



**BLOCKCHAIN-ENABLED SYSTEM FOR SECURE CERTIFICATE
VALIDATION**

G. Pushpa¹, B. Bhargavi², J. Kavitha³

¹ Assoc. Professor, Department of Computer Applications, Aurora's PG College (MBA),
Uppal, Hyderabad
Email: gunde.latha@gmail.com

² Assistant Professor, Department of Computer Applications, Aurora's PG College (MBA),
Uppal, Hyderabad
Email: burrabhargavi@gmail.com

³ Assistant Professor, Department of Computer Applications, Aurora's PG College (MBA),
Uppal, Hyderabad
Email: kavithajilla@gmail.com

ABSTRACT

In order to secure academic credentials, ensure accurate maintenance, and stop certificate counterfeiting, we are transforming all certificates into digital signatures as part of this project. A blockchain server will be used to store this digital signature since it allows for tamper-proof data storage, which ensures that no one can hack or change the data. In the unlikely event that the data changes, verification will be unsuccessful at the following block storage, and the user may be notified of the change. Blockchain technology saves similar transaction data across several servers with hash code verification. The hash code will change, so if data is changed on one server, it will be detected on the other. For example, data is kept across numerous servers with Blockchain technology. The hash code will alter on one server if malevolent people make changes to the data there, but it will stay the same on the other servers. Verification will reveal this altered hash code, stopping any more dangerous user modifications. A fresh block of transaction data is uploaded to the blockchain and each piece of data is preserved by comparing it to previous hash codes. If the older hash codes remain unchanged, the data is considered original and unaltered. The hash code of each newly created data storage block will be verified.

Keywords: Hyper Ledger Fabric, Blockchain, Server, Secure, and Certificate Validation

1 INTRODUCTION

The academic world has long struggled with the problem of fake academic credentials. An effective technological strategy protecting authentic credential certification and reputation didn't emerge until the Massachusetts Institute of Technology Media Lab released their project of Block-certs, a method that is primarily implemented by fusing the hash value of



local files to the blockchain but still has many issues. Based on Blockcerts, a number of cryptographic fixes are suggested to address the aforementioned problems. These fixes include the implementation of a multi-signature scheme to improve certificate authentication, a safe revocation mechanism to increase the dependability of certificate revocation, and a secure federated identification to verify the identity of the issuing institution. The system that addressed the aforementioned problems was designed and put into operation as part of the project. The project also includes a thorough assessment of the system security, and the assessment results offer compelling proof that the implementation is workable, dependable, and secure. Additionally, they may provide some hints about crucial architectural considerations regarding the security characteristics of other blockchain-based systems. The implementation is covered in this part from the standpoints of system and database architecture. The database architecture and system architecture both demonstrate how the system was created from an engineering standpoint. The primary business logic, which covers certificate applying, examining, signing, and issuing, is handled by the issuing apps. The certificate's hash will be combined in a Merkle tree by the issuing applications, which will then send the Merkle root to Blockchain while the majority of the community members sign it. The cancellation of certificates was also a part of the applications for issue. The primary business logic, including applying for, reviewing, signing, and issuing certificates, is handled by the issuing applications. The certificate's hash and a Merkle tree are combined by the issuing software, which then sends the Merkle root to the Blockchain. The applications for issuing certificates also cover the cancellation of certifications. The verification application focuses on examining the validity and reliability of the given certifications. There are two main parts to it: an Android application and a web website. They employ the same approach and retrieve the transaction message via the blockchain API before comparing it to the verification information on the receipt. The mechanism can be summed up as follows: confirm the authenticity of the authentication code; validate the hash against the local certificate; confirm the hash is in the Merkle tree; confirm the Merkle root is in the blockchain; confirm the certificate has not been revoked; and confirm the certificate's expiration date. Additionally, it must be noted that for the sake of sharing the certifications, The Android-based application enables instant QR code scanning for document verification. The blockchain serves as a distributed database for storing the authentication data as well as the infrastructure of trust. The Merkle root, which is created using hashed information from thousands of certificates, typically makes up the authentication data. Since the MongoDB successfully supports JSON-based certificates and offers high availability and scalability, the MongoDB is used as our database.

The way that people live has changed as a result of developments in information technology, the widespread use of the Internet, and the widespread use of mobile devices. Digital coins known as virtual currency, which were initially created for usage online, are now widely used offline. The ease of the Internet has led to the growth of many virtual currencies, the most well-known of which are Bitcoin, Ether, and Ripple [2], the value of which has lately increased. The blockchain, the core technology behind these innovative currencies, is starting



to attract attention. Blockchain provides a decentralized, unchangeable database with great potential for a variety of uses. Blockchain is a decentralized database that's frequently used to log various transactions. Once various nodes have come to an agreement, A block that already contains records of numerous transactions is expanded by the transaction. The hash value of a block's most recent connection counterpart is contained in each block. A blockchain is created when all the blocks are connected to one another [1]. Data are decentralized because they are distributed among numerous nodes (the distributed data storage). As a result, the nodes jointly maintain the database. A block on the blockchain can only be considered validated once it has been checked by several

2.LITERATURE SURVEY AND RELATEDWORK

In order to grasp the current state of the art in this topic, a literature review on blockchain-based certificate validation would involve looking through research publications, papers, and other literature. As of my most recent knowledge update in September 2021, the important study areas, conclusions, and trends connected to blockchain-based certificate validation are summarized here. Please be aware that this field may have undergone significant changes since then.

1. An Overview of Blockchain Technology:
Give a brief introduction to blockchain technology, its underlying ideas, and how it relates to certificate validation to start your literature review.
2. Blockchain-Based Certificate Validation:
Review papers and publications that cover the topic of using blockchain technology to verify diplomas and credentials, such as academic degrees, professional certifications, and other credentials.
3. Security and Trust –
Studies on the security ramifications of blockchain-based certificate validation, including how blockchain ensures the integrity and immutability of certificate data. Think about publications that go over the function of trust in blockchain systems and how it affects certificate validation.
4. Decentralization:
Investigate the literature that outlines the benefits of decentralization in certificate validation, such as lowering the risk of fraud and offering a tamper-proof ledger of credentials.
5. Smart Contracts:
Review study on the application of smart contracts in blockchain-based certificate validation systems, focusing on their function in automating validation procedures.
6. Interoperability:
Read articles addressing the issues and potential solutions relating to communication between various blockchain networks or between blockchains and conventional certificate systems.



7. Privacy and Data Protection: -
Search for literature that discusses privacy issues with blockchain-based certificate validation, notably in conformity with GDPR and other data protection laws.
8. Case Studies: -
Examine real-world applications of blockchain-based certificate validation systems and case studies, highlighting successful initiatives and lessons gained.
9. Scalability:
Look at studies that examine the scaling issues with blockchain technology in the context of processing a lot of certificate validation transactions.
10. Regulatory Considerations: -
Research the legal and compliance problems related to the regulatory environment for blockchain-based certificate validation.
11. User Experience: -
Studies and papers that employ blockchain technology to improve user experience in certificate validation processes.
12. Future Trends and Challenges: -
Recognize new developments in blockchain-based certificate validation, including the incorporation of artificial intelligence and machine learning, governance structures, and sustainability issues.
13. Comparative Studies:
Evaluate the pros and cons of blockchain by reading research that contrasts blockchain-based certificate validation with conventional techniques or other technology.
14. Blockchain Platforms and Tools:
Research the various blockchain platforms and software development tools that can be used to create certificate validation solutions.
15. Standardization Efforts:
Investigate the efforts being made to standardize blockchain-based certificate validation in order to ensure compatibility and consistency amongst various implementations.
After my last knowledge update in September 2021, keep in mind to check for the most recent publications and research findings to keep your literature survey current. To provide a well-rounded and organized summary of the subject, you should also think about segmenting your survey into sections or themes.

3 PROPOSED WORK AND ALGORITHM

It takes too long to validate since the certificate is manually verified and kept in a centralized location. The certificates issued to any private sector (banks) are not secure. However, the data may be edited, destroyed, or amended. It is simple to compromise certificates and create copies of them. On the day of the interview, students bring their certificates. Certificates lack any security.

1. Blockchain network: Choose the blockchain type (public, private, or consortium) that best



meets your requirements. Consensus Mechanism: Select a consensus algorithm that satisfies your security and scalability criteria (such as proof of work or proof of stake).

Blockchain Platform: Decide on a blockchain platform that supports smart contracts and satisfies your technical needs (such as Ethereum or Hyper ledger Fabric).

2. Security: Data Encryption: Use robust encryption to safeguard the confidentiality of certificate data. Implement stringent access restrictions to make sure that only those with permission can interact with the blockchain. Immutability: Make sure that certificate documents, once they are put to the blockchain, cannot be changed Security consensus: Put strong security measures in place to defend against attacks, such as 51% attacks in proof-of-work networks.

3. Smart Contracts: Create and test smart contracts that specify the policies and logic governing certificate validation. Code Audit: To find vulnerabilities in smart contracts, conduct code audits and security assessments.

Gas expenses: When executing smart contracts, take into account gas costs (transaction fees) and make sure they are manageable.

4. User Authentication: Use secure user authentication techniques to confirm the legitimacy of people and organizations engaging with the system. Identity Management: User Authentication. Identity confirmation: To avoid fraud, confirm the recipients and issuers of certificates are who they claim to be.

5. User Interface: User-Friendly Interface: Create simple, user-friendly user interfaces (web or mobile) for certificate validation. Provide API integration so that outside systems can connect to the certificate validation system Six. Scalability Make sure the system can scale horizontally in order to accommodate an increasing volume of certificates and validation requests. Utilize load balancing techniques to evenly distribute traffic among servers or nodes. Performance optimization: Make blockchain interactions and database searches more effective. A blockchain-based certificate validation system should be designed and implemented based on these system requirements. To guarantee the system's dependability and security while meeting the needs of users and stakeholders, careful planning, testing, and continuing maintenance are essential. In order to ensure compliance with pertinent rules and regulations, you should also speak with legal professionals.

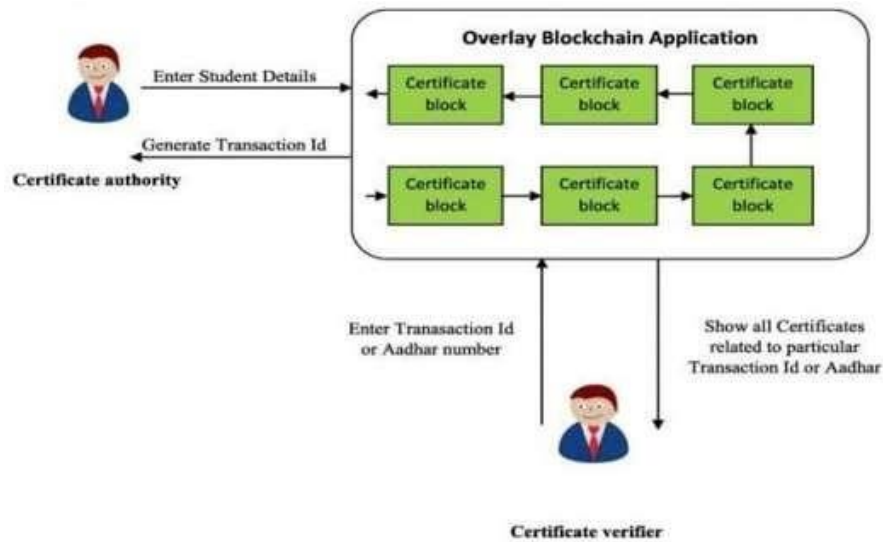


Fig-1: System Architecture

4 METHODOLOGIES

1. Save the certificate with a digital signature first:

With the use of this module, an admin user can upload student information and academic credentials. The application will then transform the credentials into digital signatures, and the signatures together with other student information will be recorded in a blockchain database.

2. Check the certificate:

In this module, the verifier, the company, or the administrator will collect the student's certificate and upload it to the application. The application will then convert the certificate into a digital signature, which will be checked at the Blockchain database. If a match is found, the blockchain will retrieve all the student's information and display it to the verifier; if not, the certificate will be deemed to be fake or forged.

5.RESULTS AND DISCUSSION

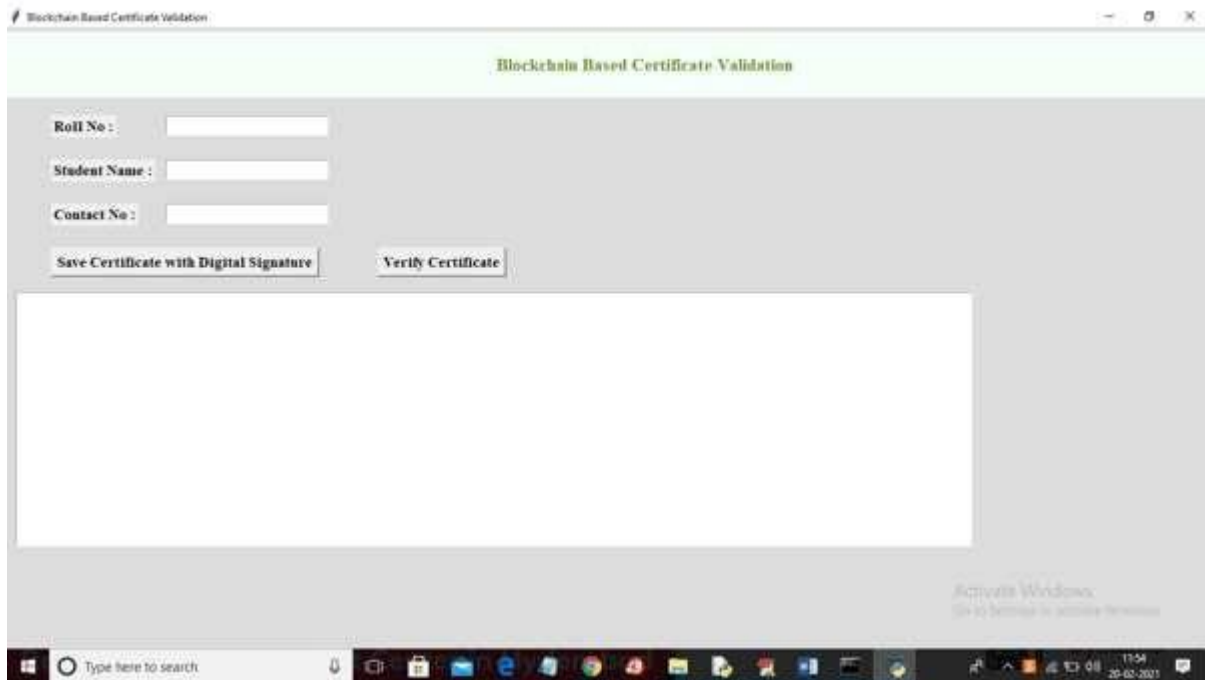


Fig 2:- Blockchain based certificate validation interface

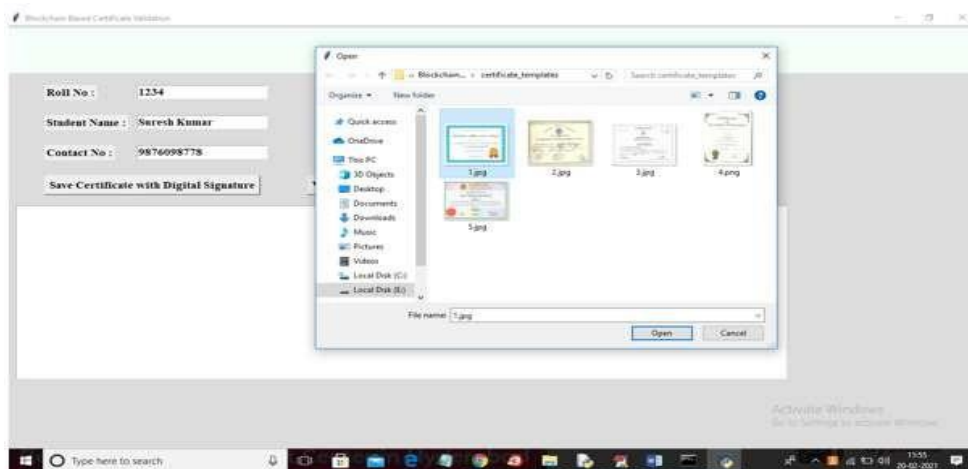


Fig 3:- Uploading the certificate

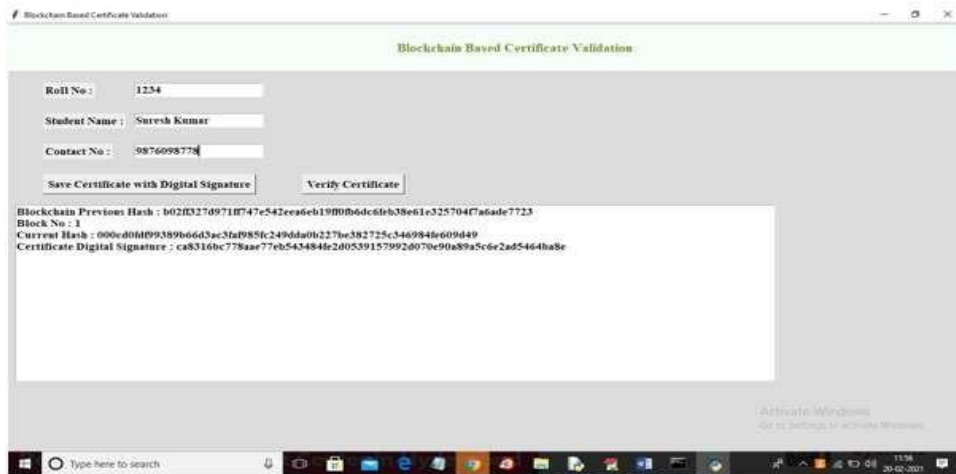


Fig 4 :- Saving certificate with digital signature

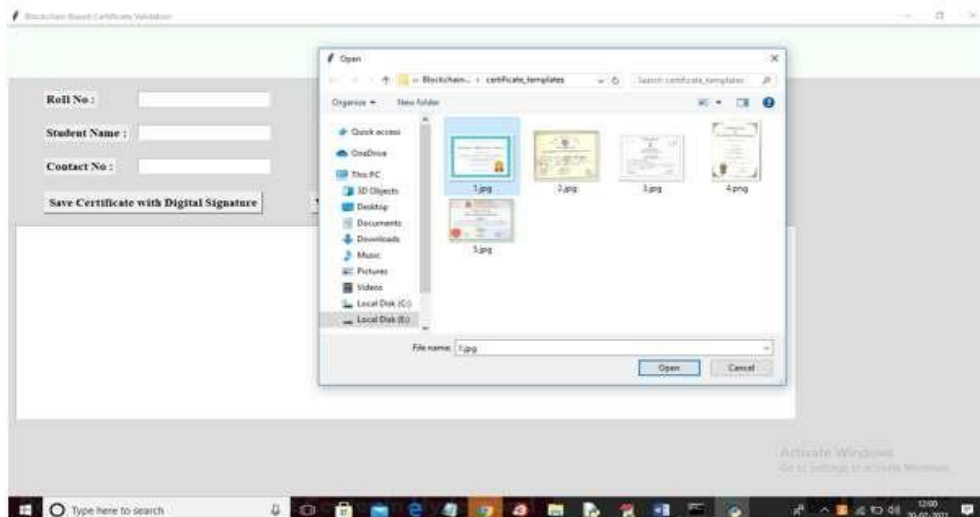


Fig 5 :- Uploading the certificate for validation

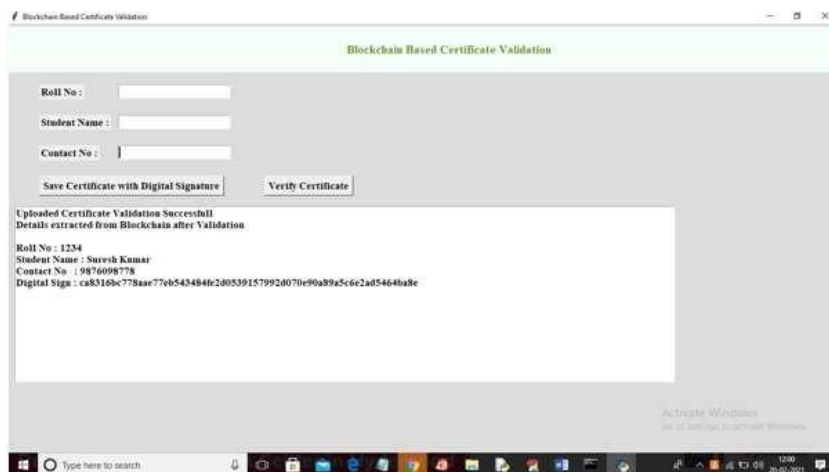


Fig 6 :- Getting details of the certificate

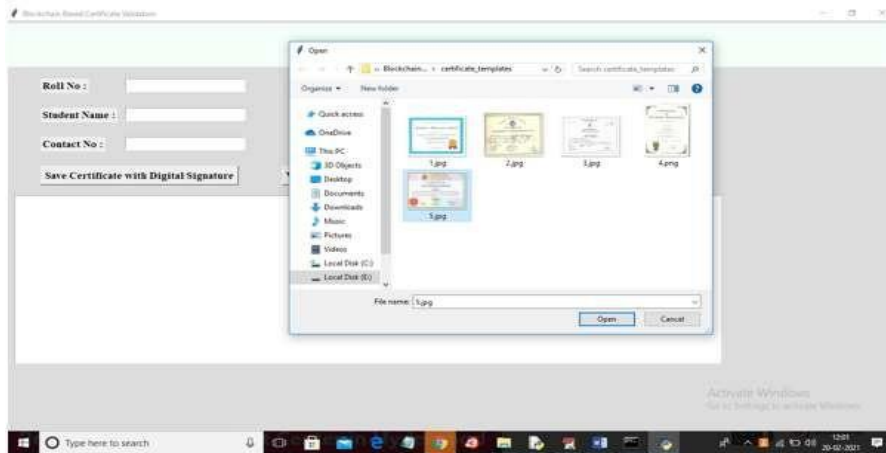


Fig 7 :- Uploading the certificate

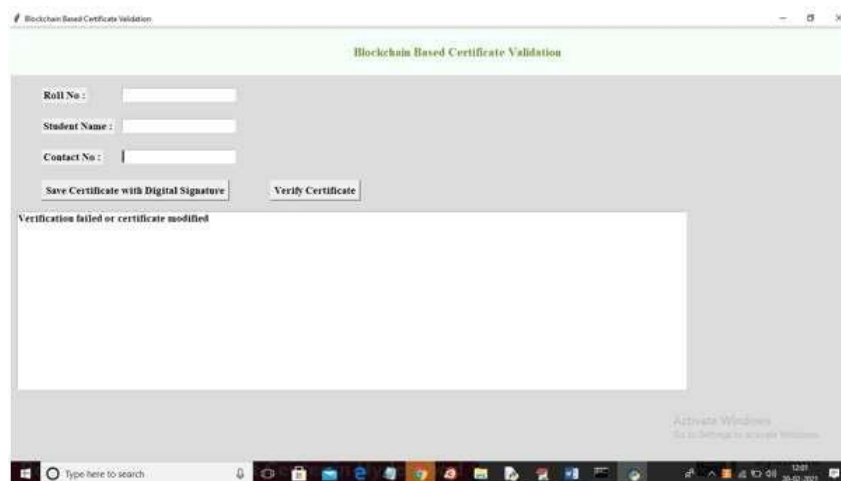


Fig 8 :- Getting the details of uploaded certificate as not valid

6. CONCLUSION

By comparison, the MIT Media Lab unveiled its blockchain-based credential system in June 2016, which is not dependent on third-party arbitration like current alternatives are. It is harder to forge, more dependable, and more secure. However, a weak revocation mechanism and a few serious authentication problems limit the project's prevalence and breadth. To get around these problems and improve the concept's viability, we created and constructed a number of innovative cryptographic protocols for our project, such as multi-signature, a trustworthy federated identification system, and a revocation mechanism based on the BTC address state.

Since the majority of the academic committee members must sign each progress report, the multi-signature approach among these protocols greatly increases the difficulty of forging.



Furthermore, it strengthens the security of the private key storage because different devices and people possess the private keys. The BTC-address-based revocation procedure further improved the stability of the certificate revocation because BTC addresses are dependable and constantly reachable. Furthermore, by using the same multi-signature technique that involves several signatories throughout the cancellation procedure, this tactic reduced the possibility that revocation would fail. Federated trustworthy identity was able to prove the authenticity of the certificate by effectively utilizing both the trusted path and federated identity. Our study's methodology can also be used to similar domains like digital right protection and contract proofing. For example, our protocol mitigates concerns about credential forging by enabling the two organizations to use multisignature to link their contract to the block chain instead of the traditional third-party-based work mode.

We also developed a blockchain-based certificate system that integrated all of the previously described protocols using Java and JavaScript. The problem with Blockcerts has been largely resolved by this method, improving the viability of the idea of a blockchain-based certificate. Lastly, we conducted several security assessments from the perspectives of network security, protocol security, data security, and operational safety. The evaluation's findings provide strong evidence that the system satisfies enterprise application standards security requirements.

Last but not least, even though they fall outside the scope of this work, the following limitations nevertheless need to be taken into account: The Bitcoin blockchain, which is backed by thousands of users in the cryptocurrency community, serves as the foundation for our initiative. A wide range of stakeholders can have an impact on the blockchain ecosystem or business model, therefore it would be foolish to assume that the Bitcoin system will continue to operate effectively in the future. We'll eliminate the causes of instability in the upcoming years by utilizing a range of blockchain technologies, such as Hyperledger and Ethereum.

7. REFERENCES

[1] Tengyu Yu, Blockchain operation principle analysis: 5 key technologies, iThome, <https://www.ithome.com.tw/news/105374>

[2] JingyuanGao, The rise of virtual currencies! Bitcoin takes the lead, and the other 4 kinds can't be missed. Digital Age, <https://www.bnnext.com.tw/article/47456/bitcoinether-li-tecoin-ripple-differences-between-cryptocurrencies>

[3] Smart contracts whitepaper, <https://github.com/OSELab/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 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.

[9] Weiwen Yang, Global blockchain development status and trends, <http://nmarlt.pixnet.net/blog/post/65851006->

[http://nmarlt.pixnet.net/blog/post/65851006-%E5%85%A8%E7%90%83%E5%8D%80%E5%A1%8A%E9%E7%88%87%E8%B6%A8%E5%8B%A2%E7%88%87%E8%B6%A8%E5%8B%A2%E7%99%BC%E5%B1%95%E7%8F%BE%E7%88%87%E8%B6%A8%E5%8B%A2](http://nmarlt.pixnet.net/blog/post/65851006-%E5%85%A8%E7%90%83%E5%8D%80%E5%A1%8A%E9%E7%88%87%E8%B6%A8%E5%8B%A2%E7%99%BC%E5%B1%95%E7%8F%BE%E7%88%87%E8%B6%A8%E5%8B%A2)

[10] 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.