Blockchain-based Authentication and Verification System for Academic Certificate using QR Code and Decentralized Applications

Shivam Gangwar
Department of Electronics and Communication Engineering
University Institute of Engineering &Technology Kurukshetra,
Kurukshetra University Haryana, India- 136119

Anushka chaurasia
Department of Computer Science and Engineering
National Institute of Technology Meghalaya
Shillong India

ABSTRACT

Recently, the creation of fake degrees has become widespread, presenting a significant challenge to the current education system. Consequently, authenticating students' educational records when seeking admission to courses or applying for jobs has been deemed essential. Academic credentials have needed verification, which has often been time-consuming and has required third-party involvement. This paper includes a proposed approach known as a blockchain-based decentralized application (DAPP) to address these issues. The proposed architecture has comprised a front-end built with ReactJs, a back-end utilizing Ethereum 2.0, and a QR code verification process. In this proposed model, a QR code has been added to enable degree verification in minimal time. Smart contract management through Solidity and secure storage via the IPFS protocol have been seamlessly integrated into the system. This proposed method has been progressively implemented, examined, and verified on an Ethereum-like test network. The objective of this paper has been to reduce costs and combat fraudulent degrees. The results have indicated that the cost of issuing degrees using the proposed method is much lower than the traditional approach, with no server maintenance costs. The conclusion has emphasized the research's success in significantly enhancing the security of degree authentication and offering a cost-effective, scalable solution. This innovative system has set a new standard for academic credential verification, and the promising results have indicated that blockchain-based decentralized applications hold great potential for the future.

Keywords

Blockchain, Certificate Verification, Decentralized Application, QR Code

1. INTRODUCTION

Education, the journey of learning and growing, has been a part of human life for as long as we can remember. Imagine this: learning happened in small groups or communities early on. It was like having a wise elder or mentor sharing their knowledge with the folks around them. But as more and more people sought knowledge, our way of learning evolved, leading to the establishment of schools and universities. With this evolution, however, came a pressing challenge — ensuring that the certificates and degrees people earned were genuine. Remember when your teacher was not just someone at school but also your neighbor; everyone in your village knew each other. That's how education began, with trust built within close-knit communities. Fast forward to today, where people move around the world, attending various schools and colleges. Checking if someone's degree is legitimate has become quite complex. In the past, our parents or grandparents had paper certificates that proved they completed their studies, but in our current digital age, everything is online, and verifying the authenticity of a digital certificate isn't always straightforward. Fortunately, blockchain technology can be a protector for our digital era. Blockchain was introduced in 2008 as a peer-to-peer ledger recording Bitcoin transactions[1] [2]. Its decentralized design aimed to eliminate third-party intermediaries, enabling direct user-to-user transactions. Each node in the network holds a replica of the transaction ledger, writes entries upon receiving consensus, broadcasts user transactions to other nodes, and regularly verifies ledger consistency across the network. The blockchain structure consists of blocks linked in a chain, secured with cryptographic methods such as digital signatures and cryptographic hashes. Transactions are first sent to a Mempool, where miners validate them by solving mathematical problems, known as Proof of Work [3]. Once validated, the transactions are added to a block, and miners are rewarded. It is worth noting that blockchain technology can be used for more than just cryptocurrencies [4]. Its attributes, such as immutability, transparency, and trustworthiness, have been successfully employed in banking, transportation, education, medicine, and supply chains [5] [6] [7]. Despite still being in its early stages of development, researchers have investigated its potential in various fields, including certificate management, assessing students' abilities, and examination reviews.

The blockchain structure comprises two primary blocks, as depicted in Fig. 1. The initial block is called the header or the genesis block, containing no prior hash or transactions. It contains the previous block's hash, timestamp, and Merkle root [8]. The hash of blocks is generated with the help of SHA-256 because it accepts input files of any length and provides an output file of only 256 bits. Timestamp tells the time of block generation. Merkle Root

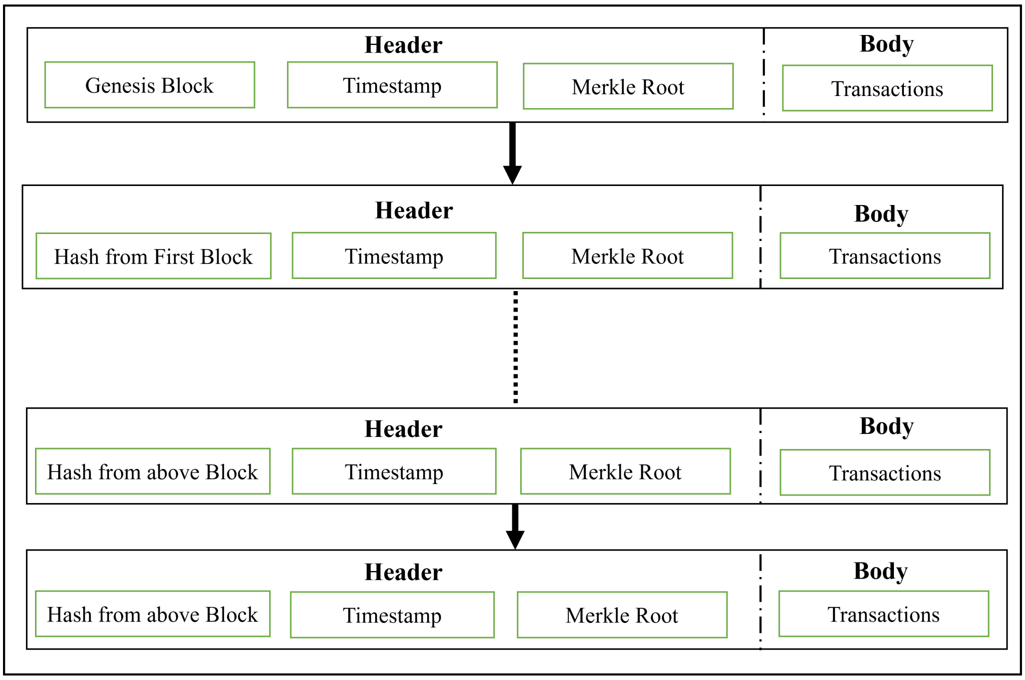


Fig. 1: Blockchain Structure.

gives the transaction count of all the blocks in a single hash. In the Bitcoin blockchain, each block's average generation time is 10 min, while in the Ethereum blockchain, each block's generation time is 12-14 sec. The second block, the body, contains only the transaction part. The Conventional education systems are now considering adopting the latest technology to enhance their effectiveness, recognizing the transformative potential of blockchain in modernizing educational processes. The educational system currently distributes the degree document at the end of the academic program as it is considered proof of completion of that degree [9][10][11]. Therefore, companies or higher education institutions may use degree documents to confirm applicants' educational histories. Every year, higher education institutions allocate substantial funds to manage inquiries for validating academic credentials, leading to the considerable task of diminishing both the financial burden and intricacy of confirming degrees. Since the time of Covid-19, the education system in our country has changed completely. Every university is moving towards digital technology, but digital technology works on centralized systems because centralized systems depend on the central server. However, due to heavy load, centralized systems become very slow. Another disadvantage of this system is that anyone can easily hack the university's data, such as the records of the students. This task is challenging as universities require secure data and a cost-effective, simplified degree verification process.

To address all the aforementioned issues, we have proposed a method that offers a solution aforementioned issue. The main objective of this research is to implement the use of DAPP technology based on Blockchain, which will enable the verification and issuance of degree certificates through QR codes. The ultimate goal of this approach is to significantly reduce the time and expenses involved in the production and verification processes. The main contributions of this manuscript are:

—To propose a secure and safe system for issuing and verifying degrees using blockchain technology.

—To incorporate DAPP to streamline issuing and verifying degree certificates.

—To integrate QR codes with the DAPP which reduces the time and cost of producing and verifying certificates.

The rest of this article is structured as follows: Section 2 analyzes various articles on blockchain-based education systems. Section 3 discusses an existing framework. Section 4 proposes a new framework. Section 5 presents the results and discussion. Section 6 concludes the paper and considers prospects.

2. RELATED WORK

In this section, we examine previous studies on using blockchain technology in education. We review related research papers and discuss them below. Cheng et al. [12] introduced a model that utilizes the Ethereum platform powered by EVM [13]. The model includes three types of users: service providers for system maintenance, certification units that issue certificates, and students who fulfill specific criteria. It employs a GUI, assigning a unique serial number and QR code to each student, verifies the data, and adds it to the Blockchain. Padmavati et al. [14] described a secure certificate validation process using GUI-based Remix, MetaMask and a solidity smart contract. Students log into the system to request a certificate, which is then verified and approved by the issuer. There are two types of users in this model: Admin and student. The admin stores data in blocks, issues certificates, and sends the hash to the students. Students can request and view the certificate. Gayathiri et al. [15] suggested a system that uses a mobile application for certificate validation. Techniques were used to convert a physical certificate into a digital image. They then generated a hash value and stored the certificates in the Blockchain. The mobile application performed the certificate validation to provide digital certificates. Jing Chen et al. [16] proposed an efficient Blockchain-based certificate audit. The author incorporated four layers - application layer, extension layer, network layer, and data layer - to create a certificate management system. The system model consists of four entities: client, domain, CAs, and Bookkeepers. They primarily evaluated three factors: Block generation speed, average Block size, and Block capacity. Vidal et al. [17] proposed a novel approach for certificate revocation on the Blockchain, utilizing Blockcerts Version 1.0. The revocation data is stored directly in the Blockchain, and a JSON file is linked to the certificate hash to facilitate the transfer of distributed resources, such as IPFS. The hash is generated using the SHA-256 algorithm, resulting in a fixed length of 32 characters. Despite its advantages, this system has a drawback in the form of a dual-payment system required for each revocation process. In another study Tariq et al. [18] proposed a blockchain-based solution to verify academic credentials effectively. It integrates with existing credential management systems, considers real-world threats, and offers features like data privacy, transcript verification, and selective data disclosure. A unique on-chain credential revocation mechanism using smart contracts is also proposed Wang et al. [19] [20] proposed a prototype system implemented in Firefox and Nginx. This system records certificates and their revocation status information in the global Blockchain. The majority of P2P nodes determine certificate validation. However, this system lacks formal security proof. SHIXION YAO et al. [21] suggested a Blockchain-based validation scheme of certificate status, addressing two main issues: the separation of revoked certificate control and storage plane and the design of an obfuscated response for privacy preservation for the clients. This was achieved by using PKI and maintaining a Merkle hash tree. This approach was found to be effective in security analysis and experimental evolution. A study done by fedorova et al. [22] suggest a blockchain technology in higher education, citing the benefits of decentralized open data, secure information storage, and reduced transaction costs. It examines case studies from MIT and Sony Global Education, and highlights the University of Nicosia's pioneering use of smart contracts and cryptocurrency. It also explores blockchain's role in massive open online courses and its potential in Russia's educational system. Overall, the literature suggests that while significant strides have been made in applying Blockchain technology for certificate validation, there are still areas to explore and challenges to overcome. Specifically, the balance between efficient validation processes, using QR codes, user-friendliness, and robust security remains an ongoing study area. Upon conducting a literature review, we have identified a research gap. Thus, the primary objective of this paper is to introduce a decentralized blockchain-based DAPP system that can authenticate a student's data through the use of their degree certificate number and QR code, and subsequently provide their degree certificate. The proposed framework, DAPP, revolutionizes the issuing and accessing of academic degree certificates. Students can access immutable and tamper-resistant digital certificates through the platform, eliminating the need for physical copies. Sharing credentials with employers or universities becomes effortless. This innovation reduces costs for institutions, as there's no requirement for maintaining servers. Verification of degree certificates is simplified for employers, saving time and effort. The DAPP operates on Web 3.0, using React.JS for high-speed performance and a user-friendly interface. Even non-tech-savvy individuals can easily understand and utilize the system. The DAPP streamlines certificate management, making it secure, efficient, and accessible for all stakeholders.

3. EXISTING FRAMEWORK

The prevailing system of distributing certificates to students poses verification hurdles in today's digital era. Physical certificates are not readily adaptable to digital validation, paving the way for potential deceit. Once these credentials are issued, bridging the gap between students, institutions, and their awarded certifications becomes challenging. This disconnect can create obstacles when cross-checking candidates' academic histories for job roles. Often, the validation method is manual, leading to time-consuming checks and heightened risks of alteration. While certain institutions have ventured into digital certificate storage, the absence of time-stamping and centralized storage compromises their security. Fig. 2 illustrates the current procedure, from a student's enrollment to confirming a graduate's qualifications by potential employers.

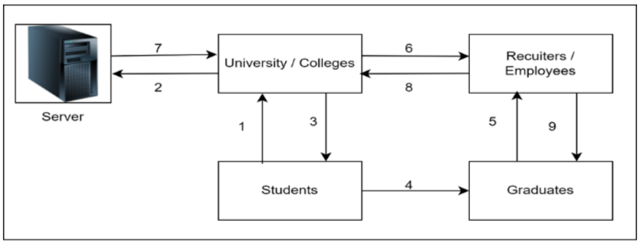


Fig. 2: Existing Framework.

Here are the different stages involved in the process:

(1) **Admission:** Students are admitted to a university, affiliated college, or autonomous college.

(2) **Results:** The results are stored in a register or server after the semester or year-end exams.

(3) **Degree:** The marks statements or original degrees in paper form are issued.

(4) **Graduation:** The students are now graduates with degrees.

(5) **Job placement:** Employers or recruiters offer suitable jobs to graduates.

(6) **Verification request:** Companies ask educational institutions to confirm an employee's qualifications.

(7) **Data retrieval:** Universities access information from the primary database or main server to confirm its authenticity.

(8) **Validation:** The given data is compared with the retrieved data to validate and report to the employer.

(9) **Confirmation/rejection:** The graduate's appointment is either confirmed or cancelled based on the received report.

4. PROPOSED METHODOLOGY

This section elucidates the proposed architecture for an educational system and the workflow of degree issuance and verification through a decentralized application. The credential validation and accreditation process has been broken down into a life cycle involving several key players and stages. An authoritative accreditation organization has collaborated with multiple parties, such as educational institutions and monitoring groups (e.g., watchdogs and citizen organizations), to operate a specialized, permissioned blockchain network. In this system, universities have sent transactions containing essential information that validates the credentials

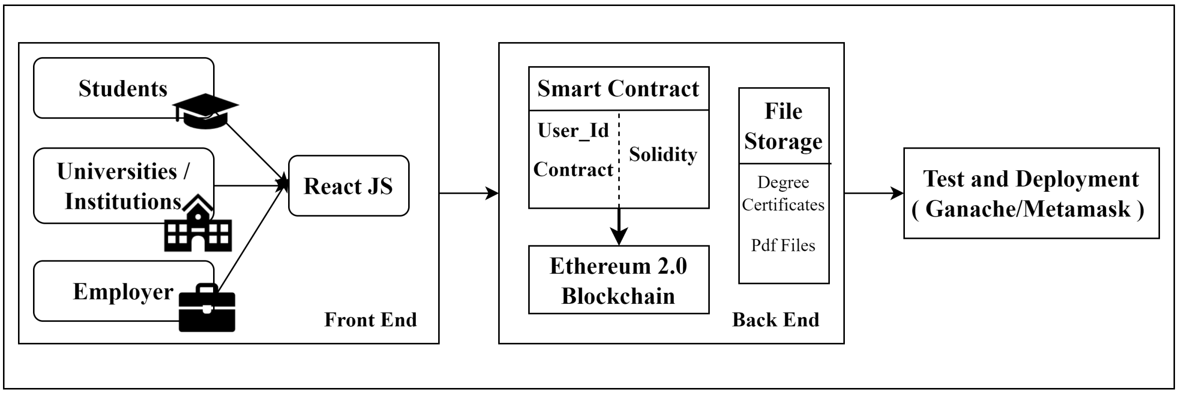


Fig. 3: Proposed Architecture for Decentralized Application for an Educational System.

awarded to students. These transactions have been gathered periodically by the accreditation organization and assembled into blocks, which have then been appended to the blockchain. Various spectator groups have been engaged to oversee the entire process, ensuring integrity and proper compliance with standards.

Upon a student's graduation, the university has issued both a physical degree certificate and an accompanying transcript. Simultaneously, the university administration has crafted a transaction that includes a digital representation (or fingerprint) of the student's credential details. This digital fingerprint and similar details for other graduates have been encrypted and digitally authenticated by the university's registrar. It has subsequently been broadcast on the designated network (e.g., the Cerberus network), where nodes associated with the accreditation organization have validated it. Once verified, it has been mined into a block and annexed to the existing blockchain, marking the official issuance and accreditation of the credential.

The tangible degree certificate given to the student, referred to here as Alice, has been printed with a QR code. This code enables swift verification of the certificate's authenticity. Should an employer, Bob, wish to confirm Alice's degree, he can scan the QR code through a mobile app or access it via a web portal. These platforms connect to the Cerberus network in real-time, retrieving and authenticating the necessary information linked to the QR code and the degree. Alice has had the ability to enhance her resume with a QR code, which permits others to confirm her degree without the need for the physical certificate. If necessary, the university can initiate a dedicated revocation transaction to revoke Alice's degree. Once this transaction has been confirmed and added to the blockchain by the accreditation body, any future attempts by Bob or others to verify Alice's degree will result in a notification that the degree has been officially revoked.

This outlined procedure also paves the way for additional features and functionalities, as detailed further in the solution. The entire life cycle demonstrates a robust, transparent, and efficient method for managing, issuing, and verifying educational credentials, employing the potential of blockchain technology.

4.1 Proposed Architecture

This section discussed the proposed methodology of designing a decentralized application (DAPP) based on blockchain [23] to issue and authenticate degree certificates. The DAPP architecture primarily comprises two essential components: the front end, or client side, and the back end, or server side. Moreover, there is an essential testing and deployment element that aids in the transition and assembly of smart contracts.

Fig. 3 depicts the suggested DAPP framework for educational systems. This architecture depicts the different components and their interconnectivity. The first component is the Front end which serves as the primary point of interaction for all users, accessible through their preferred browser. ReactJS [23]is an optimal technology for this particular component, although it is possible to integrate other options such as Angular or Vue with Drizzle. In order to establish a connection between the application and the blockchain, it is crucial to have a browser extension in place. Additionally, an API is utilized to facilitate seamless communication between the client side and the application. The second component is the backend which utilizes Blockchain technology Ethereum2.0 [24] . Furthermore, this architecture has the capability to utilize other Blockchains such as Hyperledger or Tron, depending on the specific needs of our users. For the management of smart contracts, Solidity language [25] is used, which is specifically designed for the Ethereum platform, and for the secure storage of multimedia files such as documents and images, IPFS protocol [21] is used that creates a unique hash key for each file and stores it in the blockchain, which not only enhances security but also ensures optimal efficiency. The last component is the test and deployment that is supported by a local blockchain along with the assistance of Ganache. This allows for a seamless and reliable running of the application before it is officially launched. We take the necessary steps to ensure that the application has been thoroughly tested and verified to be functioning correctly so that we can proceed to implement it on the Mainnet. By doing so, we are able to provide a robust and reliable platform for our users [26] [27].

4.2 Proposed Workflow through DAPP

The proposed workflow has been segmented into two essential parts: degree issuance and verification. Three categories of participants have been involved: issuers, recipients, and verifiers. The issuer refers to the university authority responsible for issuing degree certificates and adding data to the blockchain. Each educational institution has possessed a distinct blockchain smart contract address, ensuring that their data is kept in separate blockchain networks specific to that institution. It is crucial to note that the information on the degree certificate has been made permanent and cannot be altered, updated, or removed by the issuer or any other party. Once this information has been established, it provides robust security and remains impervious to unauthorized modifications or hacks. The individual receiving the degree certificates is the recipient. They can retrieve their certification by inputting the certificate number into the Decentralized Application (DAPP) platform, and their certificate will be promptly displayed. This method has been user-friendly, offering immediate access to genuine credentials. Lastly, the verifier, who could be an employer or recruiter, verifies the authenticity of a certificate. They can do so by entering the certificate number on a DAPP or scanning the QR code. Until recently, students and verifiers had to rely on traditional methods, which involved physically submitting and collecting educational certificates. However, with the advent of this decentralized application, validators have been able to confirm the validity of certificates with greater ease and efficiency.

4.2.1 Degree Issuance through DAPP. Fig. 4 illustrates the workflow for degree Issuance, where students, referred to as recipients, request a digital degree certificate from the university authority. The issuer then enters all degree-related details into the proposed DAPP platform. Subsequently, the DAPP generates a digital degree certificate with a QR code. The issuer meticulously verifies all degree-related information before uploading it to the blockchain. If discrepancies are found, the issuer re-issues the digital degree certificate with a QR code. However, if all details are confirmed as accurate, the process moves forward. The DAPP stores data on the blockchain via smart contracts and embeds the transaction hash key into the digital degree certificate with a QR code upon a successful transaction. Once the final degree is issued, the university authority delivers the digital degree certificate to the student.

Algorithm 1 Creating the Degree Certificate

```
Input: PassingYear, Nameofdegree, name, division, rollno, stream, certificateNo
if adminList[msg.sender] == true then
    require PassingYear.length > 0
    require Nameofdegree.length > 0
    require name.length > 0
    require division.length > 0
    require rollno.length > 0
    require stream.length > 0
    require certificateNo.length > 0
    if all requirements are satisfied then
        certificateMapped[certificateNo] = studentData[Input]
    else
        revert “Not allowed to create certificate”
    end if
end if
```

Algorithm. 1 outlines a ”Certificate Creation Algorithm” designed for a system where authorized administrators can issue student certificates. The algorithm takes several input parameters, including PassingYear, Nameofdegree, Name, division, roll no, stream, and certificate No. To ensure that only authorized administrators can create certificates, the algorithm checks whether the sender of the transaction (msg.sender) is listed in the ”adminList” as true. If not, the process halts, and the certificate creation is denied. Subsequently, it verifies that all the required input parameters have valid values (i.e., their lengths are greater than zero) using ”require” statements. If any required field is empty, the algorithm reverts with an error message, preventing certificate creation. If all the requirements are met, the algorithm creates a certificate by mapping the certificate number (certificateNo) to the relevant student data provided in the input.

4.2.2 Degree Verification through DAPP. Fig. 5 displays the process of degree verification using a Decentralized Application (DAPP) and QR code. Validators or students can confirm the legitimacy of a degree certificate's details through DAPP by submitting the certificate number for verification. Upon submission, DAPP cross-references the certificate number with data stored on the Ethereum 2.0 blockchain. If the degree certificate is authentic, all relevant details will be returned. If the degree certificate is not valid, a ”not verified” message will be displayed. Additionally, the authenticity of the degree certificate can be assessed by scanning its associated QR code. If the degree certificate is legitimate, scanning the QR code will provide all pertinent details. If the degree is invalid, a ”not verified” message will be shown. Algorithm 2 is a ”Certificate Verification Algorithm” designed to validate the authenticity of a certificate using its unique certificate number (certificateNo). Upon receiving the certificate number as input, the algorithm calls the function ”certificateMapped(certificateNo).” This function is expected to retrieve the associated data from the ”certificateMapped” data structure, which likely contains information about the student to whom the certificate was issued, such as their Name, degree, passing year, and other relevant details. If the certificate number is found in the mapping (i.e., the certificate exists and is valid), the algorithm returns the corresponding ”studentData,” thereby confirming the certificate's authenticity. Conversely, if the certificate number is not present in the mapping, the algorithm returns ”Not verified,” indicating that the certificate is either invalid or not registered in the system.

Algorithm 2 Degree Certificate Verification

```
Input: certificateNo
Calling function certificateMapped(certificateNo)
if certificate is already mapped then
    return “studentData”
else
    return “Not verified”
end if
```

5. RESULT AND DISCUSSION

A framework has been created utilizing React JS for the frontend, Node JS for the backend, and Solidity for creating contract certificates. The application has been tested on the Ganache and Goerli test networks. All transactions have been executed through a publicly available smart contract on Goerli Etherscan. When transactions are conducted with a Metamask wallet, they can be viewed on Goerli Etherscan. Similarly, when transacting on Ganache, all transactions become visible on Ganache. This feature has enabled tracking transaction addresses and activities on the Ethereum blockchain. The ABI is required to interact with smart contracts deployed in Ethereum. Therefore, without the smart contract address and ABI, it has been impossible for anyone to engage with this creation and verification procedure. Consequently, fraudsters and scammers have been unable to access or manipulate this system.
Tables 1 to 4 depict the process of deploying a smart contract, while Fig 4 displays the final degree certificate. This includes a status block that provides the transaction's outcome, indicating whether it has been successfully executed. Each transaction has been assigned a unique identifier, known as a transaction hash or transaction ID

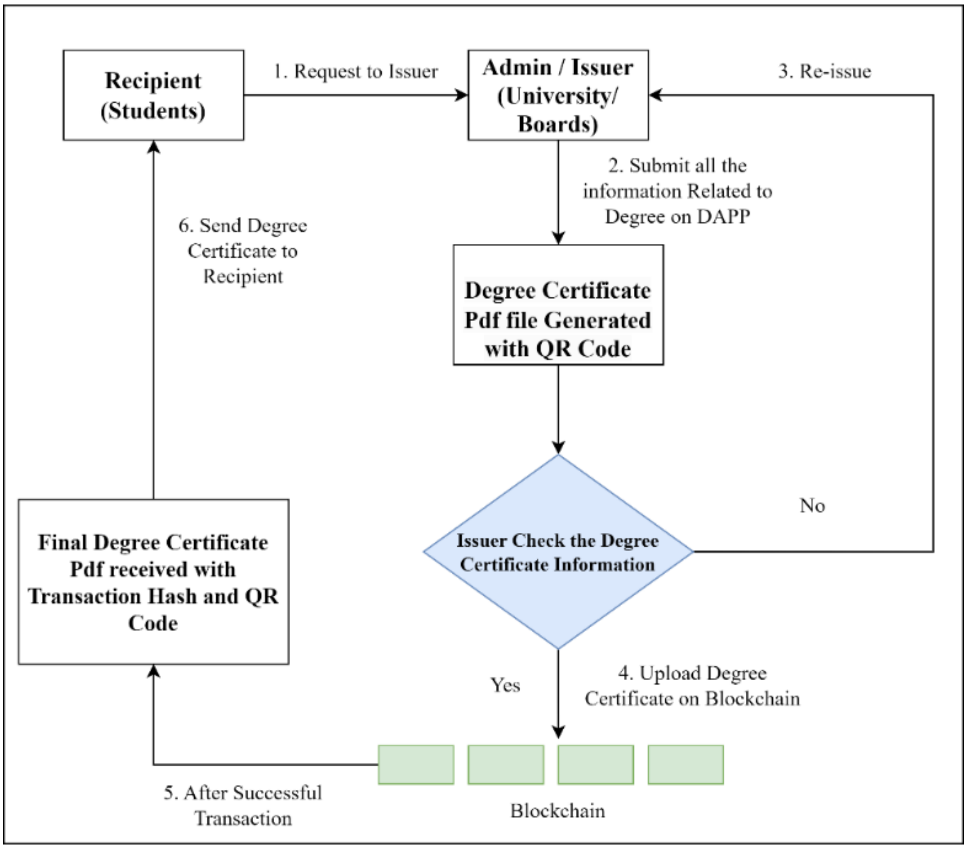

Recipient (Students)
1. Request to Issuer
Admin / Issuer (University/ Boards)
3. Re-issue
2. Submit all the information Related to Degree on DAPP
6. Send Degree Certificate to Recipient
Degree Certificate Pdf file Generated with QR Code
No
Final Degree Certificate Pdf received with Transaction Hash and QR Code
Issuer Check the Degree Certificate Information
Yes
4. Upload Degree Certificate on Blockchain
5. After Successful Transaction
Blockchain

Fig. 4: Workflow for Degree Issuance through DAPP.

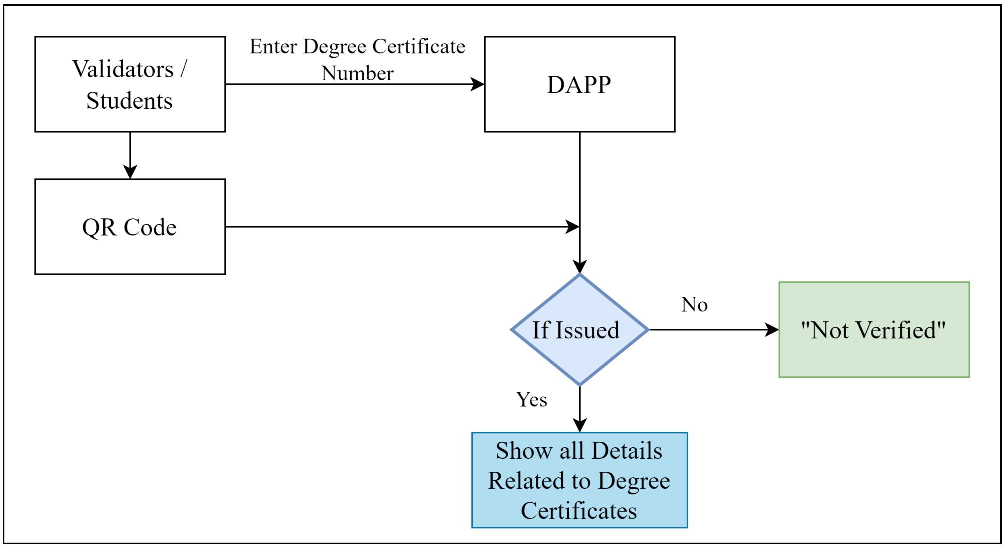

Validators / Students
Enter Degree Certificate Number
DAPP
QR Code
If Issued
No
"Not Verified"
Yes
Show all Details Related to Degree Certificates

Fig. 5: Workflow for Degree Verification through DAPP and QR Code.

when added to the blockchain. This identifier has been generated by applying a cryptographic hash function to the transaction data, yielding a fixed-length string of characters. This hash has served as a distinctive fingerprint for the transaction, enabling users to look up and confirm the transaction on the blockchain. The ’from’ parameter indicates the originating user, while ’to’ represents the

Table 1. : Successful Transaction for Smart Contract Deployment.

status	true Transaction mined and execution succeed
transaction hash	0x4808dda6af22ed31651766afdff665734152cf86acaefc3956aadc26033607e0
block hash	0x0e074744d060534f308f86c9661c82116173c57f0f1c6f0071ca5d5c321a05f8
block number	9646258
contract address	0xD546A399b3d8ce8AbEeb3Cfa88218FA767093400
from	0x309691734cf04E950172454cB140e14E89785A5b
to	DMCgeneration.(constructor)
gas	1282357 gas
transaction cost	1282357 gas
input	0x608...20033
decoded input	{}
decoded output	-
logs	[]
val	0 wei

recipient. The 'gas' parameter refers to the computational effort required to execute operations. The term 'input' denotes the data transmitted during a transaction while interacting with a smart contract. When a smart contract has been deployed, the input has encompassed the contract's compiled bytecode, along with any constructor parameters. Given that smart contracts often involve encoded complex data types for efficiency, the 'decoded input' function has transformed this encoded data into a more comprehensible format. 'Decoded output' refers to the human-readable version of raw output data resulting from a smart contract function call. It signifies that the data returned by the smart contract could range from the result of a computation to the value of a state variable and other related information. 'Logs' have provided a means to trigger and record pertinent information regarding the execution of smart contracts. The 'value' field comes into play when a cryptocurrency transfer (such as Ether in the Ethereum network) is involved in the transaction. For instance, if the function being called has necessitated a certain payment or if a contract has been deployed that required sending some cryptocurrency along with it, the amount has been specified in the 'value' field.

The smart contract deployment process has been crucial in this research work as it is the primary function. Fig. 5 has demonstrated this process. The code for the smart contract has been written in Solidity. As per the proposed method, a smart contract has been created for DMC generation. The execution and deployment of the code have been straightforward if it has no errors. However, the code could not be executed and deployed if there have been any errors. This deployment process has been the initial step in blockchain technology. 2 has illustrated a transaction conducted on the Ethereum blockchain, wherein an individual or entity has engaged with the DMCgeneration smart contract to include a new administrator. This transaction has exemplified the fundamental attributes of smart contracts, which possess both dynamic and permissioned qualities. These contracts have had the capacity to perform specific operations, such as appointing an administrator, thereby facilitating alterations to the state of the contract. The DMCgeneration contract has enabled the dynamic incorporation of administrators by means of the addAdmin function, thereby establishing a decentralized and permissioned governance mechanism. The aforementioned attributes have highlighted the inherent capacity of blockchain technology to enable the establishment of robust, accountable, and flexible systems capable of accommodating dynamic requirements.

Table. 3 illustrates a transaction conducted on the Ethereum blockchain. This transaction involves an individual or entity interacting with the DMCgeneration smart contract to create and register a new educational certificate. The use of blockchain technology in digitalizing and securing academic credentials is exemplified through this transaction. It demonstrates how blockchain can be innovatively used in the educational sector. Institutions can use the createCertificate function of the DMCgeneration contract to digitalize, register, and secure academic certificates on the Ethereum blockchain. The certificateAdded event is emitted, which provides an additional layer of validation by confirming the successful addition of a certificate. The hash associated with the logs serves as a unique identifier that ensures the certificate's authenticity and immutability. This approach not only protects academic credentials from tampering but also simplifies the verification process for employers and other stakeholders.

Table 4 presents a transaction on the Ethereum blockchain. Information about an educational certificate has been requested using its unique identifier through the DMCgeneration smart contract. This has demonstrated how blockchain technology can ensure that educational qualifications are genuine and immutable. The Ethereum address has identified the person or entity who initiated the transaction, serving as a unique identifier for individuals within the blockchain system. The "To" Ethereum address has represented the DMCgeneration smart contract. The Ethereum network has utilized a unique identifier for smart contracts that manage and authenticate educational certificates. The certificateMapped (string) function in this transaction indicates that the user intended to verify the certificate using its unique identifier. The input has been the specific

Table 2. : Successful Transaction for Adding Address of Admin

status	true Transaction mined and execution succeed
transaction hash	0x606e1cc78c905011b9667d0472567bf07316977fdc0134ef804bc76a15d837be
block hash	0xb67e35c044f2f97b289a3cfe224df9ed7999c46f0432051ec8382de21ae2f31a
block number	9646275
from	0x309691734cf04E950172454cB140e14E89785A5b
to	DMCgeneration.addAdmin(address) 0xD546A399b3d8ce8AbEeb3Cfa88218FA767093400
gas	26714 gas
transaction cost	24526 gas
input	0x704...85a5b
decoded input	{ ”address newAdmin”: ”0x309691734cf04E950172454cB140e14E89785A5b” }
decoded output	-
logs	[]
val	0 wei

Table 3. : Successful Transaction for Degree Certificate Generation process.

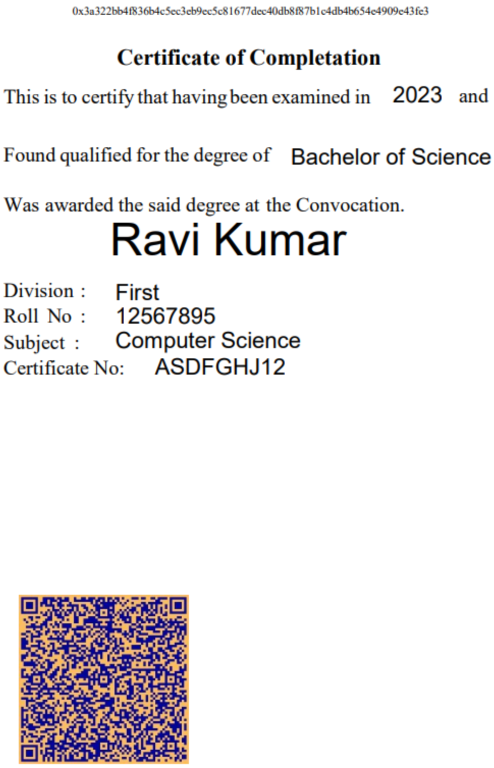
Status	Transaction mined and execution succeed
Tx Hash	0x3a322...e43fe3
Block Hash	0x5a346...8a5aaf
Block No.	9646278
From	0x309691...85A5b
To	DMCgeneration.createCertificate(...) 0xD546A399b3d8ce8AbEeb3Cfa88218FA767093400
Gas	191021 gas
Tx Cost	191021 gas
Input	0xd06...00000
Decoded Input	{ ”uint256 _PassingYear”: ”2023”, ”string _Nameofdegree”: ”Bachelor of Science”, ”string _name”: ”Ravi Kumar”, ”string _division”: ”First”, ”uint256 _rollno”: ”12567895”, ”string _stream”: ”Computer Science”, ”string _certificateNo”: ”ASDFGHJ12” }
Decoded Output	-
Logs	[{ ”from”: ”0xD546A399b3d8ce8AbEeb3Cfa88218FA767093400”, ”topic”: ”0xb0c07c...d1d8cb02”, ”event”: ”certificateAdded”, ”args”: { ”0”: { ”_isIndexed”: true, ”hash”: ”0x6ade...3dadb2d” } } }]
Val	0 wei

identifier assigned to the certificate requiring verification. In this example, ”ASDFGHJ12” has been used to retrieve the corresponding information. The output displayed the details retrieved from the smart contract based on the given input parameter.

Fig. 6 shows the certificate that is generated after degree issuance of the student from the college. The certificate contains the pass-out year, degree name, roll no., Name, division, and certificate number of the student. The recruiters can verify the certificates using the QR code mentioned in the certificate and using the hash key whenever required. Even recruiters can also verify the generate details on Goerli etherscan.io by entering the hash code that is printed on the top of generated certificate “0x3a322bb4f836b4c5ec3eb9ec5c81677dec40db8f87b1c4db4b654e4909e43fe3”.

Table 4. : Successful Transaction for Degree Certificate Verification.

From	**0x309691734cf04E950172454cB140e14E89785A5b**
To	**DMCgeneration.certificateMapped(string) 0xD546A399b3d8ce8AbEeb3Cfa88218FA767093400**
Input	**0xf7f...00000**
Decoded Input	**{ ”string ”: ”ASDFGHJ12” }**
Decoded Output	**{ ”0”: ”uint256: PassingYear 2023”, ”1”: ”string: Nameofdegree Bachelor of Science”, ”2”: ”string: name Ravi Kumar”, ”3”: ”string: division First”, ”4”: ”uint256: rollno 12567895”, ”5”: ”string: stream Computer Science”, ”6”: ”string: certificateNo ASDFGHJ12” }**
Logs	**[]**



0x3a322bb4f836b4c5ec3eb9ec5c81677dec40db8f87b1c4db4b654e4909e43fe3

Certificate of Completation

This is to certify that having been examined in 2023 and

Found qualified for the degree of Bachelor of Science

Was awarded the said degree at the Convocation.

Ravi Kumar

Division : First
Roll No : 12567895
Subject : Computer Science
Certificate No: ASDFGHJ12

Fig. 6: Generated Degree Certificate.

6. CONCLUSION

The research demonstrates the potential of a blockchain-based DAPP in transforming degree certificate verification. This paper achieves its first objective by progressively implementing the proposed model and the developed DAPP, analyzed and verified on an Ethereum-like test network. The architecture consists of a front end (using ReactJS), a back end (leveraging Ethereum2.0), testing and deployment components, and smart contract management with Solidity, and secure storage via IPFS protocol. A unique QR code verification process enhances security, aiming to eliminate mediators, reduce costs, and combat fake educational degree certificates. The financial implications associated with the implementation of the proposed decentralized application is meager, less than a dollar, without server maintenance expenses, highlighting the power of using Web3js, React, and Ethereum to build decentralized applications. A systematic explanation of the proposed smart contract and the application development environment is presented. The thorough testing and verification phase confirmed the robustness and reliability of the platform, and the DAPP shows promising potential in combating fraudulent degrees. This innovative approach significantly enhances the security of degree authentication and represents a cost-effective, scalable solution, setting a new standard for academic credential verification. In the future, the provision of document integrity can be expanded not only within the educational field but also to governmental sectors that necessitate a digital document timestamp. The blockchain-based decentralized applications hold great promise for the future, and further customization and integration with various educational and professional institutions could expand their applicability and effectiveness across different domains. In the future, we can include an email ID option in the proposed DAPP platform. This will simplify the certification generation process by automatically sending the certificate to the particular student as soon as it is generated. Currently, we are manually filling in the students' details. However, in the future, we can integrate this platform into the cloud network. This will enable the automatic addition of university-wise student data and the generation of degree certificates.

7. REFERENCES

[1] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” *International journal of web and grid services*, vol. 14, no. 4, pp. 352–375, 2018.

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[3] Y. Himeur, A. Sayed, A. Alsalemi, F. Bensaali, A. Amira, I. Varlamis, M. Eirinaki, C. Sardianos, and G. Dimitrakopoulos, “Blockchain-based recommender systems: Applications, challenges and future opportunities,” *Computer Science Review*, vol. 43, p. 100439, 2022.

[4] C. Holotescu, “Understanding blockchain opportunities and challenges,” in *Conference proceedings of eLearning and*

Table 5. : List of Abbreviations

API	Application Programming Interface
DAPP	Decentralized Application
EVM	Ethereum Virtual Machine
GUI	Graphical User Interface
IPFS	Interplanetary File System
JSON	JavaScript Object Notation
POW	Proof of Work
P2P	Peer to Peer
PKI	Public Key Infrastructure
QR CODE	Quick Response Code
SHA-256	Secure Hash Algorithm-256

Software for Education (eLSE), vol. 14, pp. 275–283, Carol I National Defence University Publishing House, 2018.

[5] P. P. Bokariya and D. Motwani, "Decentralization of credential verification system using blockchain," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 10, no. 11, 2021.

[6] M. S. Zulfiker, N. Kabir, A. A. Biswas, P. Chakraborty, and M. M. Rahman, "Predicting students' performance of the private universities of bangladesh using machine learning approaches," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 3, pp. 672–679, 2020.

[7] E. Nyaletey, R. M. Parizi, Q. Zhang, and K.-K. R. Choo, "Blockipfs-blockchain-enabled interplanetary file system for forensic and trusted data traceability," in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 18–25, IEEE, 2019.

[8] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-based applications in education: A systematic review," *Applied Sciences*, vol. 9, no. 12, p. 2400, 2019.

[9] K. D. Kumar, P. Senthil, and D. Kumar, "Educational certificate verification system using blockchain," *international journal of scientific & technology research*, vol. 9, no. 3, pp. 82–85, 2020.

[10] S. Pathak, V. Gupta, N. Malsa, A. Ghosh, and R. Shaw, "Blockchain-based academic certificate verification system—a review," *Advanced Computing and Intelligent Technologies: Proceedings of ICACIT 2022*, pp. 527–539, 2022.

[11] T.-T. Kuo, H. Zavaleta Rojas, and L. Ohno-Machado, "Comparison of blockchain platforms: a systematic review and healthcare examples," *Journal of the American Medical Informatics Association*, vol. 26, no. 5, pp. 462–478, 2019.

[12] J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen, "Blockchain and smart contract for digital certificate," in *2018 IEEE international conference on applied system invention (ICASI)*, pp. 1046–1051, IEEE, 2018.

[13] L. S. Barbosa and S. A. Shaikh, "Selected contributions from the open source software certification (opencert) workshops.," *Sci. Comput. Program.*, vol. 91, pp. 139–140, 2014.

[14] P. E. Gundgurti, K. Alluri, P. E. Gundgurti, G. Vaishnavi, *et al.*, "Smart and secure certificate validation system through blockchain," in *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 862–868, IEEE, 2020.

[15] A. Gayathiri, J. Jayachitra, and S. Matilda, "Certificate validation using blockchain," in *2020 7th International Conference on Smart Structures and Systems (ICSSS)*, pp. 1–4, IEEE, 2020.

[16] J. Chen, S. Yao, Q. Yuan, K. He, S. Ji, and R. Du, "Certchain: Public and efficient certificate audit based on blockchain for tls connections," in *IEEE INFOCOM 2018-IEEE conference on computer communications*, pp. 2060–2068, IEEE, 2018.

[17] F. R. Vidal, F. Gouveia, and C. Soares, "Revocation mechanisms for academic certificates stored on a blockchain," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1–6, IEEE, 2020.

[18] A. Tariq, H. B. Haq, and S. T. Ali, "Cerberus: A blockchain-based accreditation and degree verification system," *IEEE Transactions on Computational Social Systems*, 2022.

[19] Z. Wang, J. Lin, Q. Cai, Q. Wang, D. Zha, and J. Jing, "Blockchain-based certificate transparency and revocation transparency," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 681–697, 2020.

[20] S. Yao, J. Chen, K. He, R. Du, T. Zhu, and X. Chen, "Pbcert: Privacy-preserving blockchain-based certificate status validation toward mass storage management," *IEEE Access*, vol. 7, pp. 6117–6128, 2018.

[21] S. K. Shawon, H. Ahammad, S. Z. Shetu, M. Rahman, and S. A. Hossain, "Diucerts dapp: A blockchain-based solution for verification of educational certificates," in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp. 1–10, IEEE, 2021.

[22] E. P. Fedorova and E. I. Skobleva, "Application of blockchain technology in higher education.," *European Journal of Contemporary Education*, vol. 9, no. 3, pp. 552–571, 2020.

[23] A. Mardan, Mardan, and Corrigan, *Practical Node. js*. Springer, 2018.

[24] Dimensions Network, "Ropsten ethereum (reth) faucet," 2021. [Online]. Accessed: 08-Mar-2021.

[25] Solidity Documentation, "Solidity documentation," 2023. Last accessed on 2020-12-01 at 1:00 PM.

[26] O. S. Saleh, O. Ghazali, and N. B. Idris, "A new decentralized certification verification privacy control protocol," in *2021 3rd International Cyber Resilience Conference (CRC)*, pp. 1–6, IEEE, 2021.

[27] P. Vallejo Seade, "Asset tokenization in real estate through the means of token standards available on the ethereum blockchain," 2022.