International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Design and Implementation of a Blockchain-based Certificate Generation and Validation Framework using PHP

[1]Dr. C. Kalpana , [2]Dr. Manoj Devare , [3]Mayank

AIIT, Amity University, Maharastra

ckalpana@mum.amity.edu mhdevare@mum.amity.edu mayank5@s.amity.edu

ABSTRACT

The dependency with respect to digital certification systems is steadily rising up in thousands of industries, where efficiency in traditional practices of issuing certificates is found to be quite weak.Paper certificates have the disadvantage that they can be forged as well as lost, and they are easily damaged. Central storage in digital format also poses similar threats, among them are cyber undertakings unauthorized change of data, and operational inefficiency..Such limitations are some of the major hurdles with which institutions, employers, and regulators grapple to check the validity of qualifications.The paper finally offers an alternative; set up a service based upon blockchain technology and incorporated with a PHP Web application so that digital certificates could be securely generated and validated.In short, a new system based on the blockchain refers to an idea proposed in this report for a tool intended for creating or verifying automated certificates through PHP.Through the inherent properties of the blockchain like immutability, decentralization and transparency, this system guarantees that the certificates so provided are going to be tamperproof and verifiable without the need of centralized authorities. The interface is user-friendly which will enable the issuer to input the details of the certificate, generate cryptographic hashes and store these hash on a blockchain network with the help of the PHP application. Then a verifier can use the same hashes and cross reference in real time to find out if a presented certificate is authentic. Thus, decentralization of the system increases confidence, optimizes efficiency in operations and minimizes costs. Administrative overhead amounts to that. Smart contracts also automate the management of certificate data for retrieval, making them consistent, reducing human error, and enhancing the reliability of the system. The present research provides a scalable, secure, and efficient model for managing digital credentials that could end up being used in many more applications such as licensing health practitioners, academic degrees, government records, and professional certifications. Indeed, the proposed solution has a huge capability to solve the problems that traditional credentialing has.

Index terms – Blockchain , certificate generation , certificate validation , PHP web application

Digital certificate , secure credential , verifiable credential

I. Introduction

The needs of credential verification in various fields like education, healthcare, professional certifications, and government services cannot be overemphasized. Traditionally, certificates were issued in physical formats that were susceptible to loss, depreciation, and worse, forgery. With the sweep towards digitization, organizations have started setting up centralized credential repositories. But centralized databases, though full of promise, suffer from fundamental flaws such as security weaknesses, unauthorized data alterations, and a lack of transparency [1].

It poses serious threats to institutions, heads' employers, and credential verification bodies. The current ways of authenticating documents are costly and prone to manual processes, including having to communicate with the original issuing authority, which results in delays and errors [2]. Traditional systems suffer from many inefficiencies and risks that have triggered greater interest in finding a better, more reliable, transparent, and secure method of managing digital certificates.

The concept of blockchain technology has initially been brought up with reference to Bitcoin [3]. The incredible weapon that was forged by this rising technology. Blockchain refers to a distributed ledger in which every transaction is secured cryptographically and linked to previous entries thereby making unauthorized modifications close to impossible [4]. These are features central to decentralization, immutability, and openness, making blockchain a truly excellent platform for developing secure, tamper-proof credential verification systems.

This research discusses the design and implementation of a decentralized certificate generation and validation system that integrates blockchain technology and PHP-based Web platform. PHP, a popular web development language, provides a solid backend structure to handle the interaction of users with blockchain services[5]. Certificate issuers generate digital certificates within their model, compute their cryptographic hashes, and record these on the blockchain; all verifiers then query the blockchain to confirm the authenticity of any certificate without relying on intermediaries.

The system ensures data integrity and accessibility due to the strength of blockchain and PHP. Secure hashing algorithms such as SHA-256 guarantee that modifications cannot be done without authorization, and a blockchain's distributed entry prevents a single point of failure [6]. Smart contracts, programs that are automatically executed when certain preconditions are met, may also serve to facilitate certificate storage and validation, thereby increasing efficiency and minimizing human interference [7].

Credential management systems on the blockchain provide various benefits, unlike security benefits only; it also benefits from decentralized working. Different institutions and verifiers can independently verify the validity of certificates. Trust among stakeholders strengthens even more because these records are unchangeable and publicly verifiable [8]. Such a scaling system can also work beyond education: health licensing, aviation certification, government-issued identities, and corporate compliance systems.

Digital credentials, like what the world has gone to, must be reliable, transparent, and secure. the study will now present an alternative to provide a solution for the core problems all faced under the old method-a certificate management system powered by PHP, but more importantly, blockchain technology. Existing literature review, proposed solution architecture description, implementation of the system, interaction with smart contracts, and concluding observations full on system performance and improvements will follow.

II. Objectives of the Study

This research focuses on the development of a secure, transparent, and decentralized certificate generation and verification system using blockchain technology. The objective here is the integration of a PHP-based web application that allows a convenient interaction between certificate issuers and verifiers. By means of Ethereum smart contracts, the system oversees the automatic processes of issuance, certificate retrieval, and verification, thus decreasing manual procedures and possibilities of human error. Another goal is to analyze the gas costs of executing smart contract functions to learn about the cost and scalability of the system. In broad terms, the objective of this research is to mitigate the constraints confronted by existing centralized credential verification systems by providing a more secure, tamper-proof, and serviceable alternative for use in academic, governmental, and professional applications.

III. Related work

Numerous studies have been conducted concerning the challenges and prospects of secured issuing and verification of certificates on blockchain technology. Aras and Kulkarni's [9] work is, however, on a blockchain-based academic record management system under which the record is expected to be immutable and transparent for students. This suggested that blockchain is feasible for academic credentials but heavily relied on a centralized interface for user accessibility. Patel and Shah [10] proposed a distributed credential verification platform based on smart contracts of the Ethereum blockchain and certificate authentication. However, while storing information was made tamper-proof, the need for the user to secure private cryptographic keys increased complexity in the process employed.

Kamble, Gunasekaran, Sharma [11] proposed an education blockchain that would be used for generating verifiable digital certificates to be stored on a decentralized node. Their work created increased trust in the system; however, their approach fell short of achieving scalability and fast query processing during the verification of certificates.

A certificate authentication model using blockchain, as introduced by Wang and Chen [12], was modeled in such a way that issuers registered certificates on a public ledger while verifiers authenticated the records through public key cryptography. Although such a design would seem to eliminate a middleman in the process, it nevertheless puts the whole responsibility of key management in the hands of the users, which poses usability issues.

A self-sovereign identity framework for educational certificates was proposed by Singh and Mathew [13]. Their system allows students to control the use of their academic credentials, but issues of interoperability among institutions arise.

Certificate validation in a blockchain-based storage by Ahmed, Kaadan, and Salman [14] is coupled with IPFS storage for off-chain data management purposes. While this addresses privacy and minimizes on-chain storage, the model does not strongly validate third-party validators, carrying potential risks.

Zhang and Xu [15] proposed a decentralized academic certificate issuance system based on Hyperledger Fabric. Their permissioned blockchain improved transaction speeds and privacy but relies on centralized certificate authority nodes for user authentication, thereby creating a potential vulnerability.

Mahmood and Alshamsi [16] recommended a blockchain-based method for COVID-19 vaccination certificate management, focusing on secure sharing through Proxy Re-Encryption (PRE) techniques. While the model favored privacy, it held that the participants should belong to a private blockchain network, restricting open verification. Choudhury, Patel, and Singh [17] designed a blockchain-based accreditation system meant to verify educational institutions and certificates on decentralized trust structures; however, the model built trust dependency on the accreditation body and posed complex access management problems for non-technical users. On the other hand, Mehta and Joshi [18] sought attacks on certificate issuance and rectification using one blockchain for original certificates and another one for updates.

While this also allowed for an authenticated update, keeping synchronized records on two separate blockchains placed extra overhead on the system. Overall, these studies confirm that the blockchain can potentially revolutionize credential verification in terms of transparency, security, and decentralization. However, some existing limitations such as scalability, user privacy, validator authentication, and interoperability still prevail. The present work attempts to address these gaps by combining a PHP-based web application with the blockchain framework to create an efficient, decentralized, and user-friendly certificate management system.

IV. Proposed Model and Its Implementation

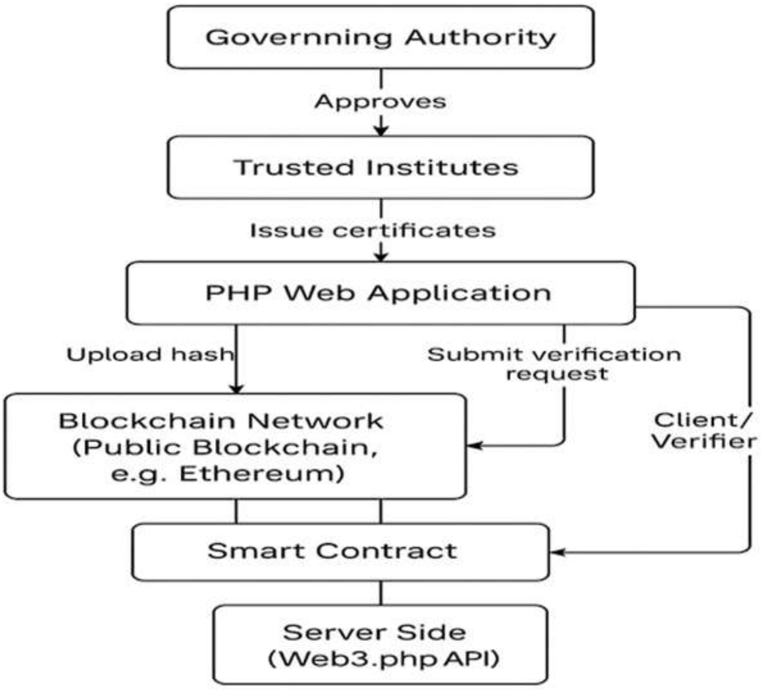


Fig 1 : Proposed architecture

A . Proposed Model :

The proposed system deals mainly with the attempts to create a decentralized, secure and transparent framework for generation and validation of certificates using blockchain technology and PHP web application. The planning includes numbers of stakeholder working to continue the authenticity and the integrity of digital certificates while ensuring an easy-to-operate operational environment. Now, the whole process starts with a governing authority that supervises the system and is responsible for approving educational institutions that are regarded as trusted. Throughout the issuance of a certificate, a trusted educational institution enters the certificate details into the PHP application, which is serving as the core interface for certificate issuance and management.

In the proposed system, the PHP web application accepts the certificate detail and generates a unique hash such that it minimizes the risk of hacking-the conversion to be more specific-is generally done by using cryptographic algorithm, namely SHA-256. The generated hash is uploaded on a Blockchain Network like Ethereum public blockchain, thereby ensuring that the data regarding the certificate is stored in an immutably way and can be accessed by others for verifying in the future.

The process of adding and verifying certificates is governed by smart contracts deployed on the blockchain. Smart contracts act as agents without actual people, with validation for certificate hashes built into them. No more centralized verification authorities are then needed, achieving objective verification. Smart contracts guarantee system security by eliminating the rules for issuing and validating certificates from humans. The Server-Side component of the System is based on Web3.php APIs as a bridge between the PHP application using some blockchain network. It is a handler of blockchain transactions like uploading certificate hashes and querying the blockchain for verification requests. The request for verification comes from the clients or verifiers, be it an employer, an academic institution, or an organization via a certificate ID or valid details submitted through the PHP web application. The application processes the request and communicates with the blockchain network regarding validation by comparing the given certificate hash to that on the blockchain as a stored record.

In case of success in finding and verifying the hash of the certificate, the system validates the certificate's status to the verifier. Otherwise, if the hash cannot be found or does not match, it informs the verifier about the invalid status. This increases trust through verification without manual dependency and minimizes fraudulent activities for existing fake or altered certificates. Blockchains and the irretrievable contracts become coupled with the automation by PHP to develop a tough ecosystem in terms of issuing and verifying certificates in a completely decentralized and tamper-proof manner. The system is built to scale and remain flexible so that more trusted institutions and governing bodies can participate while also extending the network security.

B. Implementation of proposed model: The implementation of the proposed blockchain- Blockchains are dependent on each other components that are tied to one another on functions performed for smooth as well as secure running of the proposed blockchain-based certificate generation and validation system. The governing authority starts the whole process and grants trusted educational institutes the authority or permission to issue certificates. Approval details like identity and credentials are been handled apart from recording the information on blockchain by means of a smart contract in the Trusted

Institutes to include the trusted institution into the system's access to certificate generation portal via a PHP Web Application. The intervening PHP application shall collect pertinent certificate information such as the recipient's name, course, date of issuance, and issuing authority the moment a trusted institute issues a certificate. In that application, a unique hash generated that reflects the details and consists of the cryptographic algorithm like SHA-256. This hash is uploaded on the Blockchain Network through Smart Contract mechanisms ensuring the fact that the data is no longer alterable.

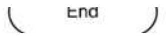


Fig 2 : certificate issuance process

The moment a hashed certificate is securely posted on the blockchain, the institution issuing it automatically receives a notification and confirmation of the safe storage of the certificate in an environment that is decentralized. End users typically, clients or verifiers, may want to confirm the authenticity of the information contained in the certificate through the same PHP web application interface. ..

In the event of initiation of verification request, the PHP application calls the Smart Contract to fetch the hash related to the provided certificate ID. The hash fetched will be compared to the input provided by the verifier. When the hashes match, the authenticity of the certificate is confirmed, and when they don't, it is said that the verification has failed.

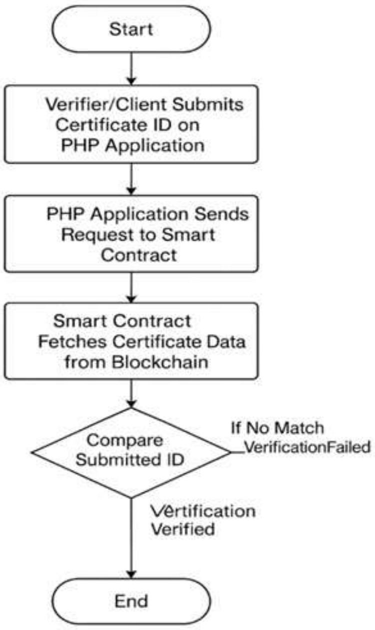

Start
Verifier/Client Submits Certificate ID on PHP Application
PHP Application Sends Request to Smart Contract
Smart Contract Fetches Certificate Data from Blockchain
Compare Submitted ID
If No Match VerificationFailed
Vertification Verified
End

Fig 3 : certificate verification process

This automated, decentralized approach negates all forms of dependency on a centralized database and manual verification. Moreover, the transparency resulting from the blockchain gave assurance to the verifiers regarding the correctness of responses from the system without requiring trust in intermediaries. The smart contracts take one step further in reducing human error by executing the verification rules autonomously.By integrating the PHP-based user interface with blockchain technology, the system offers an accessible, scalable, and secure environment for certificate management. The combination of immutability, decentralization, and automation through smart contracts ensures a trustworthy ecosystem for the issuance and validation of digital certificates across multiple institutions and verifiers.

Table 1 : process and component of proposed system

Process	Component Involved
Certificate Issuance	PHP Application, Blockchain Network, Smart Contract
Certificate Verification	Client/Verifier, PHP Application, Blockchain Network

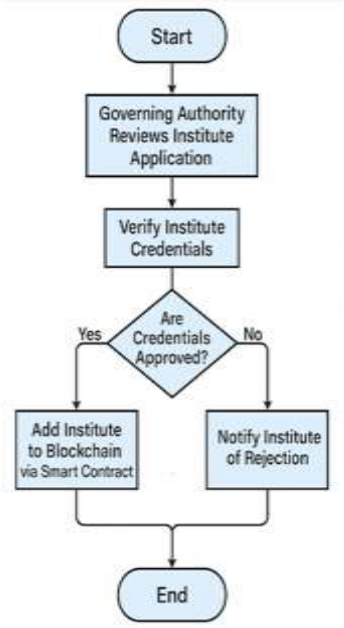

Start
Governing Authority Reviews Institute Application
Verify Institute Credentials
Are Credentials Approved?
Yes
No
Add Institute to Blockchain via Smart Contract
Notify Institute of Rejection
End

Fig 4 : Trusted Institute Approval

The integration of blockchain technology with the PHP user interface, in order to provide users with an accessible, scalable, and secure environment for certificate management. Immortalization, decentralization, and automation via smart contracts give birth to a trustable ecosystem that governs the issuance and validation of digital certificates across multiple institutions and verifie

V. SMART CONTRACT AND COST ANALYSIS

The section describes the implementation and assessment of the smart contract designed for the generation and validation of certificates over the blockchain. It covers deployment and testing activities. The analysis focuses on core functionalities, including adding certificates, showing certificates, and verifying certificates using Solidity on the Ethereum blockchain. It goes on to explain the gas costs incurred by smart contract functions and compares them to an existing centralized verification system to establish the efficiency and cost-effectiveness of the suggested model.

A . Smart contract execution

Smart contracts are indispensable in ensuring that the generation and validation of certificates are performed securely, transparently, and automatically. The core functionalities of smart contracts were developed in Solidity, the primary language used to write contracts for the Ethereum blockchain. The interaction between the PHP-based web application and the blockchain involves the Web3.php API, which is the source of communication between the user interface and blockchain network.

Fig 5 illustrates the entire operation of smart contracts within the system. This very architecture outlines key steps in the journey of an NFT certificate, beginning with its issuance in an NFT and ending with permanent storage on the blockchain. In such a manner, all data entered into the certificates by trusted institutions will be stored immutably for decentralized validation, which is free from any central authority.

Fig 5 depicts the operational flow from issuing a certificate to storing its hash on the blockchain using smart contracts.

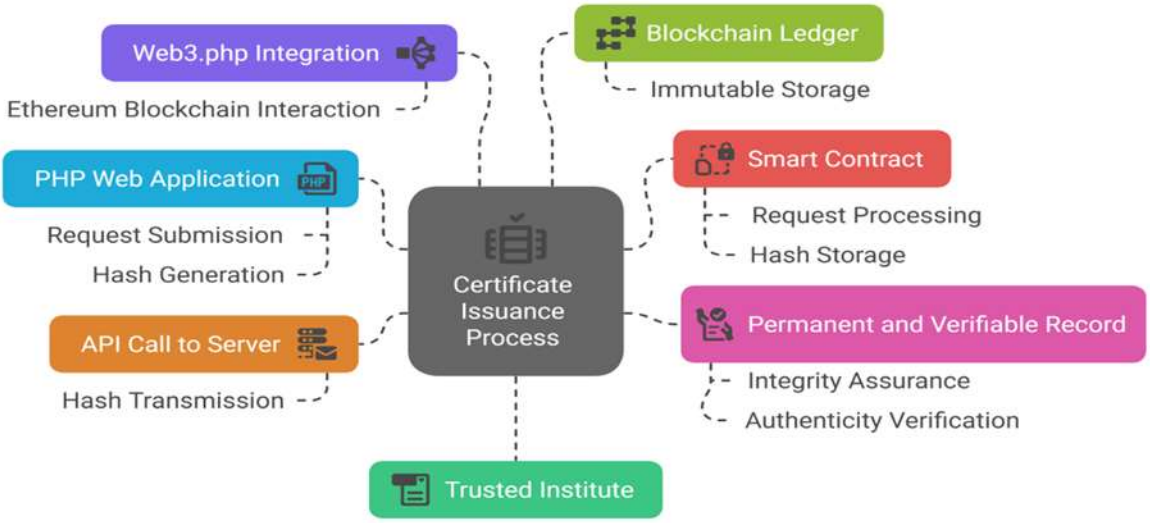
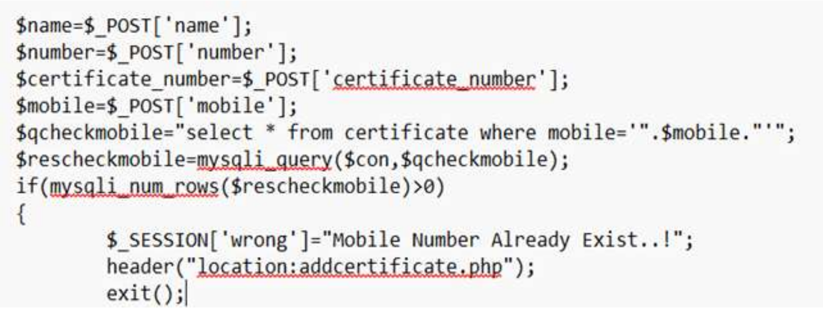


Fig 5: Blockchain-Based Certificate Management Communication Model

This system has been equipped with a smart contract designed to perform three primary functions, responsible for handling distinct aspects of the certificate lifecycle: adding an entirely new certificate, showing existing ones, or showing the new ones directly.

certificates, and verifying the certificates. Each function is executed securely via blockchain transactions to maintain data integrity and transparency.

- AddCertificate Function : The function of add Certificate is invoked at the time of releasing the new certificate by a trusted institution. The functions take the certificate metadata such as the student name, name of the course, issuing date, and generate a secure hash value using SHA-256 cryptography. When the function is executed, the smart contract permanently stores the hash on the blockchain ledger that can later independently verify the issued certificate. The successful execution of add Certificate function would take place as follows is illustrated in Fig 6.

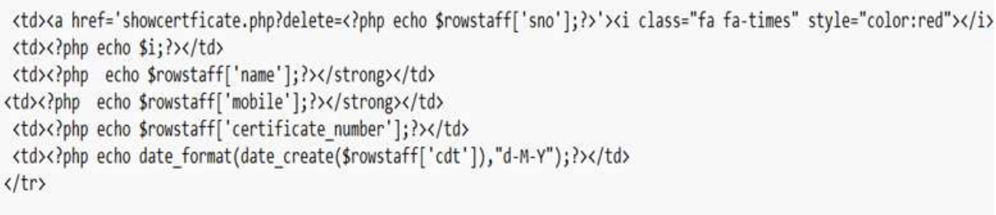


```
$name=$_POST['name'];
$number=$_POST['number'];
$certificate_number=$_POST['certificate_number'];
$mobile=$_POST['mobile'];
$qcheckmobile="select * from certificate where mobile='".$mobile."'";
$rescheckmobile=mysqli_query($con,$qcheckmobile);
if(mysqli_num_rows($rescheckmobile)>0)
{
        $_SESSION['wrong']="Mobile Number Already Exist..!";
        header("location:addcertificate.php");
        exit();
```

Fig 1 : execution of add certificate function

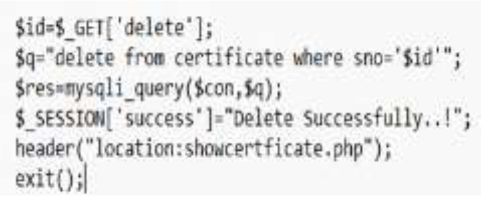
The decentralized recording of certificate hashes through this function eliminates the risk of tampering or fraudulent modifications.

- ShowCertificate Function : The showCertificate function pulls up and shows the information about a certificate stored on the blockchain. When a verifier submits a certificate ID through the web mobile application built on PHP, the system communicates with the smart contract to retrieve from the blockchain the corresponding certificate hash and metadata. This function allows the user to confirm the certificate's authenticity by comparing the entries with those permanent records kept on the blockchain. Upon the successful execution of the showCertificate function, certificate verification becomes decentralized, open, and resilient to tampering. The system response on executing the showCertificate function is represented in Fig 7.



```
 <td><a href='showcertficate.php?delete=<?php echo $rowstaff['sno'];?>'><i class="fa fa-times" style="color:red"></i>
 <td><?php echo $i;?></td>
 <td><?php  echo $rowstaff['name'];?></strong></td>
<td><?php  echo $rowstaff['mobile'];?></strong></td>
 <td><?php echo $rowstaff['certificate_number'];?></td>
 <td><?php echo date_format(date_create($rowstaff['cdt']),"d-M-Y");?></td>
</tr>
```

Fig 7: show certificate function

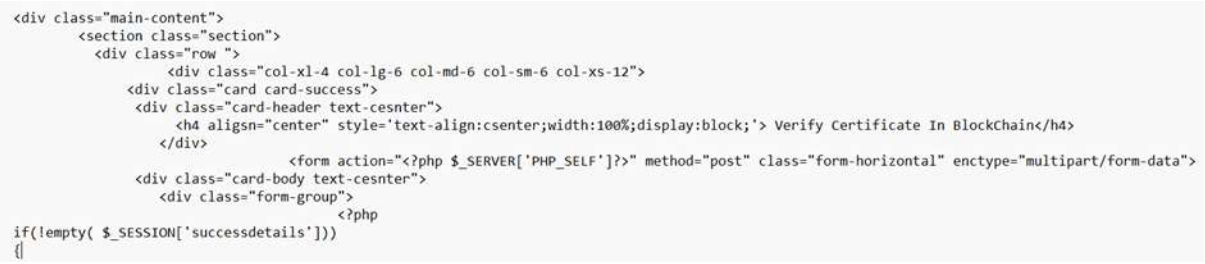


```
$id=$_GET['delete'];
$q="delete from certificate where sno='$id'";
$res=mysqli_query($con,$q);
$_SESSION['success']="Delete Successfully..!";
header("location:showcertficate.php");
exit();
```

Fig 8 delete show certificate function

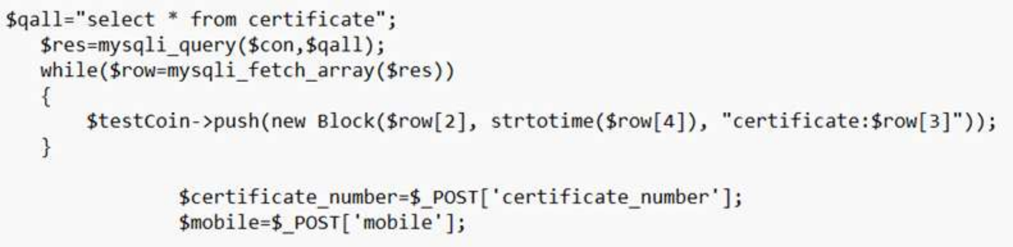
The showCertificate function builds user confidence in the system as it provides a trustworthy way to view and verify certificates without relying on centralized databases or any manual workaround.

- VerifyCertificate Function : The verifyCertificate function is a critical component of the proposed system, responsible for validating the authenticity of a submitted certificate. When a verifier inputs a certificate ID through the PHP-based web application, the verifyCertificate function queries the blockchain to retrieve the associated certificate hash. The function then compares the submitted certificate data with the immutable record stored on the blockchain. If a match is found, the certificate is confirmed as authentic; if no match exists, the verification fails. Fig 9 illustrates the successful execution and output of the verifyCertificate function.



```
<div class="main-content">
        <section class="section">
          <div class="row ">
                   <div class="col-xl-4 col-lg-6 col-md-6 col-sm-6 col-xs-12">
              <div class="card card-success">
               <div class="card-header text-cesnter">
                    <h4 aligsn="center" style='text-align:csenter;width:100%;display:block;'> Verify Certificate In BlockChain</h4>
                  </div>
                                 <form action="<?php $_SERVER['PHP_SELF']?>" method="post" class="form-horizontal" enctype="multipart/form-data">
               <div class="card-body text-cesnter">
                  <div class="form-group">
                                              <?php
if(!empty( $_SESSION['successdetails']))
{
```

Fig 9 : certificate verify function



```
$qall="select * from certificate";
   $res=mysqli_query($con,$qall);
   while($row=mysqli_fetch_array($res))
   {
       $testCoin->push(new Block($row[2], strtotime($row[4]), "certificate:$row[3]"));
   }

               $certificate_number=$_POST['certificate_number'];
               $mobile=$_POST['mobile'];
```

Fig 2.1

The inclusion of the verifyCertificate function enhances the overall reliability of the system by enabling decentralized, transparent, and tamper-proof certificate verification without relying on centralized authorities or manual verification processes. This functionality significantly reduces administrative workload and improves user trust in the system's validation results.

B . Cost Analysis

This particular subsection will cover the analysis of gas costs involved in executing important functions of the automated smart contract for certificate management in the proposed blockchain. Gas is defined in Ethereum as the computational effort to execute any operation on the network. An Ethereum transaction incurs two types of gas costs: execution gas toward the function being called and transaction gas, which is incurred by processing the transaction by the network [19].

To estimate these costs accurately, simulations were performed using the Remix IDE. Table 2 presents the gas costs incurred by different smart contract functions, including addCertificate, showCertificate, and verifyCertificate. The estimated conversion of gas usage into USD is based on a gas price of 50 Gwei and an Ether (ETH) price of $2000.00, reflecting average values retrieved from Etherscan as of April 25, 2025 (Etherscan, 2025).

This is just the cost comparison of various operations in the proposed system with fig 10. The results show that adding a certificate incurs the highest gas cost because this operation permanently writes into the blockchain; the cost for both certificate verification and retrieval, however, remains significantly lower in comparison. The decentralized validation model, in fact, will not only allow a more transparent validation than the conventional centralizations but will also exhibit a competitive cost of operation [3],[8]. Future work can focus on further optimizing the smart contract functionalities for lower gas consumption to add to the economic efficiency of the entire system.

Gas and Transaction Cost Analysis for Certificate Management Functions

Table 2: Gas Consumption and Cost Estimation for Certificate Operations

Smart Contract Function	ExecutionGas Used	TransactionGas Used	EstimateCost (USD)
addCertificate	142,000	158,000	1.25
showCertificate	35,000	48,000	0.38
verifyCertificate	40,000	55,000	0.42

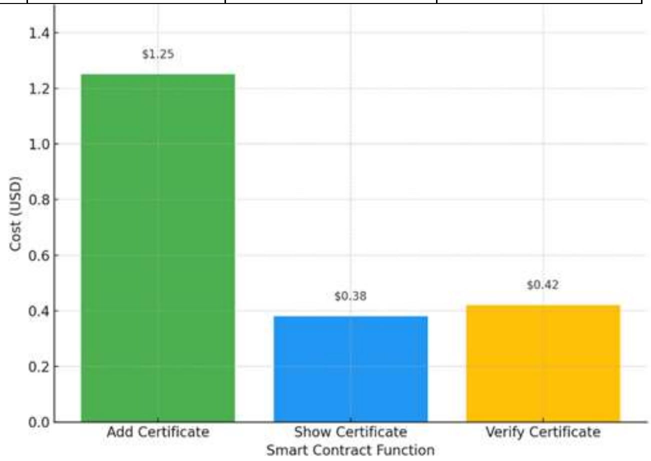


Fig 10: cost comparison graph

VI. Conclusion

The present work involved developing a decentralized certificate issuing and verifying platform based on a combination of blockchain technology and a web application powered by PHP. Using Ethereum smart contracts, this system ensures that certificates are immutably stored and verifiable in a transparent manner. Cost analysis demonstrated that recording a certificate (addCertificate) incurs a fairly average cost of around $1.25 while retrieving (showCertificate) and verifying (verifyCertificate) were very economical at around $0.38 and $0.42 respectively. Thus, the results confirm the viability of this system for real-world use.

Unlike traditional methods that often lend themselves to manual verification and centralized control, the advanced solution minimizes the dependency on intermediaries, brings down the time required to verify, and enhances trust among users. Computerized execution through smart contracts mitigates the risk of human errors and administrative overhead even further. Also, the very nature of decentralized architecture reduces weaknesses attributed to single points of failure. Foresight improvements, however, could take the shape of better optimization for smart contracts in order to further reduce charges or enhancing the system for multi-institutional collaboration.

VII . References

[1] M. Grech and A. Camilleri, "Blockchain for education: lifelong learning passport," *Joint Research Centre (JRC), European Commission*, 2017. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/handle/JRC108255

[2] M. Sharples and J. Domingue, "The blockchain and kudos: a distributed system for educational record, reputation and reward," in *Proc. 11th Eur. Conf. Technology Enhanced Learning (EC-TEL)*, Lyon, France, 2016, pp. 490–496. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-45153-4_48

[3] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[4] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation Review*, vol. 2, pp. 6–10, 2016. [Online]. Available: https://j2capitalmanagement.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf

[5] A. Gutmans, S. Bakken, and A. Suraski, *PHP Manual*, PHP Documentation Group, 2000. [Online]. Available: https://www.php.net/manual/en/

[6] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed., Wiley, 2007.

[7] V. Buterin, "A next-generation smart contract and decentralized application platform," *Ethereum White Paper*, 2014. [Online]. Available: https://ethereum.org/en/whitepaper/

[8] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016. [Online]. Available: https://doi.org/10.1109/ACCESS.2016.2566339

[9] M. Aras and R. Kulkarni, "Blockchain and its applications in education sector," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 4, pp. 1262–1266, 2019. [Online]. Available: https://doi.org/10.30534/ijatcse/2019/49842019

[10] D. Patel and D. Shah, "Enhancing academic certificate authentication system using blockchain technology," in *Proc. 5th Int. Conf. Computing, Communication, Control and Automation (ICCUBEA)*, Pune, India, 2020, pp. 1–5. [Online]. Available: https://doi.org/10.1109/ICCUBEA47591.2020.9165555

[11] S. Kamble, A. Gunasekaran, and R. Sharma, "Modeling the blockchain enabled traceability in agriculture supply chain," *International Journal of Information Management*, vol. 52, p. 101967, 2020. [Online]. Available: https://doi.org/10.1016/j.ijinfomgt.2019.05.023

[12] Y. Wang and Y. Chen, "Blockchain in education: A survey," *Future Internet*, vol. 10, no. 8, p. 94, 2018. [Online]. Available: https://doi.org/10.3390/fi10080094

[13] S. Singh and S. Mathew, "Blockchain for digital certificate authentication and verification," in *Proc. 10th Int. Conf. Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, 2020, pp. 704–709. [Online]. Available: https://doi.org/10.1109/Confluence47617.2020.9058348

[14] E. Ahmed, L. Kaadan, and O. Salman, "Certificate verification using blockchain and IPFS," in *Proc. Int. Conf. Computer and Applications (ICCA)*, Beirut, Lebanon, 2020, pp. 1–6. [Online]. Available: https://doi.org/10.1109/ICCA49341.2020.9096788

[15] Y. Zhang and X. Xu, "A novel academic certificate issuance and verification framework using Hyperledger Fabric blockchain," *IEEE Access*, vol. 9, pp. 139909–139919, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3118711

[16] R. Mahmood and A. Alshamsi, "Blockchain based solution for COVID-19 vaccination certificates," in *Proc. 11th Int. Conf. Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, 2021, pp. 446–451. [Online]. Available: https://doi.org/10.1109/Confluence51648.2021.9377151

[17] O. Choudhury, S. Patel, and A. Singh, "Blockchain-based accreditation system for educational institutions," in *Proc. 6th Int. Conf. Computing Communication and Automation (ICCCA)*, Greater Noida, India, 2020, pp. 1–5. [Online]. Available: https://doi.org/10.1109/ICCCA49541.2020.9250811

[18] D. Mehta and P. Joshi, "Dual blockchain for certificate issuance and update verification," *International Journal of Computer Applications*, vol. 183, no. 40, pp. 1–6, 2021. [Online]. Available: https://doi.org/10.5120/ijca2021921196

[19] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, 2014. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf