COST-EFFECTIVE AND EFFICIENT BLOCKCHAIN FRAMEWORK FOR VERIFYING CERTIFICATE IN YEMENI UNIVERSITIES

Muna Abduallah Alkhawi [a], Anwar Saif Alshameri [b]

[a] Information System, Sana'University, Sana'a, Yemen, mona.alkhawi@su.edu.ye
[b] Information System, Sana'University, Sana'a, Yemen, anwarsaif@su.edu.ye

***Corresponding Author:** mona.alkhawi@su.edu.ye

TO CITE THIS ARTICLE:
Alkhawi , M. A., & Alshameri, A. S. . (2024). COST-EFFECTIVE AND EFFICIENT BLOCKCHAIN FRAMEWORK FOR VERIFYING CERTIFICATE IN YEMENI UNIVERSITIES. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 15(2), 206–216. https://doi.org/10.61841/turcomat.v15i2.14642

ABSTRACT: Recognizing the necessity to preserve the integrity and good name of degrees awarded by Yemeni universities. It should provide an efficient way of verifying credentials and speed up the verification process. The effectiveness of the conventional method of confirming the validity and integrity of certificates in reducing fraud has not been very strong. Therefore, it is necessary to stop this kind of fraud using blockchain technology, which has several benefits, such as encryption, sharing of data, and the capacity to store information as permanent data that cannot be altered. Low latency and low cost will be available for the issuance, sharing, and verification of these certifications in universities if the suggested blockchain-based certification system is implemented. The paper presents the proposed framework, which uses smart contracts in the Ethereum blockchain and a distributed peer-to-peer network (filebase) for certification verification by a certificate's hash. It also contains an estimate of the average cost of publishing a certificate. It also frees students from having to constantly carry paper copies of their documents by enabling them to access them. Furthermore, there is no extra cost for the verification process.

KEYWORDS: Certificate's Hash, Filebase, Smart Contract, Ethereum Blockchain, Verifying Certificates, Low Validation Cost.

1. Introduction

The traditional methods of verifying certificates are highly centralized, meaning they completely rely on the organization that issues certificates. Some organizations ask the Ministry for confirmation or stamping in order to assure extra caution. This type of verification is exhausting and mostly done by hand. Lastly, it is easy to manipulate and temper. Blockchain technology is being regulated in several nations for use in a variety of sectors, including public administration, the Internet of Things, and the supply chain.

One of the most useful sectors to employ blockchain technology to produce both short- and long-term effects is the education industry. Thanks to the widely extended offer of a stable public blockchain that can be used for secondary uses, such as a verification tool and reliable and affordable verification of official documents (Badhe, Vipul, Nhavale, Pooja, Todkar, Sonal, Shinde, Prajakta, & Kolhar, Kiran, 2020).

Decentralization is the key component of blockchain technology, and its strength is that it reduces the time it takes for transaction validation by eliminating the need for a third party to act as an intermediary in order to authenticate transactions or operations (Tenorio, 2021).

The emergence of blockchain technology in the past ten years has given rise to numerous applications of decentralization in a variety of industries, including education (Ocheja, Patrick, Agbo, Friday Joseph, Oyelere, Solomon Sunday, Flanagan, Brendan, & Ogata, Hiroaki, 2022).

Blockchain technology uses cryptography to protect data and make it impenetrable, preventing hackers from accessing and forging certificates on the network. Because of this, it is suggested to use blockchain technology to validate degree certificates due to its powerful features (Kumutha.K , S.Jayalakshmi, 2021).

Systems operating in centralized storage and management mode are susceptible to a number of threats. and storage servers are typically made so that only internal personnel may access them. Furthermore, data loss or leakage could

be easily caused by a server failure. Thus, organizations typically implement security policies to limit record sharing and access in order to safeguard personal data (Li, Hongzhi & Han, Dezhi, 2019)**.**

This work suggests a decentralized application (DAPP) built on the Ethereum blockchain and the filebase file system to validate and store certificates without requiring a centralized system or organization to manage and regulate its management while guaranteeing its ownership and immutability.
An organization may use the framework for its main website. The framework's objective was to create a verifiable online certificate system that any organization could use. In this work, we proposed a framework using blockchain, we are adding the following novelties:

1) Reduce the amount of time and money the institution has to spend on traditional certificate verification procedures.
2) The publishing system is separate from verification, which increases security.
3) Publicly validate the hash; this allows employers to view the certificate.
4) Since the majority of nations prohibit the use of cryptocurrencies, the certificate verification process does not require an Ethereum network account because there is no cost involved.
5) Any university could use the framework for its main website, and users can directly verify a certificate by its hash without waiting for a facility's response.

2.Significance Of the Study

Certificate verification has become increasingly wanted among institutions and employers, In contrast, without a trustworthy mechanism to validate certificates, the certificate forgery problem will probably worsen and continue the automated system enables easy and quick verification of certificates. In addition, the employer or establishment does not have to contact the institution directly to verify the certificate.

This issue is persistent, and the harm it causes is extensive. Employers, clients, real graduates, academic institutions, and the public sector are all affected. Blockchain technology will therefore improve certificate-verification systems by lowering costs, streamlining the process, and saving time.

3.Review Of Related Studies

Verifi-Chain (Tasfia Rahman,Sumaiya Islam,Arunangshu Mojumder, Abul Kalam,Nafees Mansoor, 2023)The system suggests using blockchain technology for certificate verification. The candidate uploads to the system the required login credentials. The applicant requests that the administrator confirm the certificates. To get confirmation that these certificates are genuine, the administrator gets in touch with academic institutions. After which, the administrator uploads the certificates to IPFS and notifies the users. It gives back a hash key, which is encrypted before being kept on the Blockchain nodes. To apply for any job, the candidate can send organizations their hash number. Employers can use the system to search for applicants and verify the authenticity of their certificates by entering the hash.

(Shaik Arshiya Sultana,Chiramdasu Rupa, Ramanadham Pavana Malleswari and Thippa Reddy Gadekallu, 2023) A proposed system that uses strong encryption techniques to guarantee the security of academic data on the blockchain. The administrator first fills in the web interface application with the academic information. Data encryption is applied, and an identity is created. The cipher text is then moved to nodes connected to the IPFS (Interplanetary File System), where the hash values for the text are kept. In the blockchain, the relevant hash values are kept. After that, the hash value's corresponding encrypted data is decrypted. Ultimately, the user is presented with the data via an online interface, facilitated by web-based knowledge management.

(Rana F. Ghani , Asia A. Salman , Abdullah B. Khudhair, Laith Aljobouri, 2022) This study suggested and put into practice an electronic certificate deployment system. The Hyperledger private blockchain was used in the creation of the system. The suggested system controlled and secured the certifications' rollout using hashing and smart contracts. The examination committee will move all of the courses the student took and their grades from the system database to the blockchain once they have successfully completed the study requirements. The student uses the online application to apply for the certification, and the application is sent to the institution. After reviewing the

student record and authorizing the procedure, the authorized organization sends the approval to issue the certificate. The online application, which can export a PDF and share it with a third party.

(Christian E. Pulmano,Maria Regina Justina E. Estuar,Marlene M. De Leon,Hans Calvin L. Tan, Nicole Allison S. Co, Lenard Paulo V. Tamayo, 2023)The architecture for creating a blockchain network for a decentralized digital credential system for e-participatory governance is provided in this article. This article specifically investigates test deployments in the domains of academic credentials and national identification as early use cases. The Hyperledger Fabric blockchain network configuration with the necessary chaincodes is covered first. Students have the option to disclose their academic records to other groups, such as prospective employers in the future. The academic credentials network also has its own channel in the network. Peer nodes can be distributed to various educational establishments and student associations in order to enhance verification. All of this was kept both inside CouchDB and in a shared ledger for the use case involving educational credentials.

(Kumutha.K1, Dr.S.Jayalakshmi, 2021) With the use of Hyperledger, this system is a tool for industry-institution interaction. Each constructed certificate will be saved in CouchDB, which will then return the unique hash produced using the SHA-2S6 technique. A valid user can upload the certificate details to the blockchain network with the necessary certificate data. Since only the necessary information—student ID, serial number, certificate issue date and time, issuing authority ID, and qualification—was kept in addition to the hash value, CouchDB was utilized to store scanned certificates. Following creation, an appropriate consensus method verifies the block, and the approved block is subsequently added to the blockchain network. Subsequently, the system will provide an OTP, QR code, and inquiry string that must be attached to a hard copy certificate in order to authenticate it over the phone and website.

4.Objectives Of the Study

The purpose of this study is to investigate the existing certificate verification systems to identify the fundamental problems with them and to create a framework for improving them by implementing blockchain technology. More precisely, draft goals have been created for the following:

- 1. Study the existing certificate verification systems and examine their convenience, efficiency, and effective.
- 2. Explain how improving the current certificate verification process can be achieved with a blockchain-based solution.
- 3. Develop a framework based on Ethereum blockchain technology for certificate-verification systems.
- 4.Certificate verification process doesn’t require cryptocurrencies or an Ethereum network account since the majority of nations prohibit the use of cryptocurrencies.

5. Proposed Framework

In this research, we proposed framework work on the Ethereum blockchain and peer-to-peer file system (filebase), to verify certificates issued by Yemeni universities after certifying the final result from the universities sending a copy of the approved certificates. The certificate file will be uploaded to the filebase. The hash (CID) value will be returned from the filebase, which points to the file that has been put in the IPFS. The inquiry string must be attached to a hard copy certificate in order to authenticate it over the website. This hash will be stored on the Ethereum blockchain. Dapps web applications will serve as the user's interface for uploading and verifying documents. Thus, this framework consists of two sections:

5.1. Section 1 publish the certificates

Uploading certificates to filebase and saving certificate hash on Ethereum Blockchain network. The following describes the steps to publish the certificates files once the university produces it:

1) Deploy smart contract on the Ethereum blockchain Initially, only once.
2) University stuff uploads certificate file through the DAPP.
3) The data will store on the distributed peer-to-peer (filebase)and retunes the CID code of the file ex:(QmaRtUGUv1KB69boat2EaqEymC3TXfRrVRsB8x7HeGFpzg).
4) The DAPP saves the CID code on the Ethereum blockchain through the smart contract.
5) The MetaMask asks the employee to confirm transaction then discount transaction cost from account on Ethereum blockchain.
6) Finally, CID code printed and attached to the certificate. figure 1 display the architecture for this section.

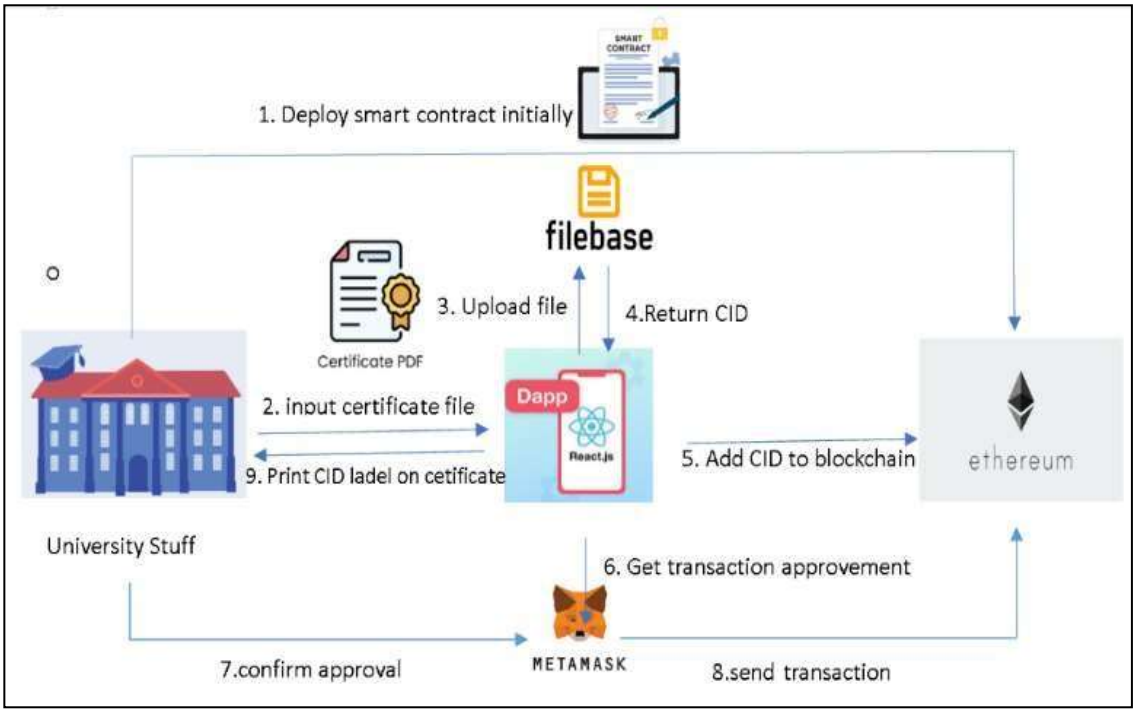

Figure.1. Publish the certificates

5.2. Section 2: verifying certificates via certificate s' hash

Public website for verifying certificates. By using the certificate hash, anyone can verify certificates. Institutions can use the website to quickly, easily, and securely validate students' certificates.

Additionally, without any extra cost it allows students to access their documents without requiring them to always carry paper copies. Figure 2 display the architecture for this section.

Figure. 2. Verifying certificates via its' hash.

5.3. Smart Contract Design

The smart contract is compiled and deployed on the Ethereum blockchain to control the certificate. Certificate hash (CID): the key of the certificate is used as the index of the certificate.

The contract defines a hashmap of type map. Mapping is the storage structure of key-value pairs used in the smart contract.

The mapping stored the relationship between: studentName and CID. There are two main functions in the contract:

storeHash(CID,StName): This function establishing the mapping relationship between CID and StName . It called only by university stuff to store the certificate hash by contract.

verifyCertificate(CID) : This function is call to verify if the specific certificate CID exists on blockchain . The input CID is identity of the certificate and the output is string. We check if the certificate exists on the blockchain by checking whether its CID exists in the Map.

Algorithm *1* storeHash*(CID,StName)*

Input: *CID* is the hash of certificate,
StName is thestudent name
Output: boolean.
1: **if** *msg.sender* is not the Address of the institution **Then**
return false;
3: **end if**
4: *HashMap[CID]* ← *StName*
5: **return** true;

Algorithm 2 verifyCertificate**(*CID*)**

Input: *CID* is the hash of certificate
Output: string.
1: **if** *CID* is NULL then 2: return null;
3: **else**
4: result= *HashMap [CID]*;
5: **end if**
6**: return** result

The two sections communicate with a single smart contract; we must obtain its address on the Ethereum blockchain as well as its ABI (application binary interface). The data structures and functionalities of the contract are represented in JSON via the ABI. Comparably, the blockchain's deployed instance of the contract is uniquely identified by its contract address.

6. Framework Modules

6.1. Ganache

Ganache is a personal Blockchain network allowing developers to quickly build and test distributed Ethereum applications. It can be used throughout development, providing a secure and predictable environment for developing, deploying, and testing dApps. (Blockchain Council, May 18, 2023)**.**

6.2. Metamask

It is a popular cryptocurrency wallet and browser extension that allows users to store, send, and receive Ethereumbased digital assets. It can bridge a user's browser and the Ethereum blockchain, enabling seamless interaction with decentralized applications (dapps) and the Ethereum network. Metamask also allows users to manage their private keys and interact with smart contracts. (What is MetaMask?, 2024)

6.3. Truffle:

Is a framework for compiling, linking, deploying, and managing smart contracts. (TRUFFLE SUITE, n.d.)

6.4. React

React is one of the most powerful JavaScript libraries for dApp development in different ways. It features multiple building blocks or components which can help in building complex user interfaces or UIs. Interestingly, React does not require developers to create all boilerplate codes from scratch. (Howell, 2023)

6.5. Web3

A powerful and adaptable set of libraries for TypeScript and JavaScript developers. It enables the use of HTTP, IPC, or WebSocket to communicate with a local or remote Ethereum node (or any blockchain that is compatible with EVM). For establishing connections and creating apps inside the Ethereum ecosystem, it is a crucial tool. (Web3.js Docs, 2024)

Interact with Smart Contract Functions by using the Web3.js instance, contract ABI, and contract address. The call () function can be used to invoke a read-only function (verifyCertificate) that does not change the state of the contract. Conversely, the send () method can be used to send a transaction to a function (storeHash) that modifies the contract's state.

7. Experimentation and Results

7.1. Implementation Setup

We write and test smart contracts using the Remix Integrated Development Environment (IDE), Ganache, and Metamask. The Sepolia and Goerli test networks are where the smart contracts are executed and tested. The script is coded using Solidity language version >=0.6.12 <0.9.0 and Remix IDE use an Intel(R) Core (TM) i5-5300U CPU @ 2.30GHz ,8.0 GB of RAM, Win10 Pro, 64-bit OS, x64-based processor.

7.2. Cost Analysis

In Ethereum, the computing effort needed to carry out different operations within a smart contract is measured in units called "gas." Any operation writing or modifying data on Ethereum needs gas. Every transaction requires a fixed quantity of gas, which the sender must pay for in ether. The cost of a single unit of gas is referred to as the "gas price." The unit of measurement for gas prices is Gwei, which is a fraction of an ether. Gas prices are based on the state of the market and generally rise when there is network congestion**.** (Gas Market: Analyzing Gas Market Dynamics in Ethereum's Network, 2023)

7.3.1. Cost of Deploy Smart Contract

A smart contract is deployed by the management organization. The cost of deploying smart contracts is the most expensive process and it paid once at system initialization. The cost of deploying Smart Contracts on Ethereum rely on complexity of the contract, and network congestion. (Blockchain cost structure: The Hidden Costs of Smart Contracts on Blockchain, 2024)

One way to reduce the cost of deploying smart contracts is by monitoring the gas price on the Ethereum network and selecting the appropriate moment when the gas price is low.

Gas per gwei can be obtained from sites like etherscan. At the time of research, the average price of gas was approximately 20 Gwei.

The deployment cost for deploy our contract according to Remix, was 460013 (gas). the formula to turn units of "gas" Gwei:

Transaction fee = Gas Price * Amount of Gas Consumed

To convert from Gwei to Eth (1Eth= 1000000000 Gwei)

To convert Ethereum (ETH) to United States Dollar (USD). At the time of research, the average is approximately: 1Eth equals $ 2,250.91. Table 1 show the cost of deploy smart contract.

Table. 1. Cost of Deploy Smart Contract

T1	Deploy Smart Contract
Gas Consu ned	460013 (Gas)
Cost (Gwei)	460013 * 20=9200260 (Gwei)
Cost (ETH)	9200260/1000000000 = 0.00920026 (ETH)
Cost ($)	20.9490($)

7.3.2 Cost of Store Certificate's Hash

The cost of saving a certificate's hash is the cost of the transaction of transmitting the code to the blockchain. The cost when the smart contract changes from one state to the next. Table 2 shows the gas used in some transactions and the cost in ether and dollars.

Table. 2. Cost of Store Certificate's Hash**.**

T.No	Gas Consu ned	Cost=Gas *gas Price	Cost (ether)	Cost $
T2	47725	954500	0.0009545	2.1734
T3	47701	954020	0.00095402	2.1723
T4	47689	953780	0.00095378	2.1718
T5	47725	954500	0.0009545	2.1734
T6	47737	954740	0.00095474	2.1739

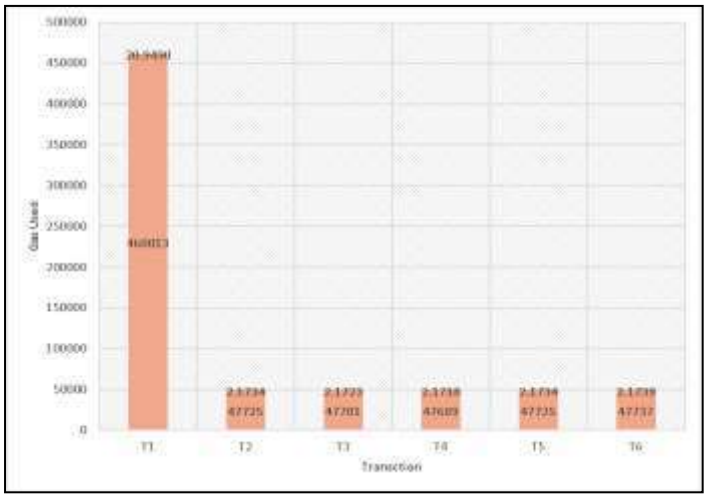

Figure .3. Transaction & Cost.

7.3.3 Cost of Certificate Verifying

The cost of verifying a certificate is zero because the function that verifies a certificate looks for a hash in the blockchain to see if it is found, without altering the state of the blockchain. This feature facilitates the process of verifying certificates by eliminating the need for an account on any Blockchain network.

7.4 Security Analysis

To achieve the highest level of transparency, we take advantage of Ethereum's "public" blockchain. Since there is no central authority managing the database, the system's functionality is guaranteed by a combination of economic incentives with a complex cryptographic data verification system managed by a specific consent protocol shared by all the nodes of the network.

Data is saved on the Sia network after it is uploaded to filebase. In doing so, Reed-Solomon erasure coding is used to shard objects into 30 pieces. These components are dispersed among servers located all over the world for optimal redundancy and security. They are encrypted. Only 10 of the 30 pieces are ever required to recover a file, providing extraordinary availability. This is an excellent method of reducing downtime without having to spend money on new infrastructure. (Jayden, 2020)

7.5 Publish DAPP

In this DAPP, after universities have sent approved certificates. The certificate pdf file will be uploaded to the filebase buckets, where it will be stored in the system. Figure 4 shows uploaded files in the filebase.

After the file has been uploaded, the CID code of the file will be returned, which can be used to access the files. Then, the CID code will be stored on the blockchain.
MetaMask will prompt a message to confirm the transaction. The confirmation of the transaction will cost a few ethers, which will be subtracted from the account. Figure 5 shows the confirm message from MetaMask. After that, the result will show the CID code of the file uploaded, and finally, it will be printed and attached to the certificate. Figure 6 shows the interface of DAPP.

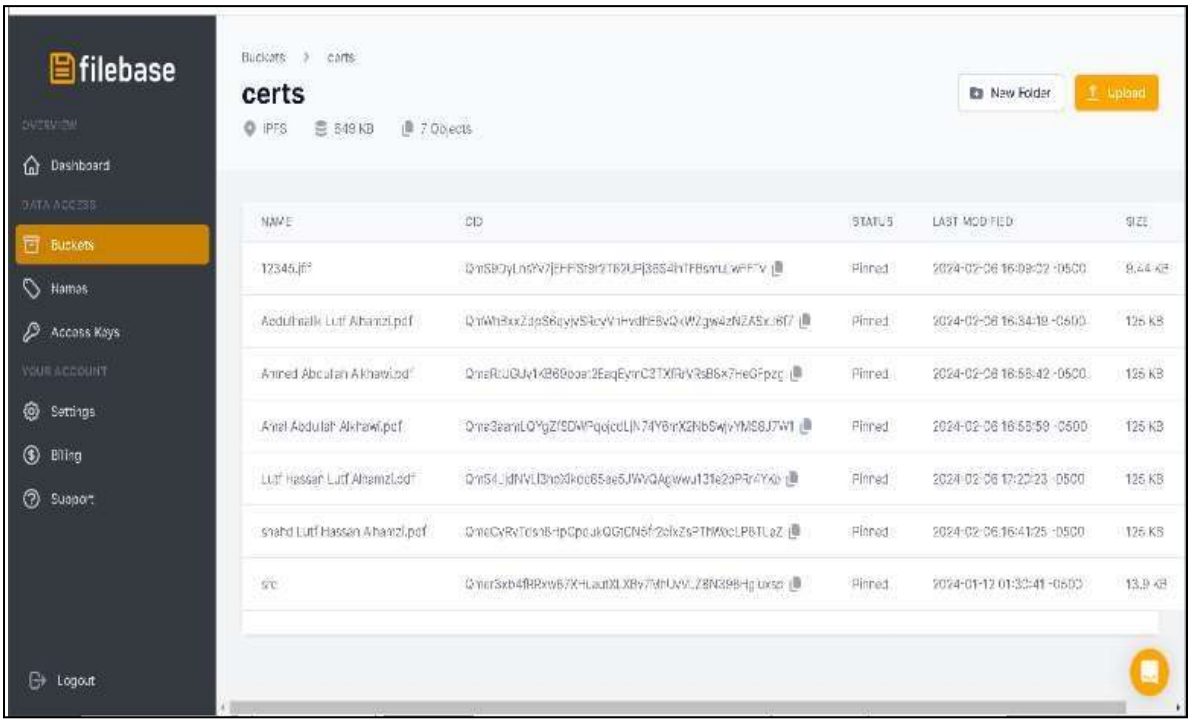

Figure .4. Uploaded files in the Filebase.

Figure5. Confirm message from MetaMask

Figure .6. Interface of publish certificates DAPP**.**

7.6. Verification DAPP

The verification process is done simply by entering the certificate hash. If the certificate hash is stored in the blockchain, the certificate file will be displayed as shown in figure 7. Otherwise, the message "certificate not found "is printed, as figure 8 shows.

Figure.7. Valid certificate hash.

Figure.8. Invalid certificate hash.

8. Conclusions

Credential fraud is a common and ubiquitous activity that erodes trust in educational establishments. This suggested solution aims to utilize filebase and blockchain to store and validate academic certificates. Because the digital certificates are stored and the certificate's hash is stored in the blockchain, the framework not only makes certificate verification simpler but also lowers the risk of missing physical certificates. All things considered, the suggested method has the lowest possible cost and the power to completely transform the academic certificate verification process, improving transparency, effectiveness, and security for all parties.

References

[1] Badhe, Vipul, Nhavale, Pooja, Todkar, Sonal, Shinde, Prajakta, & Kolhar, Kiran. (2020). Digital Certificate System for Verification of Educational Certificates using Blockchain. International Journal of Scientific Research in Science and Technology, 45-50.
[2] Blockchain cost structure: The Hidden Costs of Smart Contracts on Blockchain. (2024 , Mar 4). Retrieved from https://fastercapital.com/content/Blockchain-cost-structure--The-Hidden-Costs-of-Smart-Contractson-Blockchain.html
[3] Blockchain Council. (May 18, 2023). Retrieved from https://www.blockchaincouncil.org/blockchain/ganache-blockchain-all-you-need-to-know/
[4] Christian E. Pulmano,Maria Regina Justina E. Estuar,Marlene M. De Leon,Hans Calvin L. Tan, Nicole Allison S. Co, Lenard Paulo V. Tamayo. (2023). Towards the Development of a Blockchain-based Decentralized Digital Credential System using Hyperledger Fabric for Participatory Governance . Procedia Computer Science, 99–106.
[5] Gas Market: Analyzing Gas Market Dynamics in Ethereum's Network. (2023). Retrieved from https://fastercapital.com/content/Gas-Market--Analyzing-Gas-Market-Dynamics-in-Ethereum-sNetwork.html
[6] Howell, J. (2023, December 28). create dapp with react. Retrieved from https://101blockchains.com/createdapp-with-react/
[7] Jayden. (2020, Jun 11). movebot. Retrieved from https://movebot.io/blog/blockchain-s3-storage-withfilebase
[8] Kumutha.K , S.Jayalakshmi. (2021). The Impact of the Blockchain on Academic Certificate Verification System-Review. EAI Endorsed Transactions on Energy Web .
[9] Kumutha.K1, Dr.S.Jayalakshmi. (2021). Blockchain Technology and Academic Certificate AuthenticityReview . ResearchGate.
[10] Li, Hongzhi, & Han, Dezhi. (2019). EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme. IEEE Access, 7, 179273-179289.
[11] Ocheja, Patrick, Agbo, Friday Joseph, Oyelere, Solomon Sunday, Flanagan, Brendan, & Ogata, Hiroaki. (2022). Blockchain in Education: A Systematic Review and Practical Case Studies. IEEE Access, 4, 2016.
[12] Rana F. Ghani , Asia A. Salman , Abdullah B. Khudhair, Laith Aljobouri. (2022). Blockchain-based student certificate management and system sharing using hyperledger fabric platform. Periodicals of Engineering and Natural Sciences, 10, 207-218.
[13] Shaik Arshiya Sultana,Chiramdasu Rupa, Ramanadham Pavana Malleswari and Thippa Reddy Gadekallu. (2023). IPFS-Blockchain Smart Contracts Based Conceptual Framework to Reduce Certificate Frauds in the Academic Field. information.
[14] Tasfia Rahman,Sumaiya Islam,Arunangshu Mojumder, Abul Kalam,Nafees Mansoor. (2023). VerifiChain: A Credentials Verifier using Blockchain and IPFS. Springer Nature.
[15] Tenorio, E. M. (2021, JUNE 29). Advantages and disadvantages of Blockchain. Retrieved from https://www.bbva.ch/en/news/advantages-and-disadvantages-of-blockchain/
[16] TRUFFLE SUITE. (n.d.). Retrieved from https://archive.trufflesuite.com/docs/truffle/
[17] Web3.js Docs. (2024). Retrieved from https://docs.web3js.org/guides/getting_started/introduction
[18] What is MetaMask? (2024, March 5). Retrieved from https://sdlccorp.com/post/what-is-metamask-andits-benefits/