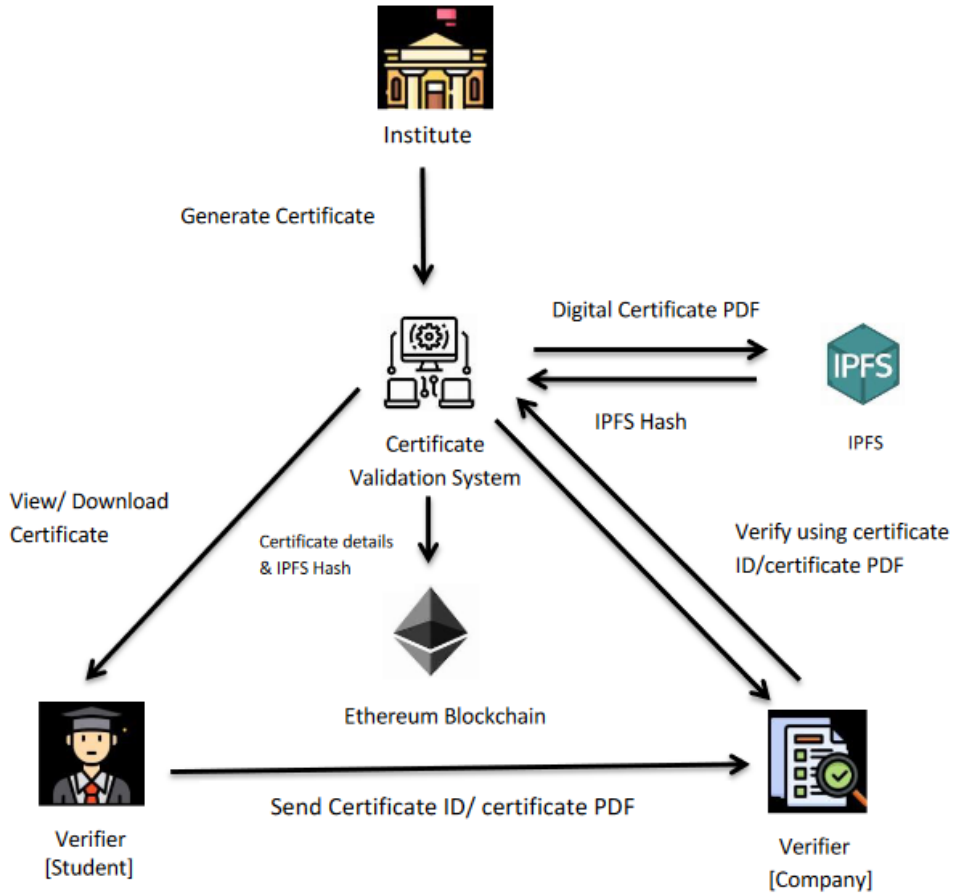

Fig 2. System Architecture for Securing, verifying and validating digital certificate

This image depicts a blockchain-based certificate verification and validation system. The institute generates a digital certificate in PDF format. The certificate is uploaded to the Inter Planetary File System (IPFS), a peer-to-peer network for storing and sharing data. A unique hash is created to identify the certificate stored on IPFS. The certificate details and the IPFS hash are recorded on the Ethereum blockchain. The student receives a digital copy of the certificate and a certificate ID. To verify the certificate, a potential employer or institution can use the certificate ID or the PDF itself. The verification system checks the blockchain ledger for the certificate ID or the hash from the PDF. If the information matches what's on the blockchain, the certificate is deemed valid.

3.1. Registration

In this system, the student or the verifier need to register in this blockchain based certificate system for the further process. After the registration is completed, student has the ability to view their certificate inorder to verify their credentials. The verifier has the ability to verify the credentials of the student.

3.2. Authentication

Authentication is the procedure by which the student confirms their identification in order to obtain access to the blockchain-based education system. Usually, this ensures by giving login credentials, like a username and password, which are safely kept and verified using the system's database. By ensuring that only those with permission can access a student's certificate or the credentials, authentication guards against unauthorised access to private information.

3.3. Smart Contract Execution

```
contract Certification {
    struct Certificate {
        string uid;
        string candidate_name;
        string course_name;
        string org_name;
        string ipfs_hash;
    }
```

Fig 3: Declaring state variables and defining the structure of a certification

This figure is a structure known as a Certificate is defined in this contract. There are five fields in this structure. uid, candidate_name, course_name, org_name, and ipfs_hash are among them. The string "uid" most likely serves as the certificate's unique identification. "candidate_name" is a string containing the name of the certificate recipient. a string containing the name of the program or course for which the certificate was obtained. The name of the college that provided the certificate is kept in a string called course_name. A hash of the certificate document, most likely kept on the Inter Planetary File System (IPFS), is saved in a string called ipfs_hash. A peer-to-peer network called IPFS is used for data sharing and storing.

```
function generateCertificate(
    string memory _certificate_id,
    string memory _uid,
    string memory _candidate_name,
    string memory _course_name,
    string memory _org_name,
    string memory _ipfs_hash
) public {
```

Fig 4: Function to generate a certificate

generateCertificate is the name of the function. The function takes six arguments. They are memory _certificate_id, memory _uid, memory _candidate_name, memory_course_name, memory _org_name, memory _ipfs_hash.

- memory _certificate_id is a string that likely represents a unique identifier for the certificate.
- memory _uid is a string that likely stores a unique identifier for the user.
- memory _candidate_name is a string that stores the name of the person who earned the certificate.
- memory _course_name is a string that stores the name of the course or program the certificate was issued.
- memory _org_name is a string that stores the name of the organization that issued the certificate.
- memory _ipfs_hash is a string that stores a hash of the certificate document, likely stored on the InterPlanetary File System (IPFS). IPFS is a peer-to-peer network for storing and sharing data.

3.4. Verification

```
    function isVerified(
        string memory _certificate_id
    ) public view returns (bool) {
        return bytes(certificates[_certificate_id].ipfs_hash).length != 0;
    }
}
```

Fig 5: Function to verify the validate a certificate

This function isVerified is used to verify and to validate the certificates of a person. The function takes a string argument called _certificate_id which is likely a unique identifier for a certificate. The function then checks if the length of the ipfs_hash property of the certificate identified by _certificate_id is greater than zero. If the length is greater than zero, then the certificate is considered valid and the function returns true. Otherwise, the function returns false.

- string memory _certificate_id is a line that declares a variable called _certificate_id of type string memory. This variable will store the identifier of the certificate that we want to verify.
- "return bytes(certificates[_certificate_id].ipfs_hash).length != 0;" is core of the function. It checks if the length of the ipfs_hash property of the certificate identified by _certificate_id is greater than zero.

IV. IMPLEMENTATION

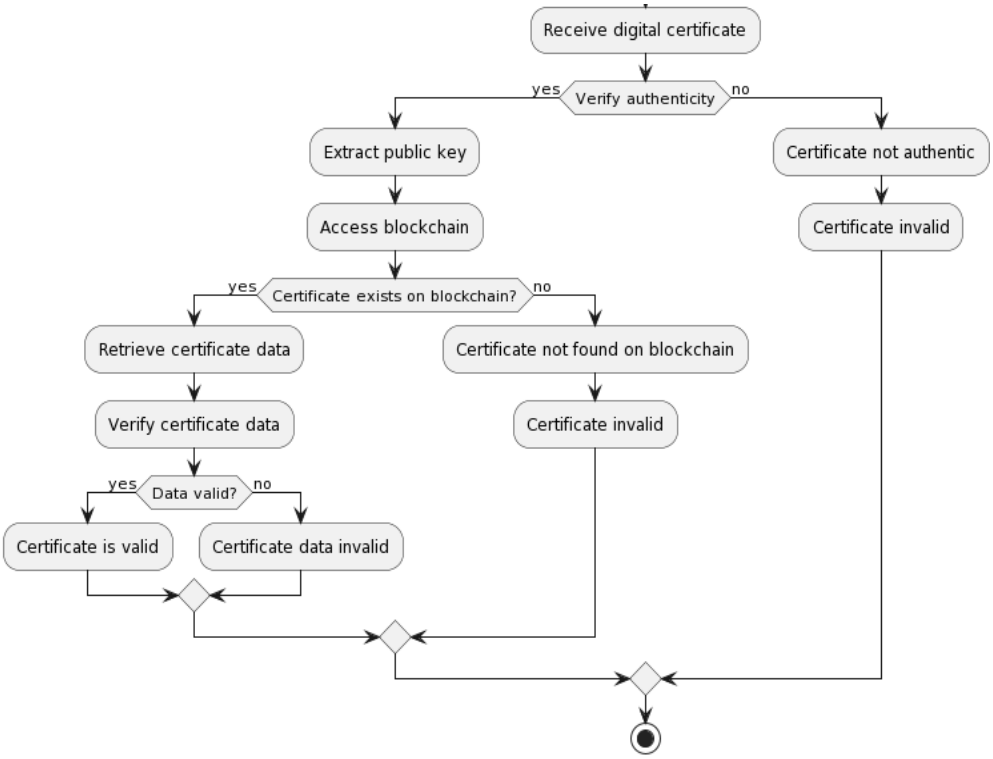

Fig 6: Work flow diagram to verify and to validate the digital certificate

This work flow diagram shows the process of verifying the authenticity of a digital certificate. Receiving a digital certificate is the starting point of the process. Verify authenticity is then split into two paths, depending on whether the authenticity of the certificate needs to be verified. Extract public key (Yes path) is used if the authenticity needs to be verified, the first step is to extract the public key from the certificate. The public key is used to verify the digital signature of the certificate. Access blockchain (Yes path) is that checks if the certificate's authenticity can be verified using a blockchain. Does certificate exists on blockchain? (Yes path) is used if a blockchain is being used, checks whether the certificate exists on the blockchain.

Retrieve certificate data (Yes path) checks if the certificate is found on the blockchain, the certificate data is retrieved. Verify certificate data (Yes path) checks if the certificate data is then verified. This may involve checking the certificate's signature and validity period. Data valid? (Yes path) checks if the certificate data is valid, the certificate is considered to be authentic. Certificate not authentic (Various No paths) checks if any of the checks fail, the certificate is considered to be not authentic. Certificate is valid (Yes path) if the end point for a valid certificate. This workflow diagram does not specify how the certificate is received or how the public key is used to verify the certificate's signature.

These details would depend on the specific system or application that is using the certificates.

V. RESULTS AND DISCUSSIONS

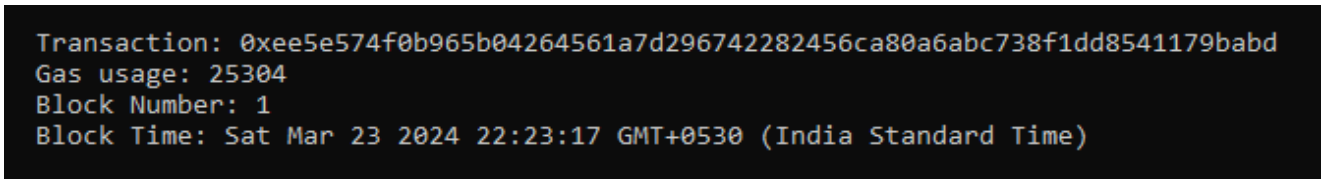

Fig 7: Creation of a block

Transaction is the line likely refers to a transaction hash on the Ethereum blockchain. Gas usage is the line indicates the amount of computational effort required to execute the smart contract or transaction on the blockchain. In this case, it consumed 25304 units of gas. Block Number refers to the block number on the blockchain where the transaction is recorded. Block 1 is might be an initial test on a private blockchain. Block Time is the line shows the date and time the block was added to the blockchain, which is Saturday, March 23, 2024, at 10:23 PM IST.

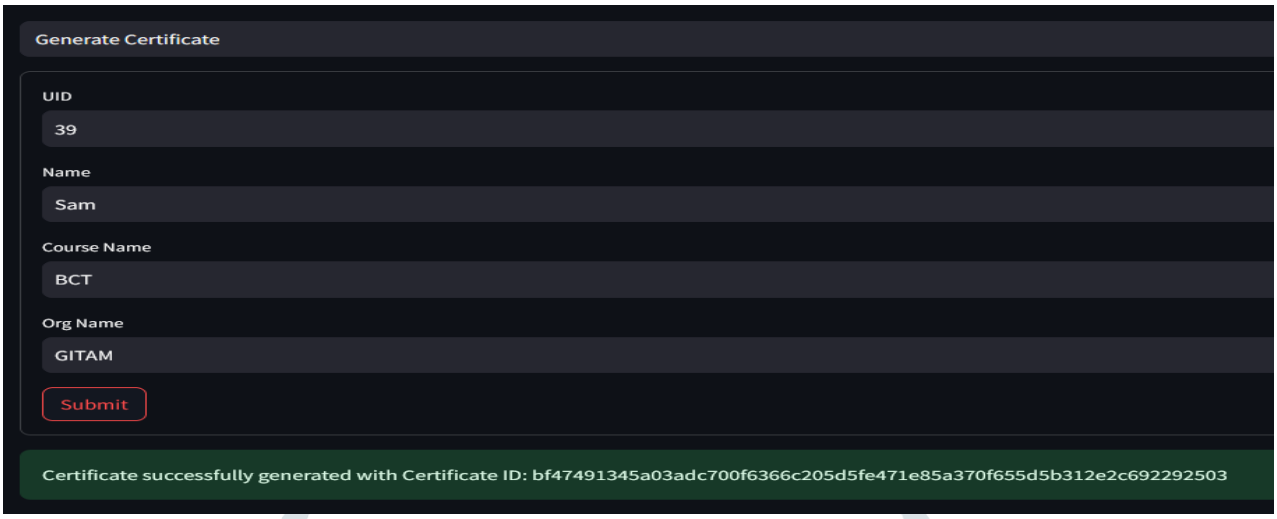

Fig 8 : Certificate Generated with Hash Value

This figure shows how the certificate is generated with unique hash value.

Fig 9: Certificate verified by ID

Fig 10: Certificate verified by uploading PDF

Verify certificate using certificate ID:

This column is in the Verifier column which is present on the home page. This column is used to verify the certificate using the certificate Id.

- If the certificate id is in the blockchain then message is generated like **certificate validated successfully**.
- If the certificate id is not in the blockchain then the error message is generated like **certificate might be tampered.**

Verify certificate by uploading certificate PDF:

This page is used to verify the certificate by uploading certificate pdf.

- If the certificate id is in the blockchain then message is generated like **certificate validated successfully.**
- If the certificate id is not in the blockchain then the error message is generated like **certificate might be tampered.**

VI. CONCLUSION

Currently, the internet is how we share information. We also communicate information in other fields (like education, where the institution has total authority) using centralized systems. Thanks to blockchain technology, this "middleman/central authority" can be eliminated. It does this by carrying out three vital tasks: generating contracts, confirming identities, and recording transactions. In conclusion, this project represents a significant step towards enhancing the security, transparency, and efficiency of certificate verification processes. The utilization of blockchain technology introduces a decentralized and tamper-resistant framework, ensuring the integrity and authenticity of digital certificates. In this project by using several cryptographic algorithms, security is enhanced.

REFERENCES

[1]. J. Cheng, N. Lee, C. Chi and Y. 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.

[2]. 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/IC-SSS49621.2020.9201988.

[3]. P. E. Gundgurti, K. Alluri, P. E. Gundgurti, S. Harika K. and G. Vaishnavi,” Smart and Secure Certificate Validation System through Blockchain,” 2020 Second International Conference on Inventive Re-search in Computing Applications (ICIRCA), Coimbatore, India, 2020, pp. 862-868, doi: 10.1109/ICIRCA48905.2020.9182975.

[4]. J. Chen, S. Yao, Q. Yuan, K. He, S. Ji and R. Du, ”CertChain: Public and Efficient Certificate Audit Based on Blockchain for TLS Connections,” IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, Honolulu, HI, USA, 2018, pp. 2060-2068.

[5]. F. R. Vidal, F. Gouveia and C. Soares, ”Revocation Mechanisms for Academic Certificates Stored on a Blockchain,” 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), Seville, Spain, 2020, pp. 1-6.

[6]. 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.

[7]. S. Yao, J. Chen, K. He, R. Du, T. Zhu and X. Chen, ”PBCert: Privacy- Preserving Blockchain-Based Certificate Status Validation Toward Mass Storage Management,” in IEEE Access, vol. 7.

[8]. Priya, Shanmuga. “Online Certificate Validation Using Blockchain.” (2019).

[9]. D. Dasgupta, J. M. Shrein, and K. D. Gupta, “A survey of blockchain from security perspective,” Journal of Banking and Financial Technology, vol. 3, no. 1, pp. 1–17, 2019.

[10]. J. Chen, S. Yao, Q. Yuan, K. He, S. Ji, and R. Du, “Certchain: Public and efficient certificate audit based on blockchain for tls connections,” in IEEE INFOCOM 2018-IEEE Conference on Computer Communications. IEEE, 2018, pp. 2060–2068.