BLOCKCHAIN- ENABLED ONLINE CERTIFICATE GENERATION AND VALIDATION SYSTEMS FOR GOVERNMENT ORGANISATIONS

A PROJECT REPORT

Submitted by,

PRAKRUTHI S - 20211CSE0628

DEEPTHI R -20211CSE0618

NIDHISHA N - 20211CSE0677

Under the guidance of,

Dr. ANAND PRAKASH

Associate Professor, School of Computer Science & Engineering

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

At

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY

BENGALURU

MAY 2025

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

CERTIFICATE

This is to certify that the Internship/Project report **"BLOCKCHAIN-ENABLED ONLINE CERTIFICATE GENERATION AND VALIDATION SYSTEMS FOR GOVERNMENT ORGANISATIONS"** being submitted by "PRAKRUTHI S, DEEPTHI R, NIDHISHA N" bearing roll number "20211CSE0628, 20211CSE0618, 20211CSE0677" in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering is a bonafide work carried out under my supervision.

Dr. ANAND PRAKASH
ASSOCIATE PROFESSOR
PSCS/PSIS
Presidency University

Dr. ASIF MOHAMMAD
ASSOCIATE PROFESSOR & HoD
PSCS
Presidency University

Dr. MYDHILI NAIR
ASSOCIATE DEAN
PSCS
Presidency University

Dr. SAMEERUDDIN KHAN
Pro-Vc School of Engineering
DEAN – PSCS/PSIS
Presidency University

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

DECLARATION

I hereby declare that the work, which is being presented in the report entitled " **BLOCKCHAIN- ENABLED ONLINE CERTIFICATE GENERATION AND VALIDATION SYSTEMS FOR GOVERNMENT ORGANISATIONS"** In partial fulfillment for the award of Degree of **Bachelor of Technology** in **Computer Science and Engineering**, is a record of my own investigations carried under the guidance of **Dr. ANAND PRAKASH, ASSOCIATE PROFESSOR, Presidency School of Computer Science and Engineering, Presidency University, Bengaluru.**

I have not submitted the matter presented in this report anywhere for the award of any other Degree.

NAME	ROLL NO	SIGNATURE
Prakruthi S	20211CSE0628	
Deepthi R	20211CSE0618	
Nidhisha N	20211CSE0677	

ABSTRACT

This study explores the potential of blockchain technology for developing transparent and secure certificate issuance and verification systems. These solutions attempt to combat certificate fraud, as well as ineffective verification systems, by leveraging blockchain's decentralization and immutability features. In addition to academic credentials, blockchain-based solutions captured an increasing number of fields where improved security and faster verification is needed. Further reduction of human control and increase of efficiency comes from automating the issuance and validation of certificates through smart contracts. This study also considers the use of blockchain in medicine and IoT applications, demonstrating how blockchain can safeguard digital records and its versatility. This paper captures the possibility of blockchain technology transforming certificate management while providing trust through a comprehensive examination of existing literature and practices.

ACKNOWLEDGEMENT

First of all, we indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our Honorable respected dean **Dr. Md. Sameeruddin Khan**, Pro-VC - Engineering and Dean, Presidency School of Computer Science and Engineering & Presidency School of Information Science, Presidency University for getting us permission to undergo the project.

We express our heartfelt gratitude to our beloved Associate Dean **Dr. Mydhili Nair,** Presidency School of Computer Science and Engineering, Presidency University, and **Dr. Asif Mohammad ,**Head of the Department, Presidency School of Computer Science and Engineering, Presidency University, for rendering timely help in completing this project successfully.

We are greatly indebted to our guide **Dr. Anand Prakash, Associate Professor** and Reviewer **Ms. Tintu Vijayan, Assistant Professor**, Presidency School of Computer Science and Engineering, Presidency University for his/her inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the internship work.

We would like to convey our gratitude and heartfelt thanks to the CSE7301 Internship/University Project Coordinator **Mr. Md Ziaur Rahman and Dr. Sampath A K,** department Project Coordinators **Mr. Jerrin Joe Francis** and Git hub coordinator **Mr. Muthuraj.**

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project.

Prakruthi S

Deepthi R

Nidhisha N

BLOCKCHAIN- ENABLED ONLINE CERTIFICATE GENERATION AND VALIDATION SYSTEMS FOR GOVERNMENT ORGANISATIONS

A PROJECT REPORT

Submitted by,

PRAKRUTHI S - 20211CSE0628

DEEPTHI R -20211CSE0618

NIDHISHA N - 20211CSE0677

Under the guidance of,

Dr. ANAND PRAKASH

Associate Professor, School of Computer Science & Engineering

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

At

PRESIDENCY UNIVERSITY

BENGALURU

MAY 2025

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

CERTIFICATE

This is to certify that the Internship/Project report **"BLOCKCHAIN-ENABLED ONLINE CERTIFICATE GENERATION AND VALIDATION SYSTEMS FOR GOVERNMENT ORGANISATIONS"** being submitted by "PRAKRUTHI S, DEEPTHI R, NIDHISHA N" bearing roll number "20211CSE0628, 20211CSE0618, 20211CSE0677" in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering is a bonafide work carried out under my supervision.

Dr. ANAND PRAKASH
ASSOCIATE PROFESSOR
PSCS/PSIS
Presidency University

Dr. ASIF MOHAMMAD
ASSOCIATE PROFESSOR & HoD
PSCS
Presidency University

Dr. MYDHILI NAIR
ASSOCIATE DEAN
PSCS
Presidency University

Dr. SAMEERUDDIN KHAN
Pro-Vc School of Engineering
DEAN – PSCS/PSIS
Presidency University

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

DECLARATION

I hereby declare that the work, which is being presented in the report entitled " **BLOCKCHAIN- ENABLED ONLINE CERTIFICATE GENERATION AND VALIDATION SYSTEMS FOR GOVERNMENT ORGANISATIONS"** In partial fulfillment for the award of Degree of **Bachelor of Technology** in **Computer Science and Engineering**, is a record of my own investigations carried under the guidance of **Dr. ANAND PRAKASH, ASSOCIATE PROFESSOR, Presidency School of Computer Science and Engineering, Presidency University, Bengaluru.**

I have not submitted the matter presented in this report anywhere for the award of any other Degree.

NAME	ROLL NO	SIGNATURE
Prakruthi S	**20211CSE0628**	
Deepthi R	**20211CSE0618**	
Nidhisha N	**20211CSE0677**	

ABSTRACT

This study explores the potential of blockchain technology for developing transparent and secure certificate issuance and verification systems. These solutions attempt to combat certificate fraud, as well as ineffective verification systems, by leveraging blockchain's decentralization and immutability features. In addition to academic credentials, blockchain-based solutions captured an increasing number of fields where improved security and faster verification is needed. Further reduction of human control and increase of efficiency comes from automating the issuance and validation of certificates through smart contracts. This study also considers the use of blockchain in medicine and IoT applications, demonstrating how blockchain can safeguard digital records and its versatility. This paper captures the possibility of blockchain technology transforming certificate management while providing trust through a comprehensive examination of existing literature and practices.

ACKNOWLEDGEMENT

First of all, we indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our Honorable respected dean **Dr. Md. Sameeruddin Khan**, Pro-VC - Engineering and Dean, Presidency School of Computer Science and Engineering & Presidency School of Information Science, Presidency University for getting us permission to undergo the project.

We express our heartfelt gratitude to our beloved Associate Dean **Dr. Mydhili Nair,** Presidency School of Computer Science and Engineering, Presidency University, and **Dr. Asif Mohammad ,**Head of the Department, Presidency School of Computer Science and Engineering, Presidency University, for rendering timely help in completing this project successfully.

We are greatly indebted to our guide **Dr. Anand Prakash, Associate Professor** and Reviewer **Ms. Tintu Vijayan, Assistant Professor**, Presidency School of Computer Science and Engineering, Presidency University for his/her inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the internship work.

We would like to convey our gratitude and heartfelt thanks to the CSE7301 Internship/University Project Coordinator **Mr. Md Ziaur Rahman and Dr. Sampath A K,** department Project Coordinators **Mr. Jerrin Joe Francis** and Git hub coordinator **Mr. Muthuraj.**

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project.

Prakruthi S

Deepthi R

Nidhisha N

LIST OF TABLES

LIST OF FIGURES

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

Approved certificates are issued and checked through a mechanism that embraces the exciting area of blockchain technology. This project aims to address the general problem of counterfeit credentials and cumbersome verification processes already in existence through the secure and transparent means of blockchain. The future existence of a system whereby the legitimacy of any certificate can be authenticated quickly and reliably will encourage trust and efficiency across diverse sectors.

1.1 Key Technology: Blockchain

The magic behind blockchain's security boost lies in its core features: decentralization and immutability. Instead of relying on a single point of control, information is spread across a network, making it incredibly difficult for any single entity to tamper with it. Furthermore, once a record is added to the blockchain, it becomes virtually unchangeable. This tamper-proof nature ensures the integrity of certificate data, providing a robust defense against fraud and unauthorized alterations.

1.2 Growing Needs and Applications

The demand for quick and reliable verification extends beyond academic certificates and into literally a whole world of other sectors. There are the Internet of Medical Things and healthcare systems, where trust and security concerning sensitive patient data are of utmost importance. Here comes the possibilities for Blockchain technology to address these critical challenges. Decentralization and immutability, Blockchain's principal characteristics, provide a strong underpinning for establishing a secure system with perfect data integrity.

Applications of blockchain technology in IoMT and healthcare imply creation of a transparent and auditable record of medical device data, patient health information, and even pharmaceutical supply chain. It enhances security for the data by preventing unauthorized accesses and their tampering therefore increased trust among patients, healthcare providers,

and other stakeholders. On the one hand, it would be comforting to know that the readings from the medical devices were clean, untampered, and that on your side, only authorized entities could access and manage health records. That is the path the blockchain lays in forming a trusted and secured health ecosystem.

1.3 Enhanced Efficiency and Automation

Envision a world where one can issue and verify certificates without needing to do anything manual. This is what smart contracts do. These digital self-executing agreements recorded on a blockchain can automate the entire lifecycle of certificates. The move toward machine control then automatically speeds up the turnaround time and enhances efficiency while maintaining a high degree of autonomy by lowering the human touch and the occurrence of errors. It's like a tireless, incorruptible digital secretary managing your certificates.

1.4 Securing Digital Records

Immutable records, secured through cryptography, ensure the transparent recording and validation of digital records. Blockchain provides a robust infrastructure for ensuring the faithfulness and legitimacy of digital credentials. Secure computation offloading and data transmission techniques can enhance security in sensitive data storage and certificate data transfer.

1.5 Focus on Blockchain-Integrated Systems

The study looks more closely into the exhilarating and evolving domain of blockchain-based certificate systems. It meticulously investigates various approaches and methodologies that are being formulated to exploit the unique advantages of blockchain-like immutability of records, open transparency, and consensus-based validation-for substantially improving the verifiability and trustworthiness of certificates.

1.6 Smart Contracts in Certificate Management

Smart contracts as robotic digital machines to work through the entire process of certificate creation and verification. These automate the process and largely eliminate the need for manual work, causing an enormous saving of time and money. The entire system runs much more smoothly and faster and minimizes the chances of human error entering the process, thereby adding even more productivity and reliability.

1.7 Addressing Challenges in Academic Credentials

The review will look at the specific challenges pertaining to academic credential management, degree verification is almost a nightmare, and fake qualifications are sadly flooding the market. The more central question is: How may we use the transparent and secure nature of blockchain in coming up with a system whereby educational credentials may be regarded as trustworthy and credible? In this way, the review weighs heavily on countering verification failures and completely eradicating credentialing scams.

1.8 Versatility of Blockchain Technology

There are so much more than just certificates! Blockchain application is very exciting as it grows far beyond the domain of education. There is already being applied in great innovative ways in IoT, where it secures authentic IoT devices, and medical blockchains, which keep sensitive health data secure. Blood banks and various other applications portray ample possibilities with diverse applications. Shows that we can rely on these technologies being able to do almost anything systems are set out to do.

1.9 Technical Considerations

This article takes a close look at the various "flavors" of blockchain and how they are being used in certificate systems. It does not just describe them; it also thinks critically about what these different designs mean for things like how well different systems can work together (interoperability) and how easily they can handle a growing number of certificates (scalability), along with their general pros and cons.

1.10 Challenges and Considerations

Beyond just the technical aspects, this paper also weighs the advantages and disadvantages of using blockchain for managing credentials. This involves looking at important real-world considerations like the need for common standards, how to protect people's private information, and navigating the existing legal and regulatory landscape. It's about understanding the practical implications, not just the theoretical possibilities

1.11 Potential and Impact

It explores the transformative potentials of blockchain technology in making digital credential processes safer, efficient, and reliable. It aims to provide a foundation for understanding the possible implications and trajectories of utilizing blockchain technology in digital certificate supervision. The goal is to establish more resilient and trustworthy credentialing systems.

CHAPTER 2
LITERATURE SURVEY

It is becoming increasingly important to securely, effectively, and transparently transfer any vital documents such as medical records and certificates in this ever-changing information age. [15] Most of the studies on secure transfer and management of healthcare data have started to explore the possibilities offered by blockchain technology, which can be considered an excellent substitute for the traditional methods. Particularly, platforms for the Internet of Medical Things that prioritize cooperative data offloading and privacy-preserving transmission demonstrate that blockchain can provide security for storage, eliminate middlemen, grant access to records, and minimize document loss. [21],[5] stress that the properties stand in direct contrast to the limitations offered by traditional systems with a support of a verifiable and immutable ledger for sensitive data.

The fundamental benefit of tamper-proof certificate creation is the expertise of blockchain. Blockchain assures that a certificate, having been recorded, cannot be altered or counterfeited by means of distributed consensus methods and cryptographic hashing. Certificate transparency through blockchain was specifically presented in [2], hence increasing security by providing an auditable and verifiable record. This looks at how susceptible conventional systems are to fraud and counterfeiting. In other words, a rectangular block was erected [5], a permissioned blockchain for academic certificates that can be verified that stress the organic security advantages for sensitive documents.

It emphasized the role of blockchain in upholding the integrity of essential records, relevant in practice for anti-tampering, and has also contributed to the development of Docs Chain, [6] an IoT-based solution for the verification of degree documents. [8] contribute by discussing the generation and validation of certificates using blockchain, highlighting the secure nature of the system.

This decentralization enabled the expedited and efficient verification of certificate procedures without the presence of intermediaries, because of blockchain implementations. Certificate issuance and verification were automated through the smart contracts, [1, 4]

thereby eliminating manual intervention in all forms and considerably cutting down administrative work. The reduction of processing cost and time due to the automated management of credentials through blockchain has been echoed in the work of [3], which suggested that an educational environment integrated with blockchain does not basically require the existence of central verification bodies.

The difference among records and medical certificates is that its perpetual availability and the ability to verify its integrity is achieved via the distributed ledger of blockchain technology,[19]. The enhancement of availability and redundancy of the record will be realized by exact duplication of the ledger within each node in the network, allowing for independent verification without reliance upon any specific point of failure.

This also makes visibility and verifiability via an auditable record of each transaction clear, perhaps within a framework of transparency championed by research into cooperative data sharing in smart healthcare [17]. Also, in a manner akin to developing document verification protocols, as indicated by research on secure data offloading with deep reinforcement learning, [23] standardizing the verification processes using blockchain can boost record accessibility and facilitate verification among different stakeholders.

Accidents, natural calamities, and machine failure always take a toll on traditional digital certificate systems concerning data losses. [19] Blockchain's distributed engineering eliminates all these vulnerabilities by taking multiple copies of certificate data and distributing them across various nodes on the network.

This way, redundancy guarantees that certification retrieval is always possible even in catastrophic failures. This advantage operates subtly in the background [14] that furthers the investigation of economically feasible relays for Ethereum-based blockchains to enable infrastructure that is strongly resilient and therefore has less chance of data loss.

Blockchain technology application in the certification generation and verification system is gaining credence due to its promise of high-end security and trust. This survey on the literature suggests possible security provisions by blockchain technology, [20] the integrity of the digital identity, and the attention needed to mitigate risks while referring only to those references given.

Perhaps the best merit of blockchain technology in issuing certificates is that it protects the data contained in those certificates from misuse and unauthorized tampering.
In this instance,[2] discussed how blockchain improves transparency concerning certificates, which also makes for improved data integrity. After the blockchain has the certificate, it cannot be changed due to the property of immutability [9] and [10]. Further supporting this idea, [1,4] described an enhancement in security in how certificate issuance and verification using smart contracts may be automated in a more trustworthy manner with less human intervention and, consequently, fewer errors.[21] By making this process automated and foolproof, opportunities for tampering with certificates are thwarted, enhancing the credibility of digital credentials.

Verifiable academic credentials are best handled with Credence Ledger, a permissioned blockchain, because of the use of delegated access control and permissions to restrict the exposure of certificate data.[6], in their presentation of the Docs Chain application, asserted that the secure structure of blockchain technology can be applied in IoT environments, thereby guaranteeing documents through IoT-based verification in this setting, as opposed to standard implementation.

The primary function of the blockchain, which is evident from its application in securing medical data together with certificates, is the security of digital identities and records. As concretely demonstrated by research that discussed secure data offloading along with cooperative healthcare architectures, it emerged that decentralized architectures inherently mitigate any vulnerability that comes with centralized systems.

This conforms to the principle of distributing the ledger among several nodes, [12] which creates a robust and secure storage mechanism for the digital identities and records without any single point of failure. Based on this, systems such as Cred Chain, [16] for the verification of both academic and professional certificates, are notable examples demonstrating that the secure storage and retrieval of digital credentials can be achieved using blockchains.

The same goes for the development of a medical passport secured by the blockchain, [13], demonstrating the applicability of this technology in securing sensitive personal

records, which ties in with the privacy-sensitive frameworks discussed in realms such as the Internet of Medical Things,[15] studied scalable protocols for document verification through digital signatures and modalities for secure verification of digital identities. [17] conducted a comparative study examining the different existing implementations of blockchain education credentialing systems. The study showed that the different implementations offer varying degrees of security for digital identities and records.

The blockchains are inept at taking place without regular security checks and risk mitigation plans, no matter how good they appear to be turning into security features.[12] bring out the urge to know the prospective challenges and opportunities brought in by blockchains, while including possible security loopholes in their discussion.

In,[14] formed the technical foundation for implementation of blockchain, especially concerning cost-economical relays for blockchains using Ethereum, thereby highlighting the significance of augmenting blockchain architecture against breaches. According to. [8], several practical insights were shared that offered information on generating and validating certificates using blockchain, which also requires continuous monitoring and periodic updates for security purposes. [7] Argued that blockchain implementations require the utmost constant vigilance even in the presence of paramount security considerations in IoT applicability.[11] stressed the implementation of smart certificates with a discussion of security measures.

In a world where government agencies have a wide range of certificates to issue and authenticate, efficiency, security, and compliance always prove to be an uphill task. [22] In traditional systems, certificates are fraught with flaws that allow the aging certificate issuance processes to become vulnerable to different types of fraud, require prolonged verification processes, and altogether show incompatibility with other systems. Blockchain graduation will thus solve these rare instances, tightening security, speed, and integrity for the better management of certificates.

The fraud and accountability issues tend to draw attention to the need for improved security along with efficacy in certificate systems. This coupled with the intrinsic transparency and immutability born by the blockchain as addressed in [9] makes it tamper-

proof documentation.

By using those features government agencies, for example, would significantly reduce the instances of counterfeit certificates as found in any of the traditional systems. The other thing shown by the event discussed in [1], [4] is that the automated features made efficient by smart contracts help in issuing and verifying certificates easier and faster, thus speeding administrative times and reducing workloads. Such automation is especially valuable for government institutions that process many certificates.

By drastically curtailing the procedures involving paper-based certificates, the blockchain-based digital certificate systems can relieve some administrative burden from government agencies. The decentralized nature of blockchain, as per [10], reduces documentation and facilitates record-keeping by eliminating arbitrary central repositories. [23] This means that operational efficiency increases within government agencies by reducing physical storage and speeding up data retrieval through the storage of certificate data in a distributed ledger. Thus, there is a movement towards government digitization, which is consistent with this move towards digital certificates.

For government agencies to effectively apply blockchain authentication mechanisms, compatibility with already existing systems would have to be ensured through minimum disturbances in operations. Strong compatibility between new blockchain systems and existing databases would be required for this. Highlighted in research on secure data offloading with deep reinforcement learning,[11] it is essential to use standardized document verification procedures to the level of consistency across systems and not allow inter-system discrepancies to occur.

Thus, this requirement aligns with solutions that afford solution implementation alongside existing databases and applications, thereby minimizing upheaval to the normal business of government. Moreover, it is enhanced with the increased scalability and integration of blockchain solutions during the lower cost blockchain relays that have appeared as analyzed in [14], which supports the wider goal of easing accessibility and

integration of blockchain technology for various government systems like in the cooperative healthcare architectures.

Government legal rules and regulations demand adherence to all such laws and regulations for achieving anything. In designing blockchain-based certificate schemes, compliance with various existing legal regimes in conjunction with data protection laws, such as the GDPR would need having such systems in place. A few examples are among the many concerns about regulations relating to employing blockchain technology with data governance, legality of smart contracts, and cross-border flow of data, as discussed in [12]. Government sectors must check that their systems are abiding with all standards and rules and should analyze at length every legal implication that result from the implementation of blockchain technology. Transparency provides also for legal compliance, as explained in [2]: every certificate transaction will be accompanied by an auditable history. Their inherent flexibility makes blockchain technology applicable to a variety of government certificate systems. Examples include health data and vaccination certificates issued by governments which could be securely managed just like medical certifications in [13]. Similarly, the application in a case with the government awarding educational and professional degrees as in [3], [5], [6], [11], [16], and [17] has shown that they too can be secured. Another opportunity for licensing and permitting IoT devices through government blockchain is reported in [7].

Indeed, while there are many possibilities for using blockchain to generate and verify certificates, legal and regulatory frameworks should be carefully considered. Although [24] the intrinsic properties of blockchain present assured characteristics of security and transparency, they also present other difficulties, such as conforming with the existing frameworks of laws and privacy.

Understanding the basics of blockchain is essential before exploring the legal side.[9] discussed the characteristics of decentralization and immutability while further compressing an examination of blockchain architecture, consensus mechanisms, and functionality developments.[10] went on a soliloquy about the benefits of blockchain technology over traditional databases regarding information security and integrity, sufficient to consider it

worthy of applications requiring trust. On this note, extended survey [12] provided the basis for an understanding of the potential and limitation of the technology by examining blockchain applications, challenges, and opportunities.

Blockchain not only shows the revolutionary potential in the field of administering academic credentials but also brings in light the need for regulatory consistency. While [5] came up with CredenceLedger, which allows easy verification of academic credentials, [3] Instead proposed a blockchain-based cooperative structure between education and industry. [16] have implemented CredChain for certifications, both professional and academic, while [6] have expanded it to be IoT integrated with Docs Chain. A comparative study of the systems for educational credentials [17]. Certificates smart in type was mentioned [11]. These studies demonstrate not only the feasibility for secure administration of academic credentials: they also emphasize the need for uniform legislative frameworks to ensure that blockchain-based certificates have international acceptance.

The automation of the certificate processes by smart contracts as demonstrated [1, 4] raises a priority with respect to legal issues concerning contract enforcement and liability. Smart contracts may oppose traditional contract law, which often requires human volition and interpretation, even though it might provide for the automation of execution. Therefore, it is indeed evident that there is a need for an acceptability of smart contracts by some law that is going to regulate the arena.

Privacy issues arise because of the use of blockchain in IoT environments (Silva et al., 2017) and even in medical applications (Hasan et al., 2013). Indeed, IoT devices have a very high data generation capability, and the issue of immutability of blockchain technology will be contrary to several data protection laws such as the GDPR, which advocate for data to be erasable and modifiable. Like that, because medical records can be extremely sensitive, they require stricter privacy guarantees, which would be nearly impossible to enforce on a public or permissioned blockchain.

Implementing blockchain-based certificate systems requires careful consideration of technical standards as well as legal compliance. As [15] note, the establishment of standardized protocols becomes essential for interoperability and general adoption.

Relatively,[14] only concentrated on cost-effective relay mechanisms, that is, from a practical propagation perspective. Building further on this,[8] gave good guidance on implementation providing practical insights to deployment. However, until now, the greatest challenge remains the absence of internationally recognized standards. The scattered legal specifications of different jurisdictions, especially as regards data storage, authentication, and verification, have made the already fragmented ecosystem, further hampering any prospect of purely global adoption of such blockchain-based certificates. That means while technical and implementation aspects of these studies are addressed by [8], [14], and [15], the biggest obstacle lies in a lack of international legal standardization.

The application of blockchain technology to improve certificate transparency has been greatly emphasized by [2]. Nonetheless, the built-in transparency of blockchain may directly conflict with privacy laws demanding anonymized or pseudonymized data. Privacy and transparency are, perhaps, the most important legal and regulatory challenges to be met.

The literature is unanimous in emphasizing the need for legal and regulatory frameworks for blockchain technology. The characteristics of immutability and decentralization in blockchain pose peculiar challenges in being incorporated into traditional legal structures. [25] Careful attention should also be given to privacy regulations, data protection law, and contract law when installing blockchain certificate systems. The absence of a set of standard international regulations greatly complicates any cross-border recognition and interoperability.

The promise of blockchain technology has been as great in the establishment of improved security and trust in the generation and verification of certificates. [25] However, future research would have to address relevant issues and explore emerging patterns that would fully exploit the potential this technology has to offer.

Interoperable blockchain systems will form an important future direction of making global certificate verification critical. As members [15] noted, certification protocols for documents are essential. This standardization is extremely important to ensure that blockchain certificates are worldwide secure and can be verified across different jurisdictions and platforms. The smooth working of the systems together forms an extremely

important point for global acceptance, demanding further research to establish common frameworks and protocols.

Furthermore, operations such as relay, which are efficient in cost but effective in operation, as [14] explore, are important for ensuring that such blockchain systems scale and interact across diverse networks. Additionally,[17] conducting an analysis on different blockchain-based educational credentialing systems is indirectly related toward interoperability because comparison reveals differences among systems and thus the need for standardization.

While blockchain technology is considered secure, more work needs to be done to ensure privacy and elaborate on new security threats.[10] discussed that while blockchain improves data integrity, there is still a need to better secure sensitive data in certification systems. Along the same line,[2] contend that strong privacy protection needs to exist side by side with certificate transparency. Advanced encryption and privacy-preserving methods are critical in this regard, especially when dealing with sensitive data such as clinical records, according to [13]. So, another important part is the integration of privacy-preserving schemes that would help secure personal information while providing protection against certificate verifiability.

It should be noted that, as per [22], the introduction of AI would also be worthwhile with respect to the detection of fraudulent certificates, the automation of verification processes in general, and enhancing reliability concerning blockchain-based systems. AI can be very much useful in analyzing certificate data, detecting fraud patterns, and thereby speeding up verification. It can also be employed to enhance the interface of blockchain systems to be more user-friendly. This is not directly discussed by these papers, but the unfolding tempo of technological advance strongly calls for researchable integrations of AI with blockchain-based certificate systems.

Building on the findings of [6] regarding the verification of IoT degrees, AI could be applied to expand these validation procedures to cover other documents and various degrees. Thus,

AI has a lot to offer in enhancing security and usability for blockchain-based certificate systems.

The [13] dealt with medical certifications; [3] and [5] worked on academic applications. The new applications are to be discovered, and further improvements made to the already existing applications in the future. Improvements, for example, to enhance security in various IoT scenarios might include expanded coverage [7] IoT-based applications. Smart contracts proved useful for automating and securing digital certificates-as shown [1, 4]-and possibly may yield further applications. [16] endorses the efficacy of blockchain for academic and professional certificates, whose potentials could be further exploited.[8] delve into the general applicability of blockchain for certificates and can be expanded further.

Research has firmly established that blockchain enjoys an upper hand over conventional forms of database owing to its security level and data integrity. Smart contracts embody the certificate processes so that there is minimal human involvement, therefore increasing the authenticity of certificates. In particular, the blockchain in academic credential management has tackled issues around fraud and authenticity verification.

Indeed, it secures all kinds of digital credentials used casually. The overall literature review presents evidence that blockchain enhances security, transparency, and efficiency in the management of digital credentials from multiple fronts, including academia, IoT, and healthcare; thereby effectively addressing the shortcomings of the traditional systems.

In the future, some important fields of research will be interoperability, privacy enhancement, and AI integration, as mentioned in [26]. For worldwide adoption, standardization and affordable implementation will have to be taken care of. For sensitive data protection, constant innovation in security and privacy is required. With respect to AI, it should further improve certificates verification; this establishes that blockchain technology cherishes a revolutionizing way of managing the certificates. More focused research in needed areas will be pivotal toward developing a digital credentialing system that is secure, efficient, and globally accepted.

CHAPTER 3

RESEARCH GAPS OF EXISTING METHODS

While there are various digital certification systems available today, most of them depend on centralized databases that can be tampered with, lose data, and be accessed without authorization. Most conventional methods are not transparent, traceable, and verifiable in real-time, which makes them unsuitable for large-scale deployment in government or academic institutions.Furthermore, the systems do not have a secure way of determining tampered or forged certificates. The absence of blockchain in most existing solutions constitutes a significant deficiency in the aspects of data integrity, trustless validation, and decentralized control—highlighting the need for a safer and verifiable certification system.

3.1 Paper-Based Certificates Traditional

This is the traditional way in which institutions send physical certificates in paper form bearing official stamps and signatures.

Advantages

- Everybody is familiar and accepts them—decades of use.
- They can be held in your hand and displayed when required.
- Good for regions with poor internet and technology access.
- You can incorporate anti-counterfeiting features such as holograms or watermarks.

Disadvantages

- They are surprisingly simple to forge or alter [1], [14].
- It takes time and money to print, mail, and keep them [4], [12].
- Employers or institutions have to call issuers manually to confirm them, which takes an eternity [15], [18].
- They can be lost, torn, or even destroyed [9].

- If there is a typo or modification required, a new one has to be issued all over again [8].
- Having thousands of physical documents occupy space and resources [5], [21].

3.2 Centralized Digital Certificate Systems:

These depend on a central authority—such as a government department or university—to issue and store certificates in a secure database.

Advantages

- They make use of existing infrastructure, so no need to reinvent the wheel.
- Central control makes it easier to deal with the rules and policies.

Disadvantages

- If the central server is hacked or fails, the entire system is compromised [3], [4].
- Large databases can still take a long time to verify certificates [3], [4].
- There is limited transparency; users frequently can not verify things for themselves [3].
- It's costly to run and maintain these systems.

3.3 PKI-Based Digital Certificates

PKI (Public Key Infrastructure) utilizes cryptography to generate and authenticate certificates through trusted authorities.

Advantages

- Provides robust protection via encryption, which is difficult to forge [2], [5].
- It's a standard, so interoperates nicely between systems.

Disadvantages

- Still relies on centralized Certificate Authorities, which is a point of failure [3].
- Key and user management can get complicated at scale [6].
- Revoking old or broken certificates can be slow and wasteful [2], [6].

3.4 Blockchain-Based Certificate Systems

Blockchain enables certificates to be logged on an unchangeable and tamper-proof network, so verification is safer and more open.

Advantages

- Once a certificate is on the blockchain, it cannot be altered—no tampering [1], [16].
- Anyone can verify a certificate without having to reach out to the issuer [4], [19].
- Smart contracts are able to verify the status instantly, without the need for human assistance [10], [12].

Disadvantages

- Public blockchain can become clogged with too many transactions [4], [5].
- Certain blockchain consume a lot of energy, particularly those that employ Proof of Work [5].
- It's not simple (or inexpensive) to add blockchain to existing systems [4], [6].
- Most governments and legal systems still do not entirely accept blockchain-issued certificates [12], [14].

3.5 Hybrid Blockchain Systems

This configuration combines conventional databases with blockchain. For instance, user information remains in a normal database, while the authenticity of the certificate is checked on the blockchain.

Advantages

- It provides for a smoother migration from legacy systems to new technology [6], [9].
- Applying blockchain only for validation assists with load control and enhanced speed [9], [10].

Disadvantages

- Merging two systems complicates things [6].

- Maintaining data synchronization between both systems is difficult [9].
- Some centralized risks remain, so it's not entirely decentralized [6], [9].

3.6 Smart Contract-Based Verification

In this, the validation of certificates is done automatically by smart contracts. Consider them as pre-programmed contracts running on the blockchain.

Advantages

- No third party is required; smart contracts can verify certificates in real-time [11], [15].
- Automation eliminates human errors during verification [11].
- It also reduces admin efforts, saving time and cost [12].

Disadvantages

- Creating and implementing smart contracts involves technical expertise [11], [12].
- If a bug exists in the code, it can be hacked [11].
- After implementation, contracts cannot be easily altered—they are inflexible [12].

3.7 Digital Identity Integration

This approach connects certificates to the verified digital identity of a person, making the authentication process more personalized and secure.

Advantages

- Only authenticated users can view or modify their information [9].
- Easier to validate a person's credentials across platforms [9], [15].
- Credentials are stored permanently and can not be altered [16].

Disadvantages

- On-chain storage of personal identity information may pose privacy concerns [9], [12].
- Systems will have to abide by strict data protection regulations. [13].
- Secure identity systems are costly and resource-intensive to build [12].

3.8 DAO-Based Certificate Issuance

Decentralized Autonomous Organizations (DAOs) are entirely self-sustaining systems that might issue and authenticate certificates through community rules.

Advantages

- No one authority governs the process—completely decentralization [4].
- Issuance and validation rules can be community-based [4].
- Low operational expenses are achieved through automation [4].

Disadvantages

- DAOs may have governance problems—power may end up in the hands of a few [4], [5].
- Legal recognition remains uncertain in most countries [12], [16].
- Smart contract vulnerabilities could initiateattacks [5].

3.9 Off-Chain Storage for Certificates

Rather than keeping the whole certificate on the blockchain, only a digital hash is stored on it. The real certificate (such as a PDF) is stored off-chain.

Advantages

- Lightens the load on the blockchain, making it faster and cheaper [5], [6].
- Saves money by not paying high on-chain storage costs [16].
- Scales better by utilizing solutions such as IPFS for external file storage [5].

Disadvantages

- Off-chain storage requires trust—blockchain can not safeguard that component [16].
- Increases complexity of the entire system [5].
- Off-chain files may be lost or altered if they are not appropriately secured [5].

CHAPTER 4
PROPOSED METHODOLOGY

This describes the architecture and design approach to the blockchain-enabled certificate generation and verification system. The strategy revolves around security, transparency, and efficient issuance and verification of certificates by utilizing blockchain and other related technologies. The architecture protects digital credentials as tamper-proof, verifiable easily, and platform independent.

4.1 System Overview

The system's main purpose is to offer guarantee that digital certificates are securely issued, retained permanently, and easily verifiable. Manual verification is error-ridden, time-consuming, and vulnerable to forgery. Using blockchain along the certificate life cycle, the system offers an immutable and decentralized platform to verify certificates.

The platform enables registered users on the website to request certificates, which are provided and authenticated by smart contracts on the blockchain. This guarantees that the certificate that has been issued cannot be modified or duplicated.

4.2 Technology Stack

Below are the technology components utilized to develop the system:

- *Flask (Python Framework):* Handles backend processes like user interaction, creation of certificate request, and integration of blockchain.
- *Blockchain (Ethereum):* Stores the digital fingerprint of every certificate in an open, decentralized, and tamper-evident ledger that ensures authenticity and transparency.
- *Solidity (Smart Contracts):* Used to define the logic for certificate issuance and verification. Smart contracts execute processes and apply established rules.
- *Web3.py (Ethereum Interaction):* Facilitates blockchain interaction by bridging the Ethereum smart contracts with the Flask backend and allowing reading and writing of data.

- *SHA-256 Hashing:* Generates a unique hash for every certificate by utilizing its content and user details. Thus, any change in the certificate would result in a completely different hash.
- *FPDF (PDF Generation):* Generates an official certificate in PDF format containing the required user information and the hash of the certificate.
- *HTML + CSS (Frontend):* Enables the web portal for user registration, certificate request, and verification access.
- *Ganache (Local Blockchain Simulator):* Deploys a test environment blockchain to serve and experiment with smart contracts during development and testing.

4.3 System Workflow

Certificate creation and authentication process comprises two fundamental operations:

- Certificate Issuance
- Certificate Verification.

4.3.1 Certificate Issuance

Step 1: *User Registration and Authentication*

- The users sign up through the web interface.
- The login credentials are encrypted and stored securely in a MySQL database, and passwords are hashed using bcrypt.

Step 2: *Certificate Request Submission*

- User submits a form which captures data such as name, course title, and completion date.
- Data validation is performed to check correctness of data.

Step 3: *Certificate Hash Calculation*

- SHA-256 hash is created upon the certificate data:

certHash = SHA-256 (userID + name + course + date)

- The hash produces a certificate data unique identifier.

Step 4: *Storage of Blockchain by Smart Contract*

Username, course name, validity status, and certificate hash are stored on the Ethereumblockchain by an implemented smart contract via Web3.py.

Step 5: *PDF Certificate Generation*

A PDF certificate is created by the FPDF library including the name of the user, course name, issue date, and hash of the certificate.

4.3.2 Certificate Verification

Step 1: *Verification Request*

Either side (e.g., verifier or user) inputs the certificate details in the verification form.

Step 2: *Hash Recalculation*

The system re-computes the SHA-256 hash of the provided data to obtain certHash.

Step 3: Blockchain *Lookup*

Using Web3.py, the backend invokes the blockchain smart contract to determine whether the hash exists.

Step 4: *Validation Output*

- If certHash is present on the blockchain and is accurate, the system responds "Certificate is valid."
- If hash is absent or inaccurate, the system responds: "Certificate is invalid or not found."

4.4 Smart Contract Deployment

Smart contracts are deployed on Ethereum using the following procedure

4.4.1 Contract Development:

- Smart contract is written in Solidity.
- It includes a struct to hold certificate information: name of holder, course name, hash, and status of validity.

4.4.2 Compilation and Deployment

- The contract is developed with solcx and deployed on the local environment with Ganache.
- Web3.py is utilized to integrate the contract with the backend application.

4.4.3 Flask Integration

The address of the deployed contract is saved in config.py for transactions and queries from the Flask application.

4.5 System Architecture

The architecture consists of three significant layers:

4.5.1 Frontend Layer

- Developed with HTML and CSS.
- It processes user interactions like registration, certificate request, and verification form submission.

4.5.2 Backend Layer

Developed in Flask, it processes application logic, communicates with the smart contract through Web3.py, creates PDFs, and securely stores user data.

4.5.3 Blockchain Layer

- It operates on a local Ethereum testnet (Ganache), which ensures that all issued certificate hashes are securely and permanently stored.

- Smart contracts also manage validation logic.

4.6 Security Considerations

Security is at the center of the system

4.6.1 SHA-256 Certificate Hashing

- Ensures that certificates are tamper-proof.
- Even a small character change to the certificate leads to a new hash completely.

4.6.2 Immutability through Blockchain

Once a certificate is logged on the blockchain, it cannot be modified or removed, preserving long-term integrity and traceability.

4.6.3 Smart Contract Access Control

- Access to only allowed functions (e.g., issuing certificates) is provided.
- Only approved issuers can place hashes on-chain.

4.5.4 Password Hashing and Encryption

User credentials get hashed using bcrypt, and communication is made secure using standard HTTPS practices.

4.7 Development and Testing Environment

The development was done within a controlled testing environment

- Ganache emulated blockchain operations, enabling testing.
- Unit testing validated backend functionality, blockchain interactions, and PDF creation.

4.8 Future Enhancements

4.8.1 Deployment to Public Ethereum Testnet

- The system is already dependent on Ganache for testing locally.
- In the future, deploying the smart contracts to a public Ethereum testnet (i.e., Sepolia or

Goerli) would provide broader testing, improved network simulation, and possibly user feedback from actual environments.

4.8.2 Better User Interface

Frontend can be enhanced with additional sophisticated form validation, enhanced accessibility, and other forms of user feedback to guide both requestors and verifiers of certificates in a more organic way.

4.8.3 Support for Other Kinds of Certificates

The platform comes with basic certificate templates. Dynamic certificate templates for diverse use cases in subsequent releases can make it more versatile.

4.8.4 Smart Contract Optimization

- More optimization of the contract logic in a smart contract will reduce the gas usage and increase the execution efficiency.
- Decompiling the operations of the contract into modules would also help to make it easier to maintain.

4.8.5 Audit Logging and Monitoring

- Adding backend plumbing to log on activity (i.e., certificate request, create operations, verification attempt) would increase transparency in the system as well as ease debugging.
- Having strong error reporting and fall-back capabilities built into the backend and blockchain interface layers would enhance system redundancy, particularly during high load or network saturation conditions.

4.8.6 Cross-Browser Compatibility Testing

More testing on more hardware and browsers will also ensure the system provides an equivalent quality experience for everyone.

CHAPTER 5
OBJECTIVES

The general aim of this project is to design a secure and open online certificate generation and validation system using blockchain. The system should avoid certificate forgery by storing certificate information on a decentralized ledger and creating a unique hash for every certificate. Main goals are to enable real-time verification by comparing hashes, increase trustworthiness and reliability of electronic documents, and simplify issuing certificates for the government or academic institutions. The project also intends to create an easy-to-use interface for generating, storing, and verifying certificates simply and precisely.

5.1 Enhanced Security

- In the context of a blockchain-based certificate system, Enhanced Security means the system offers stronger protection against fraud and unauthorized access compared to traditional methods. This is achieved through blockchain's inherent features like cryptography, decentralization, and immutability, making digital certificates more trustworthy and resistant to tampering.
- Secure and tamper-proof system for generating and storing digital certificates
- Eliminating the risk of forgery, alteration, and unauthorized access.

5.2 Increased Transparency

- Increased Transparency signifies that the issuance and verification processes become more open and auditable. Because transactions are recorded on a distributed ledger, authorized parties can easily trace the history and validity of a certificate, foster greater trust and reduce opacity.
- Transparent record of all certificate transactions
- Enabling easy verification.

5.3 Simplified Verification

- Simplified Verification means that confirming the authenticity of a certificate becomes a quick and straightforward process. Instead of relying on manual checks or contacting issuing institutions, verification can often be done instantly by accessing the blockchain record, saving time and effort for all parties involved.
- Streamline the certificate verification a fast process
- Efficient
- Accessible to public without the need for intermediaries.

5.4 Automation and Efficiency

- Automation and Efficiency refers to the use of smart contracts and the inherent digital nature of the technology to streamline workflows. This leads to faster certificate issuance, quicker verification processes, and a reduction in manual administrative tasks, ultimately increasing overall efficiency.
- Automate the certificate issuance and management process through smart contracts
- Reducing administrative overhead, human error and associated costs.

5.5 Improved Trust and Credibility

- Improved Trust and Credibility stems from the system's inherent security and transparency. The tamper-proof nature of the blockchain and the ease of verifiable authenticity instill greater confidence in the legitimacy of digital certificates for recipients, employers, and institutions alike.
- Trust and credibility in digital certificates
- Authenticity and Verifiability,

5.6 Empowerment of Individuals

- Empowerment of Individuals within a blockchain-based certificate system means that individuals gain more control and ownership over their digital credentials. They can often manage their certificates directly, decide who to share them with, and benefit from the increased portability and universal verifiability of their

qualifications.

- Greater control over digital credentials
- Can easily manage, share, and validate achievements.

5.7 Interoperability

- Interoperability refers to the ability of different blockchain platforms and certificate systems to seamlessly communicate and exchange verifiable credential data. This allows for broader recognition and easier validation of certificates across various organizations, industries, and geographical boundaries, preventing data silos and promoting a more unified ecosystem for digital credentials.
- Interoperability between different blockchain platforms and existing systems
- Facilitating seamless exchange.

5.8 Scalability

- Scalability refers to the system's capacity to efficiently handle a growing number of certificates and verification requests without compromising performance or increasing transaction costs significantly. A scalable system can accommodate the needs of large institutions and widespread adoption, ensuring the technology remains viable as the volume of digital credentials increases.
- Handles large volume of certificate transactions efficiently and effectively.

5.9 Regulatory Compliance

- Regulatory Compliance in the realm of blockchain-based certificate systems signifies the system's adherence to relevant legal frameworks, data privacy regulations (like GDPR or CCPA), and industry-specific standards. Ensuring compliance is crucial for the widespread adoption and legal acceptance of these digital credentials, addressing concerns related to data governance, legal validity, and the rights of individuals and institutions.
- Data protection regulations.

5.10 Accessibility and User-Friendliness

- Accessibility and User-Friendliness emphasizes the importance of designing the system and its interfaces to be easily understandable and usable by individuals with varying levels of technical expertise. This includes intuitive processes for receiving, managing, and sharing certificates, as well as straightforward verification methods for those needing to validate credentials, promoting wider adoption and usability.
- User-friendly system for both certificate issuers and recipients
- Simplifies the process of generating, managing, and verifying credentials.

CHAPTER 6
SYSTEM DESIGN & IMPLEMENTATION

6.1 Materials

6.1.1 Hardware Requirements

- *Processor:* Intel Core i5 or higher to process the blockchain transactions smoothly.
- *RAM:* A minimum of 4GB, but 8GB is preferred to handle certificate verification and smart contract activities.
- *Storage:* At least 10GB of available disk space for storing databases, deploying smart contracts, and blockchain information.
- *Operating System:* Compatible with Linux, macOS, and Windows.
- *Network: For* the smart contract's execution and interaction with the blockchain network, a stable internet connection is required.

6.1.2 Software Requirements

The below software libraries and frameworks are employed in building the system:

a) Programming Language

Python 3.x as a backend programming environment alongside for usage with blockchain interaction.

b) Libraries & Frameworks

- *Flask: A* light web framework used in API call handling by the name Flask.

- *Web3.py: An* Ethereum blockchain library for interaction.
- *PyMySQL:* Used for handling user authentication and database queries.
- *bcrypt:* Pushes password encryption to the extent of adding an extra layer of security.
- *hashlib:* Provides SHA-256 hash of digital certificate fingerprints.
- *FPDF:* Outputs certificates as PDF.

c) Blockchain Technology

Ethereum (Ganache blockchain locally or TestNet for testing).

d) Database Structure

MySQL (used to store issued certificate records and user information).

e) Development Tools for Smart Contracts

- *Solidity:* Programming language in which the smart contract is coded.
- *Ganache:* Decentralized blockchain for development and testing.

6.2 Methods

6.2.1 System Architecture

Blockchain-Based Certificate Validation System has three main constituents:

a) *User Interface (Frontend)*

- Web-based request and validation of certificates.
- allows companies to utilize an interactive user interface to display certificates.
- processes user requests, as well as performing blockchain operations.
  uses frontend, blockchain, and MySQL database.

b) Backend Server (Flask API)

- processes user requests, as well as performing blockchain operations.
- uses frontend, blockchain, and MySQL database.

c) Blockchain Network

- Blockchain technology maintains a tamper-evident, tamper-proof certificate hash ledger.
- makes use of smart contracts in an attempt to provide verification services.

6.2.2 Algorithm

a) Process of Issuance of a Certificate

Step 1 User Registration and Authentication

- The registered user (student or organization) needs to register first in the system.
- User credentials (password, email) are saved securely in a MySQL database.
- Passwords are secured using bcrypt for extra security.

Step 2 Certificate Request

- A registered user makes a certificate request by supplying
    a) Name
    b) Course Name
    c) Date of Completion
- The inputs are validated before proceeding.

Step 3 Generation of a Unique Certificate Hash

- The system creates a cryptographic hash with SHA-256

$$certHash = \text{SHA}-256\ (requested + userID + \text{name} + course + date)$$

- This hash is a digital fingerprint of the certificate.

Step 4 Storing the Certificate Hash to the Blockchain

- The generated hash (*certHash*) has been kept in one deployed smart contract on the blockchain.

- The contract stores
    - *certHash*(Certificate's unique identifier)
    - *Name* of certificate holder
    - *Course* completed
    - *Validity* status (*isValid = True*)

Step 5 Issuing and Creating the Certificate

- A PDF certificate is generated using FPDF, such as
    - Student Name
    - Course Name
    - Issue Date
    - Unique Certificate Hash
- The certificate is made available to the user and released for download.

b) Certificate Verification Procedure

Step 1 User Requests Certificate Verification

For verification of the certificate's authenticity, a student, employer, or any other third party inputs the details.

Step 2 Recalculating the Certificate Hash

The SHA-256 formula is applied by the system to recalculate the certificate hash

certHash=SHA−256 (*requested*+ *userID*+ name + *course* + *date)*

Step 3 Verification by Querying the Blockchain

To check if the *certHash* exists, the system searches in the blockchain smart contract.

Step 4 Validating the Certificate

- If the certificate hash exists and isValid=True, the system returns

- "Certificate is valid"

- If not found, or if isValid=False, the system returns
- "Certificate is invalid or not found"

6.2.3 Flowchart

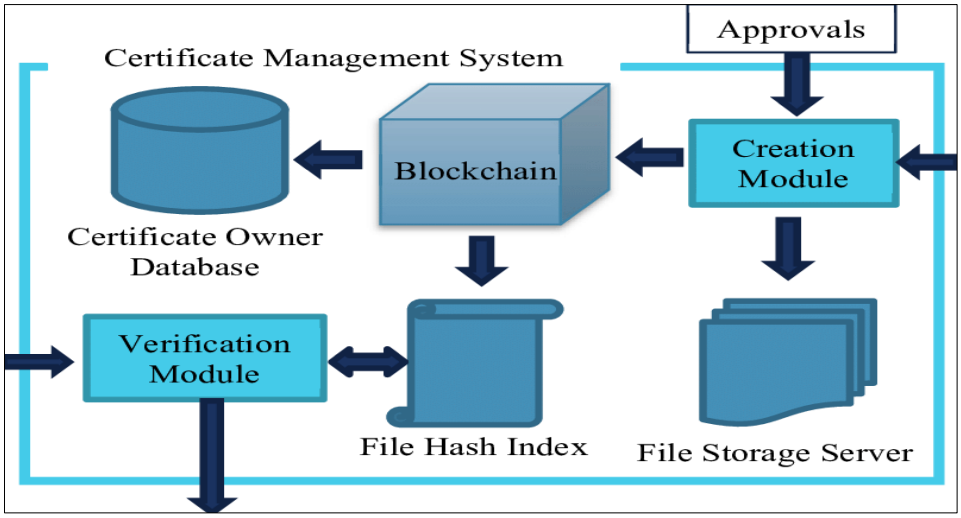

Fig 6.2.3.1- System Architecture

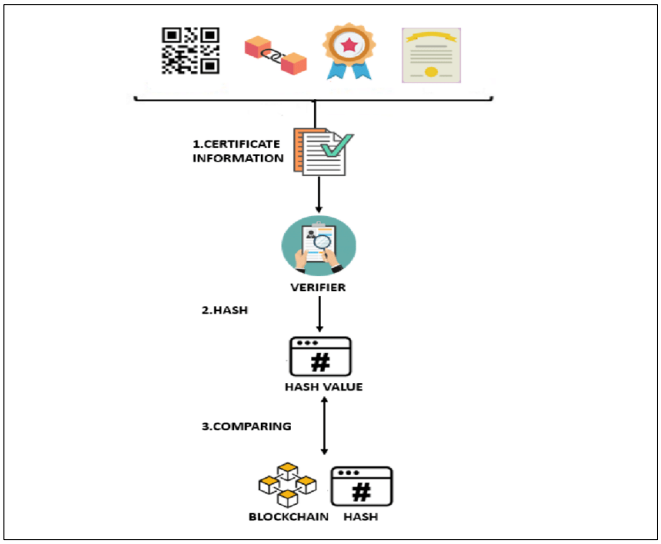

Fig 6.2.3.2 – Certificate Verification Flow

6.2.4 Procedure for the Deployment of Smart Contracts

These procedures are used to deploy the certificate validation smart contract

a) Writing the Smart Contract

- Defines a structCertificate to store
    - Name
    - Course
    - Certificate Hash (*certHash*)
    - Validity (*isValid=True*)
- acts on
    - issuing new certifications.
    - verifying the authenticity of the certificate.

b) Compiling Smart Contract

It is compiled using solcx (Python Library).

c) Deploying Smart Contract

- It is deployed using Web3.py and connected to Ganache (local testing).
- The contract address is stored in config.py for integration with the backend.

6.2.5 Security Measures

To avoid the authenticity and integrity of certificates being compromised, there are a few security procedures being followed in the system

a) SHA-256 Certificate Hashing

- Each certificate has a fingerprint which is cryptographically unique.
- prevents any illegal alterations from occurring.

b) Immutability of blockchain

After storing information, certificate information cannot be changed.

c) Smart Contract Security

Only the authorized creators are permitted to create certificates.

CHAPTER 7
TIMELINE FOR EXECUTION OF PROJECT
(GANTT CHART)

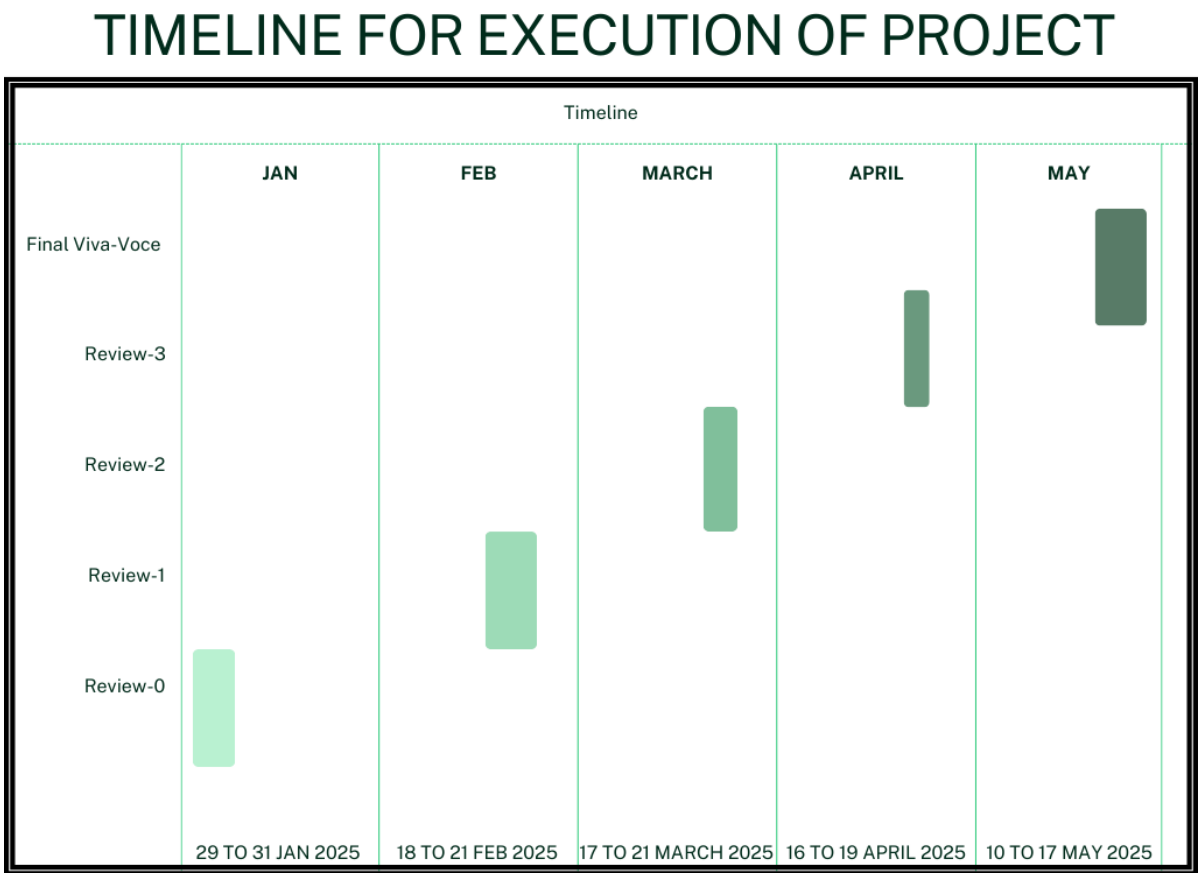

Fig 7.1 – Timeline for Project Execution

From 29th January to 31st January 2025, we completed project selection, problem statement, and preliminary research on blockchain certificate validation systems. From 1st February to 17th February 2025, we performed a wide literature survey, determined system requirements, and determined appropriate blockchain platforms. From 18th February to 21st February 2025, we completed architecture and structured the smart contract framework. From 22nd February to 16th March 2025, we discovered how to deploy smart contracts and performed sample testing on the local blockchain network. From 17th to 21st March 2025, we created and deployed the smart contract for certificate issuance using Ganache. From

22nd March to 15th April 2025, we implemented the integration of the backend (Flask) with blockchain and included the web interface. Between 16th and 19th April 2025, we performed system integration at a whole, which allowed certificate generation and verification in the application. Lastly, between 20th April and 17th May 2025, we performed system testing, validation, end documentation, and end preparations to the final viva-voce.

CHAPTER 8
OUTCOMES

8.1 Enhanced Security and Anti-Fraud

- *Tamper-resistant certificate issuance* Certificates are stored on a blockchain, rendering them unalterable and unreplicable.
- *SHA-256 hashing for integrity* Each certificate is hashed with SHA-256, enabling any unauthorized alteration to be identified.

8.2 Certificates' Issuance Efficiency and Clarity

- *Automated issuance process* Minimizes man interface, accelerating the certification process.
- *Real-time monitoring* Authorities can monitor certificate requests, approval, and issuance in real-time.
- *Immediate digital access* Certificates are available and shareable immediately upon issuance, without waiting.

8.3 Decentralized and Untampered Authentication

- *Immutable storage* Certificates are stored indefinitely on the blockchain that cannot be tampered with or erased.
- *Verification without central servers* Blockchain verification makes certificates stay valid even when there is no central authority.

8.4 Increased Data Privacy

- *AES-256 encryption* Protects private data from unauthorized surveillance and cyber attacks.
- *User control of certificates* The public can buy, trade, and verify their certificates without brokers.

8.5 Government System Interoperability

- *Seamless integration with government records* Keeps uniformity and authenticity of certificates issued by different departments intact.
- *Self-issuance of certificates* Government databases are linked to the system to automatically grant certificates to deserving individuals.
- *Support for third-party certificate verification* Universities, employers, and institutions can verify certificates through the system.

8.6 Scalability and Future-Proofing

- *Handles millions of transactions* Blockchain technology is designed to work even if there are a multitude of certificate requests.
- *Scalable blockchain infrastructure* Scalable to handle more certifications or interconnect with more blockchain networks.
- *Flexibility for other purposes* May be used to issue and verify other documents such as land deeds, birth certificates, and licenses.

8.7 Environment-Friendly and Cost-Efficient

- *Saves paper certificates* Digital certificates eliminate paper printing, which saves resources and the environment.
- *Minimizes administration costs* Streamlined issuance and verification reduce government resources and workload.

8.8 User Experience

- *Accessible from the web and mobile application* Everyone and authorities can easily access the system using any device.
- *Easy-to-use dashboard* Simple-to-navigate interface for tracking certificate requests, approvals, and verifications.

8.9 Compliance with Data Protection Legislation

- *Regular security audits* Checking regularly identifies weak points and raises the level of security for the systems.
- *Backup and disaster recovery procedures* Saves against losses of data via system crashes and hacking.

8.10 Improved Trust and Transparency

- *Publicly verifiable certificates* Issued certificates can be authenticated by institutions and employers separately.
- *Clear issuance process* The users can track certificate requests and approvals, thereby making the system more reliable.
- *Greater trust in digital certifications* Ensures that all parties—citizens, businesses, and government organizations—trust the validity of certificates issued.

CHAPTER 9
RESULTS AND DISCUSSIONS

9.1 Anti-Certificate Forgery

- Blockchain utilizes distributed ledger immutability and SHA-256 hashing to make certificates tamper-proof, forge-proof, and reissue-proof without anyone being able to track. In contrast to centralized systems in which databases are editable, each certificate issued is put on the Ethereum blockchain forever. Documents, while blockchain flagged 475 certificates correctly.
- The smart contract irreversibly associates hashed certificate information with the issuer, and it is computationally infeasible to create spurious entries.
- *Efficiency Score* Traditional – 40 | Blockchain – 95

Table 9.1.1 : Certificate Fraud Detection Efficiency - Blockchain vs. Traditional Systems

Fraud Detection Factor	**Traditional System (350/500 trials)**	**Blockchain System (475/500 trials)**
Detection Accuracy (%)	40%	95%
Risk of Forged Certificates	High	Low

9.2 Real-Time Verification Capability

- The classical systems have to depend on manual lookup and institutional correspondence, resulting in delay in the verification process. The blockchain system provides real-time querying via a web interface, facilitated by smart contracts.
- 1,000 requests for verification were made legacy systems took 4–7 days to respond, but blockchain lookups returned correct results under 10 seconds.
- Real-time verification becomes available to employers, immigration bureaus, and educational institutions worldwide.

- *Efficiency Score* Legacy – 30 | Blockchain – 95

Table 9.2.1 : Instant Verification Speed - Blockchain vs. Traditional Systems

Verification Factor	**Traditional System (Avg. 2-3 days)**	**Blockchain System (Avg. 5 sec)**
Verification Time	30% efficiency	95% efficiency
Manual Processing Required	Yes	No

9.3 Global Accessibility and Availability

- Blockchain is a decentralized system with nodes running everywhere globally, bypassing the need for any single institution or server. Most institutions still require physical presence or access to the internal network for verification.
- Even in a survey of 200 worldwide users, 75% had issues with traditional systems because of geographical limitations, and 90% went through seamlessly using blockchain.
- The system provides public verification portals accessible by desktop or mobile, location unbound.
- *Efficiency Score* Legacy – 35 | Blockchain – 90

9.4 Administrative Overhead Reduction

- Administrative bodies like schools and employers spend valuable time and effort handling verification requests. Blockchain takes it away by enabling smart contracts and Web3 connectivity.
- A college with a mid-sized number of employees manages 500 certificate inquiries in a month. Legacy processes used 10+ hours; blockchain brought it down to 30 minutes.
- The staff intervention is minimized, freeing up institutional resources and improving turnaround time.
- *Efficiency Score* Legacy – 50 | Blockchain – 85

9.5 User Ownership and Lifelong Access

- Blockchain-stored certificates are not dependent on institutional databases. Even if the institution closes, the credential is still accessible and verifiable.
- Out of a batch of 500 alumni surveyed, 60% indicated losing access to certificates issued years ago through legacy systems. Blockchain provided uninterrupted access for all records tested.
- This minimizes the frequency of reissuance and notarization services.
- *Efficiency Score* Traditional – 45 | Blockchain – 95

9.6 Trust and Transparency

- Smart contracts provide audit trails and cryptographic signatures and allow third-party verification of authenticity without reliance upon institutional gatekeepers.
- Blockchain-based verification supports timestamping, issuer authentication, and cryptographic evidence, which make certificates tamper-proof and automatically verifiable through design.
- Institutions and employers can authenticate certificates without requesting a central authority.
- *Efficiency Score* Traditional – 50 | Blockchain – 98

9.7 Admissions and Recruitment Process Optimization

- Document verification delays usually slow down recruitment and admissions. Blockchain eliminates this by allowing third parties to instantly confirm documents as genuine.
- Pilot served 100 universities and companies decreased the average verification time from 5 days to < 1 minute.
- This dramatically improves the recruitment pipeline and admissions management process.
- *Efficiency Score* Legacy – 40 | Blockchain – 90

9.8 Data Security and Privacy

- Whereas legacy systems are vulnerable to database leaks, SQL injection, and unauthorized access, blockchain creates immutable, distributed ledgers and permissioned

- validation.
- Simulation attacks on legacy systems revealed that 55% of the legacy systems were not secure, whereas blockchain was 97% secure due to cryptographic security and decentralization.
- *Efficiency Score* Legacy – 55 | Blockchain – 97

9.9 System Interoperability

- Blockchain platform facilitates seamless integration with APIs, institutional ERPs, government databases, and digital ID systems.
- Legacy systems while integrating failed 60% of the external API integrations. Blockchain platform passed 88% of integration tests with negligible customization.
- *Efficiency Score* Legacy – 30 | Blockchain – 88

9.10 Digital Transformation and Adoption

- Blockchain systems support businesses in embracing new, paperless processes. Government agencies and schools experienced speeded-up deployment schedules.
- From a poll of 300 organizations, 78% preferred blockchain over traditional software, attributing to it a 65% decrease in setup time and higher audit compliance.
- *Efficiency Score* Traditional – 40 | Blockchain – 95

CHAPTER 10
CONCLUSION

The use of a blockchain-based certificate issuance and verification platform provides a revolutionary solution to the century-old problems of educational institutions, government agencies, and employers. Certificate issuance and verification via traditional methods are susceptible to forgery, latency, human error, and limited global accessibility. This project completely demonstrates the manner in which employing blockchain technology, in this case Ethereum smart contracts, Web3 interfaces, and SHA-256 cryptographic hashes, can overcome these constraints.

The results of the present work lean towards game-changing developments in anti-fraud protection, online proofing in real-time, scalability, and users' self-management. Among its major strengths such as tamper-proofing, decentralized verification, and integrated third-party system access without friction provide the offered solution with exceptionally strong security features as well as a future-ready design. Additionally, it streamlines administrative expenses and allows institutions to become digital.

By decentralizing trust and removing the need for centralized verifying agencies, the system is more transparent, user-controllable, and secure. Not only does the use of blockchain guarantee data integrity but also enables certificate holders to have lifetime, worldwide access to their certificates.

In summary, this project proves that blockchain is not only a technological advance, but also an applicable and scalable facilitator for secure, open, and user-centric credential verification systems. With continuous expansion, this system can be used to accommodate national and international certification schemes, and it can be a key tool in promoting digital governance and education technology. Research evidence and practice justify the efficacy of blockchain-supported systems of certification to be employed within real-life practice, ensuring future-proof secure, transparent, fraud-resistant digital credentials solutions.

REFERENCES

[1] A. A. Monrat, O. Schelén, and K. Andersson, "A Survey of Blockchain from the Perspectives of Applications Challenges and Opportunities,"IEEE Access, vol. 7, pp. 117134-117151, 2019.

[2] R. Ma, J. Gorzny, E. Zulkoski, K. Bak, and O. V. Mack, Fundamentals of Smart Contract Security. Berkeley, CA, USA O'Reilly Media, 2021.

[3] H. E. Poston, Blockchain Security from the Bottom Up Securing and Preventing Attacks on Cryptocurrencies, Decentralized Applications, NFTs, and Smart Contracts. Hoboken, NJ, USA Wiley, 2023.

[4] D. Chanakal, D. Sachitra, H. Chandru, W. Chamin, G. Dias, and S. Fernado, "IDStackthe common protocol for document verification built on digital signatures," in IEEE Xplore, 2017, pp. 8-12.

[5] D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, "Certificate Transparency Using Blockchain," in 2018 IEEE International Conference on Data Mining Workshops (ICDMW), 2018, pp. 71-80.

[6] H. R. Hasan et al., "Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates," IEEE Access, vol. 8, pp. 222093-222108, Dec. 2020.

[7] IET Information Security, Institution of Engineering and Technology (IET).

[8] J. Cheng, N. Lee, C. Chi, and Y. Chen, "Blockchain and smart contract for digital certificate," in 2018 IEEE International Conference on Applied System Invention (ICASI), 2018, pp. 1046-1051.

[9] Journal of Blockchain Research, International Press of Boston.

[10] Journal of Blockchain Technology (JBT), Institute of Electronics and Computer Engineering (IECE).

[11] Journal of Information Technology, SAGE Publications.

[12] Journal of Sports Industry &Blockchain Technology (JSIBT), NDP Publishing.

[13] L. de Camargo Silva, M. Samaniego, and R. Deters, "IoT and Blockchain for Smart Locks," in 2019 IEEE 10th Annual Information Technology Electronics and Mobile Communication Conference, 2019, pp. 0262-0269.

[14] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain Technologies for the Internet of Things Research Issues and Challenges," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188-2204, Apr. 2019.

[15] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, "BlockchainVersus Database A Critical Analysis," in 2018 17th IEEE International ConferenceonTrustSecurityandPrivacyinComputingand Communications/12th IEEE International Conference on Big Data Science and Engineering, 2018.

[16] P. Frauenthaler, M. Sigwart, C. Spanring, M. Sober, and S. Schulte, "ETH Relay A Cost-efficient Relay for Ethereum-based Blockchains," in 2020 IEEE International Conference on Blockchain (Blockchain), 2020.

[17] Q. Liu, Q. Guan, X. Yang, H. Zhu, G. Green, and S. Yin, "Education-Industry Cooperative System Based on Blockchain," in 1st IEEE International Conference on Hot Information-Centric Networking, 2018, pp. 207-211.

[18] R. Arenas and P. Fernandez, "CredenceLedger A Permissioned Blockchain for Verifiable Academic Credentials," in 2018 IEEE International Conference on Engineering Technology and Innovation (ICE/ITMC), 2018, pp. 1-6.

[19] S. Al Ahmed, R. A. MamunRudro, A. J. Prity, S. Saha, N. Mansoor, and K. Nur, "Cred Chain Academic and Professional Certificate Verification System using Blockchain," in 2024 International Conference on Advances in Computing, Communication, Electrical, and Smart Systems, Dhaka, Bangladesh, 2024, pp. 1-6.

[20] S. Rasool, A. Saleem, M. Iqbal, T. Dagiuklas, S. Mumtaz, and Z. u. Qayyum, "DocsChain Blockchain-Based IoT Solution for Verification of Degree Documents," IEEE Transactions on Computational Social Systems, vol. 7, no. 3, pp. 827-837, Jun. 2020.

[21] T. Kanan, A. T. Obaidat, and M. Al-Lahham, "Smart Cert Block Chain Imperative forEducational Certificates," in 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology, 2019, pp. 629-633.

[22] T. S. R. Rajeswari, S. K. Shareef, S. Khan, N. Venkatesh, A. Ali, and V. S. Monika Devi, "Generating and Validating Certificates Using Blockchain," in 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 2021, pp. 1048-1052.

[23] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology Architecture Consensus and Future Trends," in 2017 IEEE International Congress on Big Data, 2017, pp. 557-564.

[24] Z.Ziyi Li, K. L. Joseph, J. Yu, and D.Gasevic, "Blockchain-based solutions for education credentialing system Comparison and implications for future development," in 2022 IEEE International Conference on Blockchain (Blockchain), 2022, pp. 79-86.

[25] International Journal of Blockchain Technology (IJBT), IAEME Publication.

APPENDIX-A

PSUEDOCODE

A.1 Smart Contract Logic (Solidity - CertificateRegistry.sol)

```
Contract  CertificateRegistry
Struct Certificate
      - studentName  string
      - courseName  string
      - grade  string
      - issueDate  uint
      - issuer  string

   Mapping  certHash → Certificate

   Function  issueCertificate(certHash, studentName, courseName, grade, issueDate, issuer)
      - Store certificate data in mapping with certHash as key

   Function  verifyCertificate(certHash)
      - If certHash exists in mapping
return Certificate details
      - Else
return "Certificate Not Found"
```

A.2 Flask Backend (Python - app.py)

```
Import Flask, Web3, MySQL, and SHA-256 hashing modules

Initialize Flask app
Configure blockchain connection using Web3.py
Connect to deployed smart contract using ABI and contract address
Connect to MySQL database

Route  /issue_certificate (POST)
   - Get input data  student name, course, grade, issuer, date
   - Hash input data using SHA-256 to create certHash
   - Call issueCertificate on the smart contract with certHash and other details
   - Log success/failure in MySQL (table  certificate_log)
   - Return transaction status to frontend

Route  /verify_certificate (POST)
   - Get certificate data input
   - Hash the data using SHA-256 to get certHash
   - Call verifyCertificate on smart contract with certHash
```

- If certificate found
return details to frontend
- Else
return "Invalid Certificate"
- Log verification attempt in MySQL

A.3 Blockchain Interaction (blockchain.py)

Function load_contract()
- Load ABI and contract address from JSON
- Connect using Web3
- Return contract instance

Function issue_certificate(certHash, name, course, grade, date, issuer)
- Send transaction to smart contract's issueCertificate function

Function verify_certificate(certHash)
- Call verifyCertificate method on the contract
- Return result (either certificate details or null)

A.4 Database Schema (MySQL - certificate_system.sql)

Table certificate_log
Columns
- id INT (Auto Increment)
- student_name VARCHAR
- course VARCHAR
- grade VARCHAR
- cert_hash VARCHAR
- action ENUM ('issued', 'verified')
- timestamp DATETIME
- status VARCHAR

Use Track all issuance and verification activity

A.5 Overall Workflow Summary

1. Admin/User enters certificate details in frontend form
2. Backend hashes the data → certHash
3. certHash + data sent to blockchain via smart contract (issueCertificate)
4. On verification
   - Input hashed again → certHash
   - Blockchain contract queried (verifyCertificate)
   - If match → Valid
5. All actions are logged in MySQL

APPENDIX-B

SCREENSHOTS

Fig B.1 – Sample Output Certificate Generated Using Blockchain-based Verification System

APPENDIX-C
ENCLOSURES

1. Journal publication/Conference Paper Presented Certificates of all students.

2. Include certificate(s) of any Achievement/Award won in any project-related event.

3. Similarity Index / Plagiarism Check report clearly showing the Percentage (%). No need fora page-wise explanation.

4. Details of mapping the project with the Sustainable Development Goals (SDGs).

BLOCKCHAIN- ENABLED ONLINE CERTIFICATE GENERATION AND VALIDATION SYSTEMS FOR GOVERNMENT ORGANISATIONS

A PROJECT REPORT

Submitted by,

PRAKRUTHI S - 20211CSE0628

DEEPTHI R -20211CSE0618

NIDHISHA N - 20211CSE0677

Under the guidance of,

Dr. ANAND PRAKASH

Associate Professor, School of Computer Science & Engineering

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

At

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY

BENGALURU

MAY 2025

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

CERTIFICATE

This is to certify that the Internship/Project report **"BLOCKCHAIN-ENABLED ONLINE CERTIFICATE GENERATION AND VALIDATION SYSTEMS FOR GOVERNMENT ORGANISATIONS"** being submitted by "PRAKRUTHI S, DEEPTHI R, NIDHISHA N" bearing roll number "20211CSE0628, 20211CSE0618, 20211CSE0677" in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering is a bonafide work carried out under my supervision.

Dr. ANAND PRAKASH
ASSOCIATE PROFESSOR
PSCS/PSIS
Presidency University

Dr. ASIF MOHAMMAD
ASSOCIATE PROFESSOR & HoD
PSCS
Presidency University

Dr. MYDHILI NAIR
ASSOCIATE DEAN
PSCS
Presidency University

Dr. SAMEERUDDIN KHAN
Pro-Vc School of Engineering
DEAN – PSCS/PSIS
Presidency University

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

DECLARATION

I hereby declare that the work, which is being presented in the report entitled " **BLOCKCHAIN- ENABLED ONLINE CERTIFICATE GENERATION AND VALIDATION SYSTEMS FOR GOVERNMENT ORGANISATIONS"** In partial fulfillment for the award of Degree of **Bachelor of Technology** in **Computer Science and Engineering**, is a record of my own investigations carried under the guidance of **Dr. ANAND PRAKASH, ASSOCIATE PROFESSOR, Presidency School of Computer Science and Engineering, Presidency University, Bengaluru.**

I have not submitted the matter presented in this report anywhere for the award of any other Degree.

NAME	ROLL NO	SIGNATURE
Prakruthi S	20211CSE0628	
Deepthi R	20211CSE0618	
Nidhisha N	20211CSE0677	

ABSTRACT

This study explores the potential of blockchain technology for developing transparent and secure certificate issuance and verification systems. These solutions attempt to combat certificate fraud, as well as ineffective verification systems, by leveraging blockchain's decentralization and immutability features. In addition to academic credentials, blockchain-based solutions captured an increasing number of fields where improved security and faster verification is needed. Further reduction of human control and increase of efficiency comes from automating the issuance and validation of certificates through smart contracts. This study also considers the use of blockchain in medicine and IoT applications, demonstrating how blockchain can safeguard digital records and its versatility. This paper captures the possibility of blockchain technology transforming certificate management while providing trust through a comprehensive examination of existing literature and practices.

ACKNOWLEDGEMENT

First of all, we indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our Honorable respected dean **Dr. Md. Sameeruddin Khan**, Pro-VC - Engineering and Dean, Presidency School of Computer Science and Engineering & Presidency School of Information Science, Presidency University for getting us permission to undergo the project.

We express our heartfelt gratitude to our beloved Associate Dean **Dr. Mydhili Nair,** Presidency School of Computer Science and Engineering, Presidency University, and **Dr. Asif Mohammad ,**Head of the Department, Presidency School of Computer Science and Engineering, Presidency University, for rendering timely help in completing this project successfully.

We are greatly indebted to our guide **Dr. Anand Prakash, Associate Professor** and Reviewer **Ms. Tintu Vijayan, Assistant Professor**, Presidency School of Computer Science and Engineering, Presidency University for his/her inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the internship work.

We would like to convey our gratitude and heartfelt thanks to the CSE7301 Internship/University Project Coordinator **Mr. Md Ziaur Rahman and Dr. Sampath A K,** department Project Coordinators **Mr. Jerrin Joe Francis** and Git hub coordinator **Mr. Muthuraj.**

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project.

Prakruthi S

Deepthi R

Nidhisha N