Block Verify:

Generation and Validation of e-Certificate using Blockchain

Swati Jadhav
Department of Computer Engineering
Vishwakarma Institute of Technology
Pune, India
swati.jadhav@vit.edu

Daksh Jadhav
Department of Computer Engineering
Vishwakarma Institute of Technology
Pune, India
daksh.jadhav221@vit.edu

Shivendra Jadhav
Department of Computer Engineering
Vishwakarma Institute of Technology
Pune, India
shivendra.jadhav22@vit.edu

Jiva Shelke
Department of Computer Engineering
Vishwakarma Institute of Technology
Pune, India
jiva.shelke22@vit.edu

Dheeraj Kakade
Department of Computer Engineering
Vishwakarma Institute of Technology
Pune, India
dheeraj.kakade22@vit.edu

Abstract — ***BlockVerify is a decentralized platform created to offer a safe and impenetrable way to use blockchain technology for document verification. BlockVerify guarantees the authenticity of documents by utilizing the immutability and transparency of the Ethereum blockchain. This makes it the perfect solution for individuals and organizations that need strong document verification. Users of BlockVerify can upload metadata for decentralized storage, including IPFS hashes, along with document hashes. The platform makes sure that the only people who can add and edit document records are authorized exporters who are managed and added by the contract owner. Document verification, ownership transfer, exporter management, and hash storage are important aspects. The project develops smart contracts using Solidity and Ethereum (Sepolia testnet), and it has an easy-to-use online interface using technologies like HTML, CSS and JavaScript to promote communication and MetaMask for secure wallet interactions. With future ambitions to expand to the mainnet and support new document kinds, BlockVerify intends to combat document fraud by offering a dependable way to check the legitimacy of documents.***

Keywords— Blockchain, Document Verification, Ethereum, Smart Contracts, Decentralized, Tamper-Proof, IPFS, Exporter Management, Solidity, Sepolia Testnet.

I. INTRODUCTION

With the increasing digitization of processes and documentation, the use of electronic certificates (e-certificates) has become widespread. E-certificates serve as digital credentials for various purposes such as educational qualifications, professional certifications, and identity verification. However, ensuring the authenticity and integrity of these e-certificates poses a significant challenge.

Traditional methods of certificate validation, such as centralized databases or certificate authorities, are susceptible to fraud and tampering. Moreover, these methods often lack transparency and require trust in a central authority. Blockchain technology offers a decentralized and transparent solution to these challenges.

Blockchain technology, originally brought to prominence through its application in cryptocurrencies like Bitcoin, functions as a distributed ledger that facilitates secure and transparent record-keeping across various industries. This innovative system ensures that all transactions are permanently recorded and accessible to participants, enhancing both trust and accountability. Each block in the blockchain contains a list of transactions, and once added, it becomes immutable, meaning it cannot be altered or deleted. This property makes blockchain an ideal candidate for storing and verifying e-certificates.

In this paper, we present "BlockVerify," a system that leverages blockchain technology for the validation of e-certificates. Blockify aims to enhance the security and reliability of e-certificates by providing a decentralized and tamper-proof platform for their storage and verification. By using blockchain, Blockify eliminates the need for a central authority, reducing the risk of fraud and ensuring the integrity of e-certificates.

II. RELATED WORKS

It offers a strong solution to protect and confirm digital academic credentials by utilizing peer-to-peer networks, blockchain technology, public-private key encryption, and proof of work [1].

This work proposes a Blockchain-based system using Ethereum, DApps, and smart contracts to rapidly verify academic degrees via a web application with OCR and Blockchain modules [2].

979-8-3315-1905-6/24/$31.00 ©2024 IEEE
DOI 10.1109/ICACCTech65084.2024.00039

This study introduces a blockchain-based platform for verifying academic records. It uses the decentralized nature of blockchain technology to testify student's academic honesty and scholars, while exploiting the privacy-preserving properties of the RSA algorithm [3]

It provides a decentralized blockchain based application which uses the ethereum network for secure document verification for governments, organizations, and individuals [4].

This research proposed a decentralized web application for digital document verification using P2P cloud storage and ethereum blockchain to enhance transparency and security [5].

The platform like ethereum and hyperledger used to analyze blockchain based solutions for different certificates focusing on smart contracts and cryptographic hashing [6].

It provides digitally signed certificates and are stored on the blockchain where each certificate is assigned a unique cryptographic hash and relevant metadata [7].

This research provides a simple GUI of certificate generation and validation system which allows users to define templates and format the certificate without any XML knowledge [8].

This proposes cross-domain authentication and secure certificate revocation scheme based on blockchain which address PKI inefficiencies and DD0S vulnerabilities by replacing X.509 signatures with certificate hash values [9].

The DistB-CVS cloud- based, blockchain-powered system verifies academic certificates in countries banning cryptocurrencies and offers a potential solution for academic certificate issuing [10].

The certificate authority verifies their reliability before issuing certificates, enhancing security for simple devices with lower storage and bandwidth requirements [11].

The paper proposes a blockchain-based certificate verification system to decentralize and secure the process of certificate issuance and validation. This approach aims to enhance trust, prevent fraud, and streamline verification in educational and professional settings [12].

The paper explores how blockchain technology can redefine trust in the management and verification of digital certificates by providing a decentralized, transparent, and secure framework [13].

The paper explores how blockchain can enhance privacy and security in managing personal identities. They discuss the challenges and opportunities of implementing these decentralized systems [14].

It focuses on improving the reliability, security, and scalability of blockchain systems through effective validation methods [15].

They have conducted research on addressing document forgery, emphasizing how advanced technologies enable duplication and modification of sensitive documents [16].

This study explores the potential of blockchain in higher education to enhance privacy and transparency. It presents a model for generating and authenticating academic credentials, focusing on the role of smart contracts and future testing scenarios [17].

This research explores the potential of blockchain systems in higher education to address privacy, transparency, and service digitization issues that persist in centralized systems. It presents a conceptual model and detailed architecture for generating and authenticating academic credentials [18].

III. METHODOLOGY

A. *Blockchain*

Blockchain is a cutting-edge technology that replaces the existing centralized data storage method with more security and convenience. This network stores data through transactions. With blockchain technology, a dispersed network is created to store all of the data decentralized. A blockchain network is made up of several personal computers, each of which connects to other computers in the network and functions as a separate database. Blockchain can be described as a decentralized network where each participating computer, referred to as a node, is interconnected through a Peer-to-Peer (P2P) communication protocol. In this system, personal computers that join the network act as nodes, contributing to the overall security and transparency by validating and recording transactions across the distributed ledger. Since every other node in the network has access to the real data, no one node can alter the data on its own. Also, each Block is secured through a hash code.

Additionally, each block in the network is linked to the others as a chain of blocks by storing the hash code of the block before it [2]. Any modification to a single block will instantly alter the hash code, rendering the entire transaction null and void. As a result, the network no longer has a centralized authority, making blockchain technology more trustworthy and transparent for storing and retrieving real data. Therefore, any data recorded on a blockchain network is unchangeable.

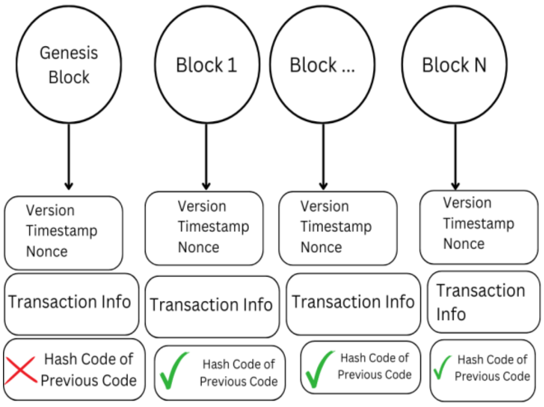


Fig. 1. Blockchain Structure

The structure is shown in Figure 1, where the genesis block—the first block—has no hash value from the previous block . Many computers located throughout the system, numbering in the thousands or even millions, validate each transaction on a block.

That block can be added to the network once the other nodes have verified it.

B. Ethereum

Ethereum is a distributed, public, worldwide blockchain network designed to manage the network's computer system infrastructure. It is an open-source platform with several features, including ether, smart contracts, and more. [6]. A smart contract is a self-executing piece of code deployed on the Ethereum network that automatically activates and runs when a predefined event occurs within a block. Smart contracts can be distributed, self-executing, and shared throughout the blockchain [11]. A coin for Ethereum-based apps is called ether. Digital currency used for trading in online transactions is known as cryptocurrency. Ether functions as a charge for transactions associated with any event. Ethereum, then, offers developers a platform on which to build any kind of decentralized blockchain application.

C. Solidity

High-level, statically typed programming languages like Solidity are made especially for creating Ethereum Virtual Machine (EVM) smart contracts. To establish self-executing contracts, developers write code in Solidity that contains the conditions of the agreement explicitly. The Solidity compiler (solc) converts the code into EVM bytecode, which the EVM can subsequently execute, when a Solidity smart contract is deployed to the Ethereum network. Solidity plays a crucial role in the blockchain ecosystem by facilitating the development and operation of automated contracts and decentralized apps (DApps) without the need for a middleman or central authority. Modularity and reusability in contract creation are encouraged by Solidity's support for features like inheritance, libraries, and user-defined types like structs and enums.

By enabling conditional function execution, modifiers in Solidity provide an additional layer of capability. Additionally, by recording significant actions that can be tracked off-chain, Solidity's event support makes it easier for smart contracts and external apps to communicate. Solidity is a fundamental tool for blockchain development because of these properties and its interaction with the Ethereum blockchain, which provide security, immutability, and transparency when carrying out intricate operations and transactions.

D. Infura

Infura is utilized in our suggested method to run a user's PC as an Ethereum node. In general, users had to first construct an Ethereum wallet in order to communicate with the Ethereum blockchain network. A user cannot utilize the cryptocurrency "Ether" or perform any transactions or pay the fees associated with each transaction if they do not have an Ethereum wallet. By removing the hassle of setting up an Ethereum wallet on their own, Infura is a hosted Ethereum node cluster that facilitates user interaction with any decentralized Ethereum application.

E. Interplanetary File System

The Peer to Peer (P2P) data distribution, storage, and transfer network protocol is known as the InterPlanetary File System (IPFS). IPFS locates each file independently, connecting every machine on a global network, using a content-based addressing scheme. It appears that this allows a user to host any content for other network users as well as receive content from any node that contains the desired content. A portion of the total data in the IPFS system is carried by specific user operators, offering a flexible mechanism for file distribution and storage. By using a data file's unique content address, any network user can host data files or other types of information, and other network users can then recognize, request, or access those files from any desktop computer that contains it.

F. Hash Function SHA-3

The hash value can be thought of as a human fingerprint that is specific to each input, as seen in Figure 2.

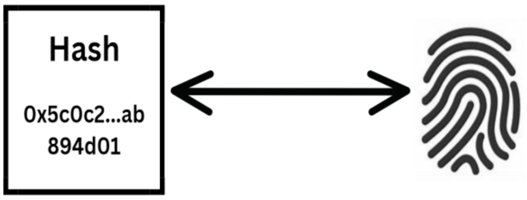


Fig. 2. Hash value

An enormous quantity of storage space would be needed for the original file in the database. Therefore, we require a method for mapping files and documents in a unique form using a smaller size than the original. To complete this task, a hashing function will be used. A complicated mathematical function known as a cryptographic hash function is one that accepts variable-length or variable-size input data and produces a unique, fixed-length or fixed-size output for each supplied data. A hash function is always one-way. Consequently, it is not computationally viable to determine a hash function's input from its hash output. Cryptography and digital signatures are two frequent uses for hash functions. For instance, blockchains, key derivation, pseudo-random number creation, and password security and message verification. Hashing mostly guarantees the highest level of security for any data content. Among a few of the algorithms, we have used Keccak (SHA-3) algorithm. SHA-3 can convert large input data to a fixed size 256 bit hash code. Each time a document is uploaded, its hash is appended along with the organization's public key and the date it was added. This serves to further confirm the document's legitimacy. Additionally, the organization will obtain an IPFS hash that only they may view and distribute with a specific user to enable additional document downloads. Thus, any document that an organization uploads into our system is added to blockchain and further information about the additional document is displayed on the screen. For additional verification, details such as the uploader's identity and public address, the upload time, and an IPFS hash for that specific file are provided. Additionally, if the document is corrupted in any way, the hash value will change, alerting the authorities to the change. In addition, any user or verifier can, for general purposes, download a document containing an IPFS hash or verify a given document without requiring access to Ethereum or IPFS, this processing is done on the server side to improve usability.

G. *Remix IDE*

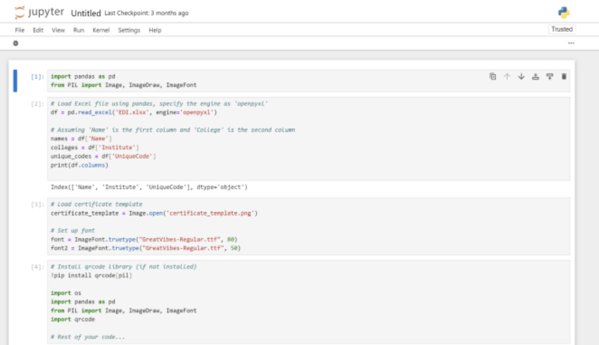
An integrated development environment called Remix IDE was created especially for creating, evaluating, debugging, and implementing Solidity smart contracts on the Ethereum network. Remix is a web-based application that makes development easier for both novice and seasoned developers by offering an approachable and intuitive user interface. Its main features are a Solidity compiler, a robust debugger for troubleshooting and optimizing smart contract code, and a code editor with syntax highlighting and autocompletion. Remix also provides an integrated deployment environment that lets developers launch their contracts straight from the IDE into other Ethereum networks, including as testnets and the mainnet. Additionally, the programme enables plugins, which increase its capabilities by adding features like code formatting, static analysis, and integration with other tools.

Remix IDE streamlines the complete contract development workflow, from creating and testing code to deployment and interacting with the Ethereum blockchain, and as such, plays a critical role in the Solidity development ecosystem.

H. Testnet

Sepolia is a testnet, a network for testing designed to resemble the Ethereum mainnet. Developers may test and debug their applications and smart contracts using it without worrying about breaking the Ethereum mainnet. Before releasing their apps to the main Ethereum network, developers may test new features and make sure their apps are stable and secure in sandbox environments like Sepolia.

I. Jupyter Notebook


jupyter Untitled Last Checkpoint: 3 months ago
File Edit View Run Kernel Settings Help
Trusted

```
[1]: import pandas as pd
     from PIL import Image, ImageDraw, ImageFont

[2]: # Load Excel file using pandas, specify the engine as 'openpyxl'
     df = pd.read_excel('EDI.xlsx', engine='openpyxl')

     # Assuming 'Name' is the first column and 'College' is the second column
     names = df['Name']
     colleges = df['Institute']
     unique_codes = df['UniqueCode']
     print(df.columns)

     Index(['Name', 'Institute', 'UniqueCode'], dtype='object')

[3]: # Load certificate template
     certificate_template = Image.open('certificate_template.png')

     # Set up font
     font = ImageFont.truetype("GreatVibes-Regular.ttf", 80)
     font2 = ImageFont.truetype("GreatVibes-Regular.ttf", 50)

[4]: # Install qrcode library (if not installed)
     !pip install qrcode[pil]

     import os
     import pandas as pd
     from PIL import Image, ImageDraw, ImageFont
     import qrcode

     # Rest of your code...
```

Fig.3 Jupyter Notebook

There are various benefits to generating certificates with this Python script in a Jupyter notebook. Jupyter notebooks offer an interactive environment that makes it simple to debug and alter the code as needed by enabling the script to be executed step-by-step and visualized. The notebook style also makes it easier to document each phase using markdown cells, which improves the process's reproducibility and clarity. This is especially helpful for creating certificates since it enables instantaneous visual feedback-based template design, font selection, and text element positioning adjustments. A streamlined workflow is also ensured by the integration of `Pillow` for image processing and `pandas` for data management within Jupyter, from reading input data to creating and saving the final certificates.

J. Security and Privacy

Our system is built on the robust security features inherent to blockchain technology, such as cryptographic hashing, digital signatures, and encryption. The following measures ensure data security and privacy: -

i.Hashing: Every e-certificate is hashed using the SHA-256 algorithm, making the data immutable and resistant to tampering. –

ii. Digital Signatures: Certificates are signed using public-private key cryptography to authenticate the issuing authority and prevent forgery.

iii. Encryption: Sensitive data (such as personal details) is encrypted to protect users' privacy during transmission and storage. Privacy Considerations Blockchain’s immutability iv.provides a high level of security but can pose challenges for personal data management.

Our system complies with data protection regulations by Ensuring that only public certificate metadata is stored on the blockchain, while sensitive personal data remains encrypted and stored off-chain. Allowing selective disclosure of certificate information, ensuring privacy for certificate holders. The primary threats to our system include Sybil attacks, man-in-the-middle attacks, and data breaches. Our use of consensus algorithms and cryptographic protocols mitigates these threats by utilizing a proof-of-stake (PoS) consensus mechanism, our blockchain system prevents malicious actors from gaining control over the network while ensuring that all data is encrypted, rendering intercepted information unreadable without the appropriate decryption keys.

K. Scalability and Deployment Challenges

Our system's performance is evaluated under both light and heavy usage scenarios. As the number of certificates generated increases, the following challenges may arise:

- Blockchain size: As more certificates are added, the size of the blockchain grows, potentially leading to slower query times.

- Transaction volume: With an increase in the number of transactions, transaction fees may rise, impacting the scalability of our system.

To address these issues, we propose the following scalability solutions:

- Layer-2 scaling solutions such as state channels or sidechains can offload some of the transaction volume from the main chain, ensuring that the core blockchain remains efficient.

- Off-chain storage: Non-essential data is stored off-chain to reduce blockchain bloat, while hashes and essential metadata remain on-chain for verification purposes.

Deployment Challenges :The deployment of the system in a real-world setting may face challenges such as:

- Network latency: In geographically distributed networks, there may be delays in reaching consensus or validating certificates.

- Infrastructure requirements: The hardware and software infrastructure required for blockchain systems can be costly to deploy at scale.

IV. WORKING

A. User Section

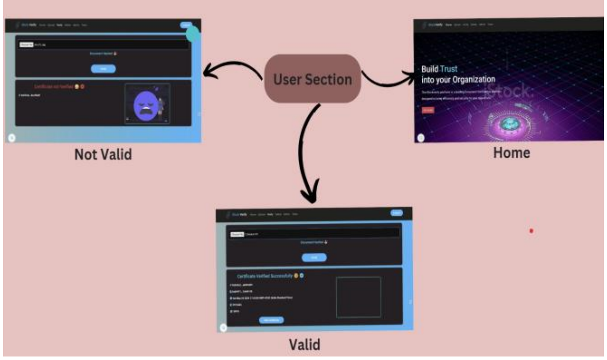
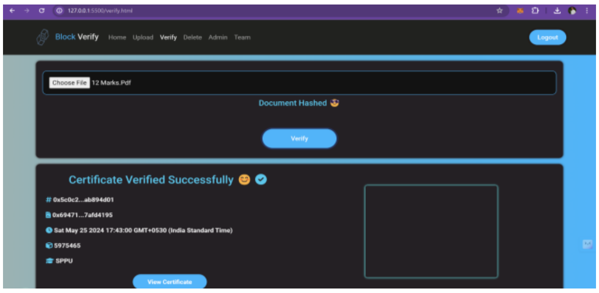


Fig.4 Flowchart of the User Section in website

The entire process is so safe that no document can be harmed. This project is therefore heavily focused on providing a strong protection against any cyberattack. Users can effortlessly access their information at any time, ensuring that their files are always secure and readily available, without the fear of them being lost or compromised by hackers.

We have used HTML, CSS and JavaScript to develop the front-end of our system, even though the back-end has numerous sophisticated technologies. The user interface of our website was meticulously created with the intention of being as user-friendly as possible. This website is easily manageable by a novice without any prior knowledge of Ethereum or blockchain, whether for professional work or otherwise.

Three crucial functions of the system are upload, verify, and download. The entire back-end procedure is displayed. There are primarily two distinct sections—one for the organization and the other for general purpose—that work together to preserve usability for every use case scenario. Any institution or organization is referred to in the admin section. Before concluding a transaction, an organization or institution may occasionally need to carefully review any documents that are provided to them , otherwise they can never be certain of the document's legitimacy . For the purpose of any organization , It should have metamask installed in order to upload a verified document in the blockchain .Thus, any document that an organization uploads into our system and hash of the uploaded documents will be stored in our blockchain and further information about the additional document is displayed on the screen .



12 Marks.Pdf

Document Hashed 😎

Certificate Verified Successfully 😊 ✓

# 0x5c0c2...ab894d01

0x69471...7afd4195

Sat May 25 2024 17:43:00 GMT+0530 (India Standard Time)

5975465

SPPU

Fig.5 Verify Section

For additional verification, details such as the uploader's identity and public address, the upload time, and an IPFS hash for that specific file are provided. Additionally, if the document is corrupted in any way, the hash value will change, alerting the authorities to the change. In addition, any user or verifier can, for general purposes, download a document containing an IPFS hash or verify a given document without requiring access to Ethereum or IPFS; this processing is done on the server side to improve usability.

B. *Admin Section*

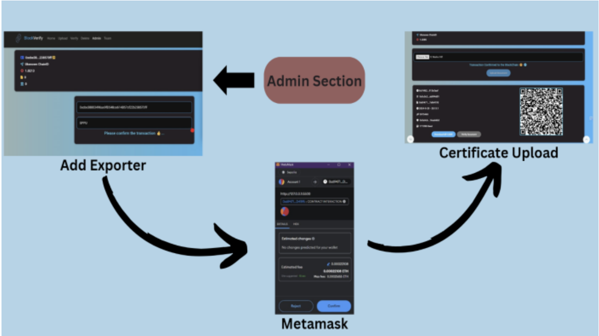
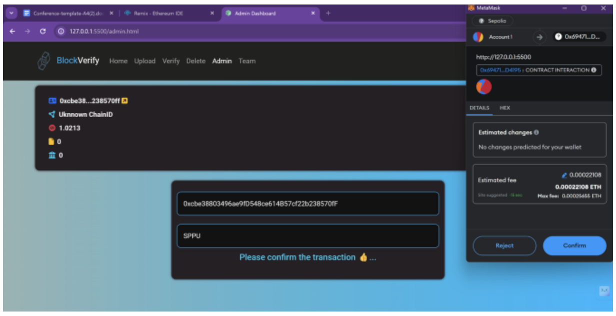


Fig.6 Flowchart of the Admin Section in website

Admins are responsible for issuing certificates. They input the necessary details, such as date of issuance, and any other relevant information. They generate a unique hash for each certificate and store it on the blockchain, ensuring the certificate's authenticity and immutability.The admin section of BlockVerify is a critical component of the platform, enabling the management of document verification processes via blockchain technology. This section provides administrators with the tools to add new exporters and upload certificates, ensuring these documents are securely and immutably recorded on the blockchain. The interface is designed to be intuitive, featuring tabs such as Home, Upload, Verify, Delete, Admin, and Team, allowing easy navigation through various functions of the platform.



0xcbe38...238570ff

Uknnown ChainID

1.0213

0

0

0xcbe38803496ae9fD548ce614B57cf22b238570fF

SPPU

Please confirm the transaction 👍 ...

http://127.0.0.1:5500

0x69471...D4195 : CONTRACT INTERACTION

Estimated changes

No changes predicted for your wallet

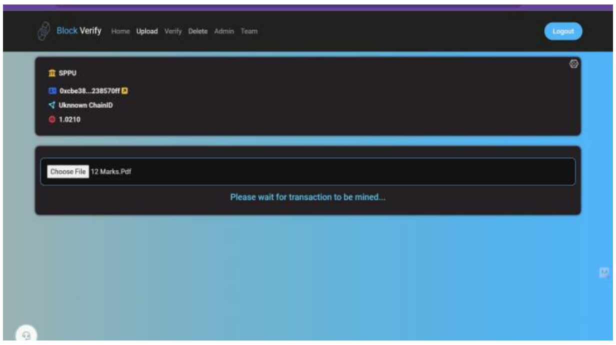
Estimated fee 0.00022108

0.00022108 ETH

Max fee: 0.00025655 ETH

Fig.7 Add Exporter

To add a new exporter, an administrator inputs the exporter's address into a designated field. Once the address is entered, the admin confirms the transaction through MetaMask, a widely used cryptocurrency wallet and gateway to blockchain applications. MetaMask provides an additional layer of security by showing the transaction details, including estimated changes and fees, before the admin confirms it. This ensures that all actions taken within the admin section are transparent and secure, reinforcing the integrity of the platform's operations.



SPPU

0xcbe38...238570ff

Uknnown ChainID

1.0210

12 Marks.Pdf

Please wait for transaction to be mined...

Fig.8 Upload Certificate and Hash of Certificate will store in Blockchain

The certificate upload process is similarly streamlined. Administrators select a certificate file (such as a PDF) and upload it to the system. Upon uploading, the transaction is confirmed on the blockchain, guaranteeing that the document is recorded in an immutable and verifiable

manners. The interface displays the document's hash and provides options to download a QR code, which can be used

for quick and easy verification. This process not only ensures the authenticity of the uploaded certificates but also simplifies verification for users.

Overall, the admin section of BlockVerify plays a vital role in maintaining the platform's efficiency and security. By integrating blockchain technology and MetaMask, it offers a robust solution for managing document verification processes. This section ensures that every action, from adding exporters to uploading and verifying certificates, is conducted with the highest level of security and transparency, making BlockVerify a reliable platform for document authentication.

One of the notable features of the admin section is the ability to view the number of documents associated with each exporter. This information is readily visible on the admin dashboard, allowing administrators to quickly assess the activity and engagement of each exporter within the system. This feature helps in managing and monitoring the volume of documents being processed and verified, ensuring that the platform maintains an organized and efficient workflow

V. RESULT AND DISCUSSION

To assess the performance, we conducted a series of tests focused on key performance indicators such as

i. Validation speed: Validation of certificates occurs in approximately **13-15 seconds** on average.

ii. Cost per transaction: On our platform, the average transaction cost for certificate validation is **0.00022108 ETH**. This cost covers the fees associated with processing and securing the transaction on the blockchain network.

Feature	**Our System**	**Blockchain Technology for Digital Certificates**	**Centralized vs Blockchain-based Digital Certificates**
Transaction Cost	0.0002 ETH	0.0005 ETH	0.00035 ETH
Time per Transaction	13-15 seconds	30 seconds	25 seconds
Security	Blockchain-based with Smart Contracts	Blockchain-based with Proof of Work	Centralized with encryption

Fig. 9 Table showing comparisons of parameters with other solutions

We conducted usability testing with a group of 8 potential users, the testing focused on:

- Ease of use of the certificate generation and validation interfaces.

- Speed and accuracy of the system's outputs.

The following feedback was collected:

User experience: 75% of users reported that the system was intuitive and easy to navigate. However, some users suggested simplifying the validation process by integrating an automatic notification system.

VI. FUTURE SCOPE

BlockVerify has a bright future ahead of it, with several important areas for development and improvement. Accessibility and user interaction will increase once Sepolia testnet moves to the Ethereum mainnet. The platform is intended to include more document types, including contracts and certificates, so that it can be used in a variety of industries. The user experience will be improved by ongoing UI development, especially mobile optimization. Investigating cross-chain compatibility may also improve communication with alternative blockchain technologies. Future plans include for using machine learning for better fraud detection with additional security features like multi-signature verification. Establishing collaborations with academic institutions and enterprises will promote broader implementation, and API creation will enable smooth integration with current systems. BlockVerify can establish by concentrating on these regions

VII. CONCLUSION

With BlockVerify, the problems of document verification are addressed in a novel way by combining IPFS with blockchain technology. BlockVerify provides a safe and impenetrable way for verification by guaranteeing the validity and integrity of digital documents through its decentralized platform. The platform offers an unchangeable and transparent record of document history by employing IPFS for distributed storage and storing document hashes on the Ethereum blockchain. BlockVerify's deployment, which prioritizes user-friendly interfaces and safe interactions using MetaMask, shows a dedication to trust and accessibility. BlockVerify thus not only meets the urgent demand for trustworthy document verification, but it also establishes a new benchmark for integrity and openness in digital transactions.

ACKNOWLEDGMENT

We extend our sincere gratitude to our project guide, Prof. Swati Jadhav and HOD Prof. Sandip Shinde, for their invaluable guidance and support throughout this research.

REFERENCES

[1] G. Balamurugan and K. K. A. Sahayaraj, "A Blockchain Based Certificate Authentication System," 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023, pp. 1-7, doi: 10.1109/ICCCI56745.2023.10128289.

[2] H. Gaikwad, N. D'Souza, R. Gupta and A. K. Tripathy, "A Blockchain-Based Verification System for Academic Certificates," *2021 International Conference on System, Computation, Automation and*

Networking (ICSCAN), Puducherry, India, 2021, pp. 1-6, doi: 10.1109/ICSCAN53069.2021.9526377.

[3] S. Huang, "Academic Records Verification Platform Based on Blockchain Technology," *2020 International Conference on Computer Science and Management Technology (ICCSMT)*, Shanghai, China, 2020, pp. 203-206, doi: 10.1109/ICCSMT51754.2020.00048.

[4] M. L. S. S, M. P. N and M. A. Shettar, "Block chain Based Framework for Document Verification," 2022 2nd International Conference on Artificial Intelligence and Signal Processing (AISP), Vijayawada, India, 2022, pp. 1-5, doi: 10.1109/AISP53593.2022.9760651.

[5] I. T. Imam, Y. Arafat, K. S. Alam and S. A. Shahriyar, "DOC-BLOCK: A Blockchain Based Authentication System for Digital Documents," *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, Tirunelveli, India, 2021, pp. 1262-1267, doi: 10.1109/ICICV50876.2021.9388428.

[6] U. B. A, M. S, M. M. H. A. S, N. Kumar, P. Aditya and A. Manjunath, "Blockchain Technology in Document Authentication: A Comprehensive Literature Review," 2023 4th International Conference on Communication, Computing and Industry 6.0 (C216), Bangalore, India, 2023, pp. 1-5, doi: 10.1109/C2I659362.2023.10431235.

[7] C. Vinay Chowdary1, V. Sudharshan2, K. Bhargav3, Ms. Mounika4 & Ms. Sterlin5 “Certificate Verification and Validation Using Blockchain” Computer Science and Engineering, Presidency University Bengaluru, Karnataka, India 560069

[8] A. D. Yusuf, M. M. Boukar and S. Shamiluulu, "Automated batch certificate generation and verification system," *2017 13th International Conference on Electronics, Computer and Computation (ICECCO)*, Abuja, Nigeria, 2017, pp. 1-5, doi: 10.1109/ICECCO.2017.8333321.

[9] P. Gu and L. Chen, "An Efficient Blockchain-based Cross-domain Authentication and Secure Certificate Revocation Scheme," *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, Chengdu, China, 2020, pp. 1776-1782, doi: 10.1109/ICCC51575.2020.9345108.

[10] M. Hasan, A. Rahman and M. J. Islam, "DistB-CVS: A Distributed Secure Blockchain based Online Certificate Verification System from Bangladesh Perspective," *2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT)*, Dhaka, Bangladesh, 2020, pp. 460-465, doi: 10.1109/ICAICT51780.2020.9333523.

[11] A. Garba, Z. Chen, Z. Guan and G. Srivastava, "LightLedger: A Novel Blockchain-Based Domain Certificate Authentication and Validation Scheme," in *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1698-1710, 1 April-June 2021, doi: 10.1109/TNSE.2021.3069128

[12] Verma, L., Budhiraja, A., Singh, S. (2024). Blockchain-Based Certificate Verification System: A Decentralized Approach. In: Woungang, I., Dhurandher, S.K., Singh, Y.J. (eds) Proceedings of the NIELIT's International Conference on Communication, Electronics and Digital Technology. NICEDT 2024. Lecture Notes in Networks and Systems, vol 1022. Springer, Singapore. https://doi.org/10.1007/978-981-97-3601-0_36

[13] Capece, G.; Levialdi Ghiron, N.; Pasquale, F. Blockchain Technology: Redefining Trust for Digital Certificates. *Sustainability* 2020, *12*, 8952. https://doi.org/10.3390/su12218952

[14] K. Gilani, E. Bertin, J. Hatin and N. Crespi, ”A Survey on Blockchain based Identity Management and Decentralized Privacy for Personal Data,” 2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS), Paris, France, 2020, pp. 97-101, doi: 10.1109/BRAINS49436.2020.9223312.

[15] Dusica Marijan, Chhagan Lal, Blockchain verification and validation: Techniques, challenges, and research directions, Computer Science Review, Volume 45, 2022, 100492, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2022.100492.

[16] Zainuddin, Muhammad & Choo, K.Y.. (2022). Design a Document Verification System Based on Blockchain Technology. 10.2991/978-94-6463-082-4_23.

[17] Rustemi, Avni & Atanasovski, Vladimir & Risteski, Aleksandar. (2023). Design of the Blockchain System for the Generation and Verification of Diplomas. 1-6. 10.1109/ET59121.2023.10279743.

[18] Rustemi, Avni & Dalipi, Fisnik & Atanasovski, Vladimir & Risteski, Aleksandar. (2024). DIAR: a blockchain-based system for generation and verification of academic diplomas. Discover Applied Sciences. 6. 10.1007/s42452-024-05984-1.