VeriSign : Blockchain based Document Verification System

Riddhi Sawant
Department of Computer Engineering
Rajiv Gandhi Institute of Technology
Mumbai, India

Aniket Singh
Department of Computer Engineering
Rajiv Gandhi Institute of Technology
Mumbai, India

Ayussh Srivastav
Department of Computer Engineering
Rajiv Gandhi Institute of Technology
Mumbai, India

Parija Vartak
Department of Computer Engineering Rajiv
Rajiv Gandhi Institute of Technology
Mumbai, India

Prof. Sunil Khachane
Department of Computer Engineering
Rajiv Gandhi Institute of Technology
Mumbai, India

***Abstract*—In our world it has become crucial to have secure, transparent and efficient processes for verifying documents. Traditional methods often rely on intermediaries, which can introduce vulnerabilities and cause delays. This abstract presents a solution. A document verification system based on technology that has the potential to revolutionize document verification. Blockchain innovation gives a powerful, scalable and private solution for verification. Blockchain is a decentralized database (distributed ledger) that records transactions or even digital events that have been executed and shared among the participating parties. Our project is a management system for the export and verification of certificates. It automates the process of generating certificates and reduces the cost and manual work needed for the verification of the same. The idea of our system about uploading a certificate by issued university. Then the system will hash it and then storing the document hash in the blockchain, in addition to storing the certificate itself in the blockchain file system. A QR code is given for verification purposes. The verifier gives a file or QR code, then the system will compare this hash with the hashes of certificates previously stored in the blockchain to verify whether it actually exists or not. If the certificate hash has existed in the blockchain, the same certificate will be retrieved from the blockchain file system. But if the certificate hash doesn't exist in the blockchain, the request will be answered negatively. The implementation of this system has shown results in terms of improved security measures, reduced fraud incidents, enhanced efficiency levels as well as cost savings.**

***Index Terms*—IPFS, Smart contracts, Verification, Privacy, IDE, Smart contract, Ethereum.**

I. INTRODUCTION

In an increasingly digital world, the exchange and verification of documents underpin countless aspects of our lives, from education and employment to finance and legal matters. Yet, the existing methods of document verification are often marred by inefficiency, opacity, and susceptibility to fraud. Enter the Blockchain-Based Document Verification System, a revolutionary solution poised to redefine how documents are verified, secured, and trusted in the digital age. Blockchain technology, renowned for its decentralization, cryptographic security, and transparency, forms the backbone of this innovative system. Rather than relying on centralized intermediaries, this system places control back into the hands of document owners and verifiers. Verifying certificates from schools and government agencies can be a hassle due to physical documents, causing delays and potential for fraud. But with blockchain technology, we can simplify this process. Blockchain is like an unchangeable digital ledger that securely stores certificate information. Once a certificate is recorded on the blockchain, it can't be altered, ensuring its authenticity. This means faster verification, less chance of mistakes, and reduced fraud. In short, blockchain offers a secure and efficient way to verify certificates, making life easier for everyone involved. Blockchain allows you to verify without having to be dependent on third parties. The data stored inside the blocks cannot be altered or deleted, which makes it unforgeable. Blockchain uses Distributed Ledger Technology (DLT), which is more reliable, more secure and cheaper compared to conventional cloud-based storage systems. With these advantages over conventional technologies, Blockchain would be an apt tool to create as to store, validate and share certificates in a secured manner, there by reducing the need for physical forms which in turn reduces cost, loss risks and mental distress .

II. RELATED WORK

In recent times, blockchain research has skyrocketed as more people realize it's not just for cryptocurrencies. At first, it was mainly used for verifying academic credentials because it's super secure. But now, businesses are also getting interested. The important thing about blockchain is how it spreads out data across a bunch of computers instead of keeping it in one place. This makes it way harder for anyone to mess with the data. Plus, once something is recorded on the blockchain, it's basically set in stone and can't be messed with. This makes it super secure and transparent. Businesses are starting to see the value of blockchain for keeping their data safe. Industries like finance, healthcare, and supply chain management are looking into using blockchain to beef up their security and protect against things like data breaches. With blockchain, they can make sure their data is legit and can't be messed with, which is a big deal in today's digital world. In a nutshell, blockchain is changing the game when it comes to security. Its decentralized setup and immutable record-keeping make it a powerful tool for keeping data safe and trustworthy, and businesses are taking notice.

The research paper outlines the development of a decentralized blockchain system, using Ethereum for document verification. It tackles challenges in authenticating documents by proposing a solution that eliminates third-party intervention, ensuring document immutability and security. The system involves local applications (”Nodes” or ”Blocks”) for verification, utilizing complex calculations to generate unique document hashes. The goal is to offer a secure and decentralized approach to document verification, avoiding single-entity control. The document discusses related works and presents the methodology, including software configurations with Truffle, Solidity smart contracts, and experimental results on the Ropsten Network, emphasizing tamper-proof security and decentralized ownership. [1]

The research paper explores a new system for verifying documents using blockchain, presented at a conference in 2022. It's designed to tackle the growing problem of fake documents by using blockchain's security features to make verification faster and cheaper. The system uses Ethereum blockchain and IPFS for storing documents, ensuring everything is decentralized and secure. It compares favorably to other systems and can be customized for different organizations. It's seen as a game-changer for verifying various documents securely and efficiently. [2]

The research paper explores the development of a blockchain-based identity verification system to replace traditional paper records. It covers objectives, literature survey findings, security solutions, methodology, and future plans. The system stores personal records on a decentralized blockchain, facilitating verification by users and authorities. The literature survey discusses blockchain applications, security issues, and regulatory challenges. The document details Agile Unified Process methodology, system design, and testing phases. Findings highlight user preferences, and future plans include real blockchain integration and biometric authentication. The conclusion stresses the importance of blockchain in securing personal data and foresees broader digitalization. Numerous scholarly references support the proposed system's development and societal impact. [3]

The research paper discusses the development of a secure document verification system using blockchain technology, with a focus on addressing document forgery challenges in Nigeria. The system stores user documents securely in the blockchain, utilizing interplanetary file system (IPFS) and digital signatures for integrity and authenticity. The study emphasizes the importance of secure document verification, comparing traditional methods and highlighting the advantages of blockchain technology. The proposed system's design, algorithms, and technical implementation are detailed, showcasing a web-based application using Java, MySQL, and Springboot. The study concludes by underscoring the system's potential to mitigate document forgery issues and enhance document integrity in various industries. [4]

The research paper outlines the creation of a Blockchain-Based Identity Verification System, aiming to overcome issues with traditional paper records. Using blockchain tech, it decentralizes personal data access for users, authorities, and third parties. Developed through the Agile Unified Process, it focuses on improving data availability and simplifying registration and verification processes. Challenges with current paper systems, like bulkiness and identity theft risks, are addressed. Future plans include enhancing security with biometrics and expanding the types of records stored. The system's acceptance and potential improvements are validated through testing and user feedback. Overall, it promotes blockchain's wider use for identity verification, emphasizing transparency and individual control over personal data. [5]

The research paper talks about creating a decentralized web app using Ethereum blockchain to verify digital documents. It aims to tackle document forgery by offering a transparent verification process. The system uses techniques like cryptography and digital signatures to verify documents securely. Each document gets a unique hash for security. It's designed for both organizations and general users. Organizations can upload and verify documents, while users can verify and download them. The system uses Infura and IPFS for secure document storage and interaction with the Ethereum blockchain. The document highlights blockchain's potential in various sectors and emphasizes its security and transparency benefits. Future plans include enhancing the system with more features for better accessibility and multiple file uploads. Overall, it aims to provide a secure and efficient solution for document verification, helping prevent data corruption and misuse. [6]

III. PROPOSED SYSTEM

Our proposed Blockchain-Based Document Verification System utilizing the InterPlanetary File System (IPFS) introduces an innovative solution to address the challenges of document security, integrity, and accessibility. Our system provides a convenient and secure way to manage your documents, ensuring they remain safe, authentic, and easily accessible whenever you need them.

A. Adding and editing document exporters

The smart contract allows the owner to manage document exporters who upload documents to the blockchain. The owner can add or edit exporters representing different entities. When an exporter uploads documents, a specific function is invoked.

B. Delete a document exporter

The owner also has the authority to delete exporters, preventing them from uploading documents in the future. This ensures control over document uploading privileges for security and integrity.

C. Uploading Documents

You start by uploading a document through our system. This function is only accessible to exporters, as it is used when each exporter uploads the documents to the blockchain and offers the user a copy of the document or QR code.

D. Deleting Documents

The owner or one of the exporters has the authority to delete a previously exported document.

E. Verifying Documents

This function verifies the validity of documents i.e. issued by particular university. When the verifier requests that a document be validated, this function is invoked.

IV. Design Details

The system architecture involve several key participants: the entity issuing the document, the document recipient (e.g., a company or another institution), and the individual presenting the document (e.g., a student or an employee). After the document is issued, it is securely stored in blockchain for added security and immutability. The individual is provided with a verification method, such as a PDF file or a QR code, which can be used for document validation. When the individual presents the document to a recipient, such as a company for job application or another institution for further studies, the recipient accesses the issuing entity’s verification platform. The validity of the document is then verified by checking it against the issuing entity’s records. Based on the verification outcome, the recipient institution makes a decision regarding the acceptance or rejection of the document. This streamlined workflow ensures the integrity and authenticity of the documents while facilitating efficient verification processes for all involved parties.

V. Methodology

A. Ethereum networks refer to the various blockchain networks that are based on the Ethereum protocol and ecosystem. These networks can differ in terms of their purpose, consensus mechanisms, scalability solutions, and governance models.

1) Polygon: Scalable layer 2 solution addressing Ethereum's limitations, offering cost-effective and fast verification. Seamlessly integrates with Ethereum's ecosystem, ideal for high-volume document processing with reduced expenses.

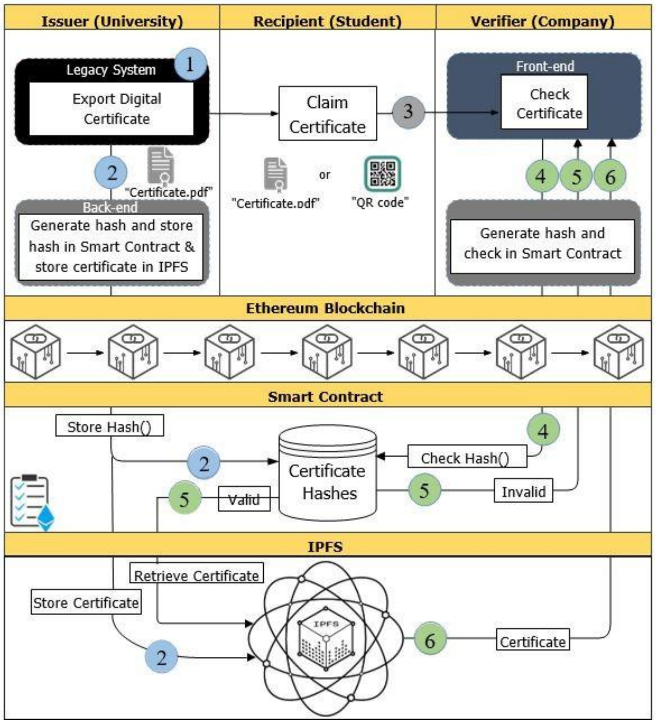


Fig. 1. Detailed System Flow of Blockchain based document verification system

2) Sepolia: Sepolia is a newer test network, the sync time for users wanting to run their own node is far less since the storage of the network is at a smaller state. It is not mostly recommended testnet due to its slower transaction times.

3) Ethereum: Mature, secure ecosystem with smart contracts for robust document verification. Reliability and decentralization ensure integrity, despite potential higher fees.

Ethereum emerges as the optimal choice for document verification due to its unmatched reliability, robust security measures, seamless compatibility with existing systems, and vibrant developer community support. With a proven track record for consistent performance, Ethereum's mainnet instills confidence in handling sensitive documents securely. Its rigorous security protocols ensure the integrity and authenticity of documents, while seamless compatibility streamlines integration efforts with other blockchain-based applications. Moreover, Ethereum's active developer community provides ongoing support, fostering innovation and ensuring the system remains up-to-date with the latest technological advancements. Despite potential benefits offered by alternatives like Sepolia and Polygon, Ethereum's comprehensive attributes position it as the preferred solution, ensuring long-term viability and trustworthiness for critical document verification applications..

B. Hashing algorithms play a crucial role in document verification systems by converting document data into a unique fixed-size hash value. This hash value can then be used to verify the integrity and authenticity of the document. Here are some commonly used hashing algorithms for document verification systems:

1) SHA -3: SHA-3, the latest SHA algorithm standardized by NIST, offers enhanced security against various attacks, supports customizable output lengths, and is suitable for a wide range of cryptographic applications requiring strong security.

2) SHA-256: SHA-256 is a widely-used cryptographic hashing algorithm that generates a 256-bit hash value. It's secure against collision attacks, efficient, and consistent. Commonly used for document verification, digital signatures, password hashing, and cryptocurrency transactions.

3) MD5: MD5 is an outdated hashing algorithm that generates a 128-bit hash value. It's now considered insecure due to vulnerability to collision attacks, making it unreliable for security-sensitive tasks. Though fast and efficient, it lacks the security of newer algorithms like SHA-256 and SHA-3. While previously used for document verification and password hashing, it's now discouraged for such applications.

We finalized SHA-3 approach with a length of 256 bits for our project as it is preferred for securing sensitive documents due to its enhanced security over SHA-256. Its resistance to attacks ensures robust protection, especially for valuable data. Being newer and continually researched, it offers future-proofing against emerging threats. Standardized by NIST, SHA-3 ensures compatibility and adherence to cryptographic standards, boosting confidence in its security. Its customizable output lengths provide flexibility, optimizing storage and integration. While not always more efficient than SHA-256, SHA-3's competitive performance makes it a secure choice for document verification systems.

C. IPFS is a peer-to-peer (P2P) distributed system for storing and accessing files. IPFS creates a hash of every single file stored in it. The files are, subsequently, accessed using these same hashes. Besides, it also features file versioning and duplicate file removal. Its uses are mostly for creating distributed file-sharing services. It is also widely used coupled with the Ethereum blockchain.

D. Consensus mechanism : Consensus mechanism is like a rulebook that ensures everyone in a blockchain network agrees on which transactions are valid and should be added to the blockchain.

1) Proof of Work :: PoW is not used in document verification systems due to its high energy consumption, slow confirmation times, scalability concerns, cost implications, and environmental impact. Other consensus mechanisms like PoS are more suitable for document verification.

2) Proof of Stake: Proof-of-stake (PoS) consensus mechanism, nodes play a crucial role in validating transactions and maintaining the integrity of the network. In a document verification system, it verifies document authenticity by validating transactions and adding valid documents to the blockchain, maintaining system integrity and trustworthiness.

VI. RESULTS

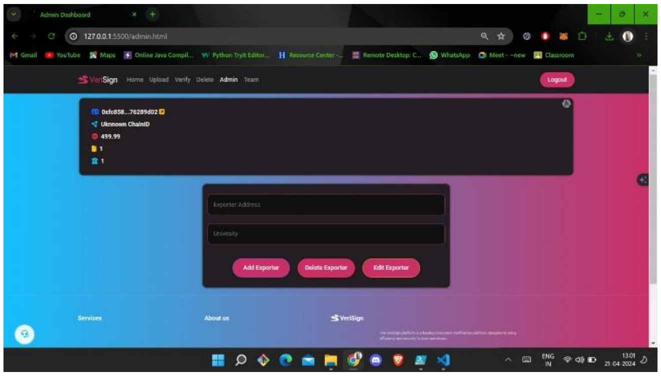
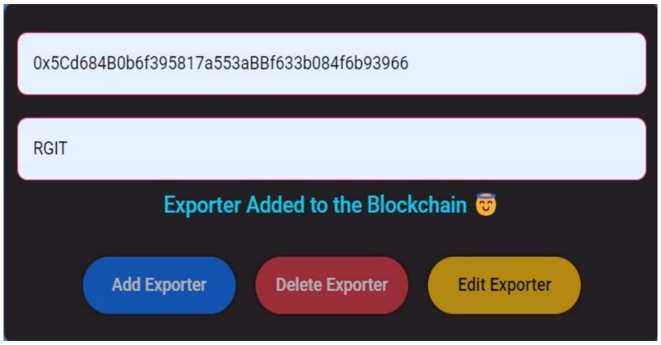


Fig. 2. Admin Page



0x5Cd684B0b6f395817a553aBBf633b084f6b93966

RGIT

Exporter Added to the Blockchain 😇

Fig. 3. Exporter Added

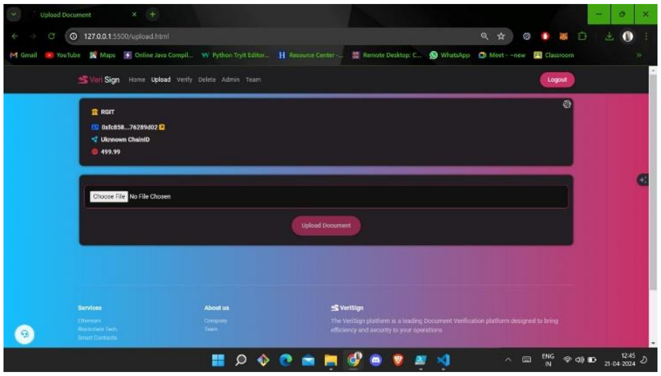
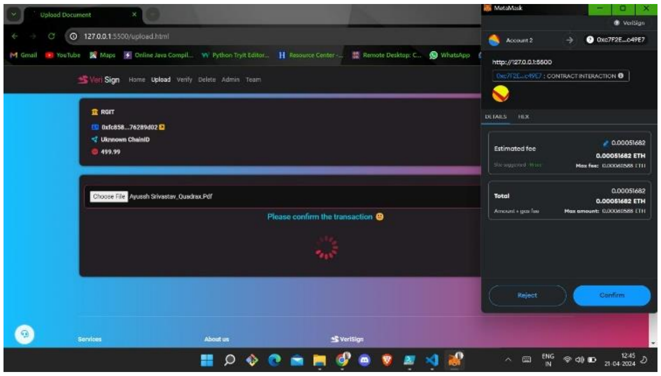


Fig. 4. Upload Page

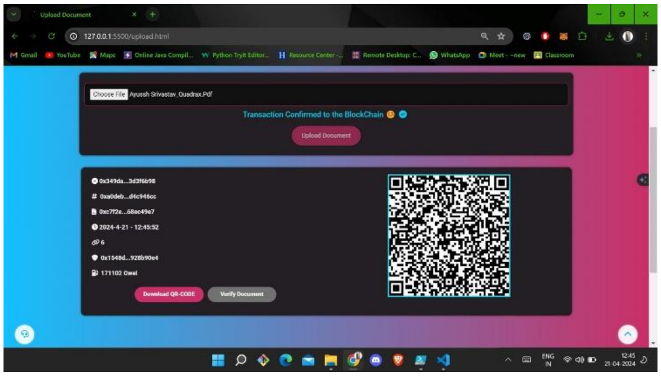


Please confirm the transaction

Estimated fee 0.00051682 0.00051682 ETH

Total 0.00051682 0.00051682 ETH

Fig. 5. Transaction Confirmation



127.0.0.1:5500/upload.html

Ayussh Srivastav_Quadrax.Pdf

Transaction Confirmed to the BlockChain

0x349da...3d3f6b98

0xa0deb...d4c946cc

0xc7f2e...68ec49e7

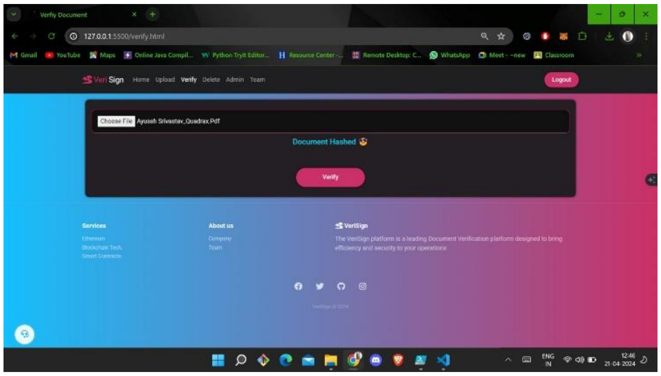
2024-4-21 - 12:45:52

6

0x1548d...928b90e4

171102 Gwei

Fig. 6. Transaction Confirmed

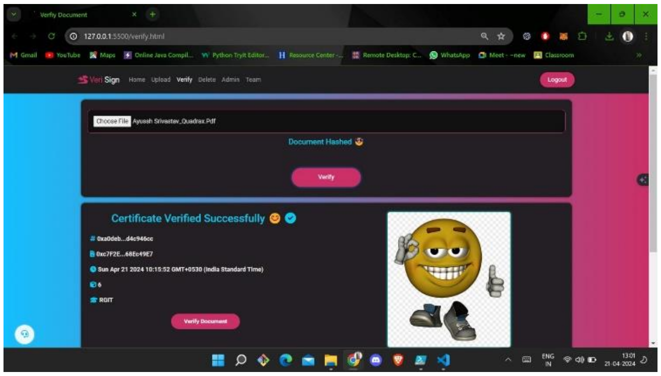


127.0.0.1:5500/verify.html

Ayussh Srivastav_Quadrax.Pdf

Document Hashed

Fig. 7. Certificate Hashed



127.0.0.1:5500/verify.html

Ayussh Srivastav_Quadrax.Pdf

Document Hashed

Certificate Verified Successfully

0xa0deb...d4c946cc

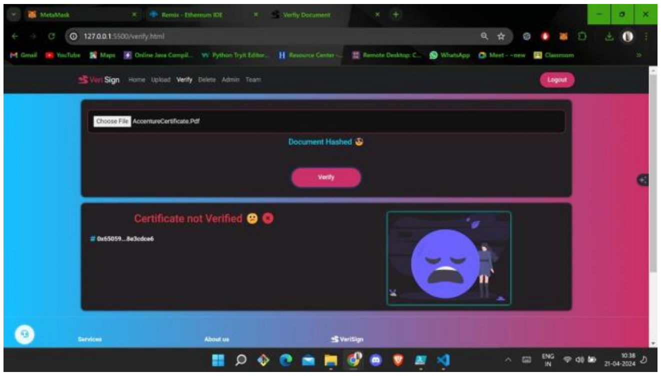
0xc7F2E...68Ec49E7

Sun Apr 21 2024 10:15:52 GMT+0530 (India Standard Time)

6

RGIT

Fig. 8. Certificate Verified



127.0.0.1:5500/verify.html

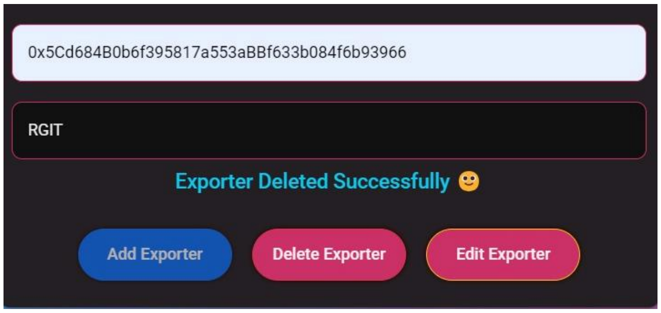
AccentureCertificate.Pdf

Document Hashed

Certificate not Verified

0x65059...8e3cdce6

Fig. 9. Certificate not verified

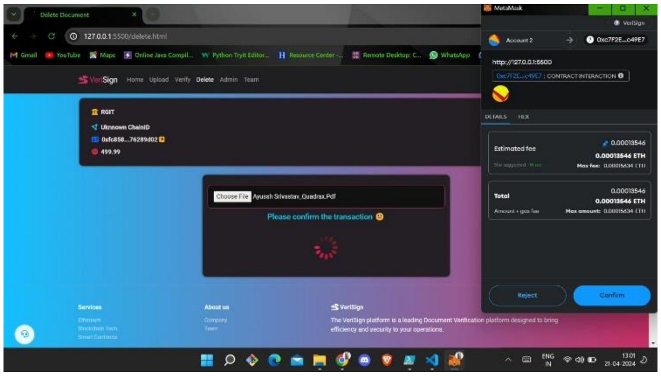


0x5Cd684B0b6f395817a553aBBf633b084f6b93966

RGIT

Exporter Deleted Successfully

Fig. 10. Exporter Deleted



127.0.0.1:5500/delete.html

RGIT

Uknnown ChainID

0xfc858...76289d02

499.99

Ayussh Srivastav_Quadrax.Pdf

Please confirm the transaction

Account 2

0xc7F2E...c49E7

http://127.0.0.1:5500

0xc7F2E...c49E7 : CONTRACT INTERACTION

Estimated fee 0.00013546 0.00013546 ETH

Total 0.00013546 0.00013546 ETH

Amount + gas fee

The VeriSign platform is a leading Document Verification platform designed to bring efficiency and security to your operations.

Fig. 11. Document Deleted

VII. CONCLUSION

The integration of blockchain with IPFS for document verification revolutionizes document management, verification, and storage. This combined system ensures high security and efficiency by leveraging blockchain's immutability and transparency along with IPFS's decentralized storage capabilities. Our automated system reduces manual verification efforts and minimizes the risk of certificate loss for students. Additionally, employing SHA3 hashing algorithm enhances data security, reducing tampering risks. The SHA3 hash function's proven safety ensures unique outputs for different inputs, preventing real information retrieval from hashes. Document retrieval is exclusively done through IPFS. Once a document's hash is recorded on the blockchain ledger, it becomes tamper- proof, ensuring its authenticity and integrity. This innova- tive approach addresses concerns like tampering, loss, and unauthorized access, making it suitable for various sectors requiring document integrity. This integration sets a new standard for document security and accessibility, promising a future of enhanced security, transparency, and user-friendliness in document management.

VIII. ACKNOWLEDGEMENT

We wish to express our sincere gratitude to Dr. Sanjay U. Bokade, Principal and Prof. S. P. Khachane, Head of Department of Computer Engineering at MCT's Rajiv Gandhi Institute of Technology, for providing us with the opportunity to work on our project, ”Blockchain based Document Verification System” This project would not have been possible without the guidance and encouragement of our project guide, Prof. S. P. Khachane. We would also like to thank our colleagues and friends who helped us in completing this project successfully.

IX. REFERENCES

[1] S. Leible, S. Schlager, M. Schubotz, and B Gipp, “A Review on Blockchain Technology and Blockchain Projects Fostering Open Science,” (2019), Front. Blockchain 2:16. doi: 10.3389/fbloc.2019.00016.

[2] A. Prashanth Joshi, M. Han, and Y. Wang, “A Survey on Security and Privacy Issues of Blockchain Technology,” (2018), Mathematical Foundations of Computing, Volume 1, Issue 2, pp. 121-147, doi: 10.3934/mfc.2018007.

[3] W. Chen, Z. Xu, S. Shi, Y. Zhao, and J. Zhao, “A Survey of Blockchain Applications in Different Domains,” (2018),
pp. 17-21, doi: https://doi.org/10.1145/3301403.3301407.

[4] Pascual, A., Marchini, K., Miller, S. (2018). 2018 Identity Fraud: Fraud Enters a New Era of Complexity. Retrieved from https://www.javelinstrategy.com/coverage-area/2018-identity-fraudfraud-enters-new-era-complexity

[5] Almuashi, M., Mohd Hashim, S., Mohamad, D., Alkawaz, M., Ali, A. (2015). Automated kinship verification and identification through human facial images: a survey. Multimedia Tools And Applications, 76(1), 265-307. doi: 10.1007/s11042-015-3007-5

[6] Chen, Z., Zhu, Y. (2017). Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging. In 2017 IEEE International Conference on AI Mobile Services (AIMS). Honolulu, HI: IEEE. Retrieved from https://ieeexplore.ieee.org/document/8027275/

[7] L. M. Arjomandi, G. Khadka, Z. Xiong and N. C. Karmakar, ”Document Verification: A Cloud-Based Computing Pattern Recognition Approach to Chipless RFID,” in IEEE Access, vol. 6, pp. 78007-78015, 2018, doi: 10.1109/ACCESS.2018.2884651.

[8] D. Yue, R. Li, Y. Zhang, W. Tian and C. Peng, ”Blockchain Based Data Integrity Verification in P2P Cloud Storage,” 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, Singapore, 2018, pp. 561-568, doi: 10.1109/PADSW.2018.8644863.