Securing College Documents Through Block chain In Cloud

Kedar Salunkhe[1], Ruturaj Landghule[2], Shubham Tarate[3], Tejas Beloskar[4], Dr.Priyanka Kadam[5]
[1,2,3,4]*Student, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India*
[5]*Professor, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India*

Abstract — Blockchain technology has grown from becoming an immutable database of transactions for crypto currencies to a programmable interactive environment for creating distributed reliable applications. While, blockchain technology has been used to solve numerous problems, to our knowledge none of the previous work centered on using blockchain to build a stable and immutable science data provenance management system that automatically verifies the provenance records. In this job, we use blockchain as a medium to promote trustworthy data provenance compilation, verification and management. According to numerous researches about one million graduates passing out each year, the diploma awarding authorities are seems to be corrupted for the security credentials of student records. Due to the lack of successful storage mechanism, incidents that allow the graduation certificate to be forged also get noticed. In order to address this problem digital certificate systems are adopted even though security problems are still remain. Blockchain is one of the most recent technologies that can be used for the data protection. The irreversible property of the block chain helps to solve the problem of certificate forgery.

Keywords— Block head formation, Blockchain creation, Terminal Key generation, Bilinear Pairing.

I INTRODUCTION

Graduation certificates and documents contain material private to the people and cannot be readily available to anyone. Hence, there is a high need for a system that can ensure that the material in such a document is original, which ensures that document has come from an authenticated source and is not false. In addition, the material in the paper should be secret so that it can only be accessed by designated individuals.

Blockchain technology is used to minimize the occurrence of certificate forgeries and ensure that the reliability, legitimacy and confidentiality of graduation certificates can be enhanced. Technologies occur in related fields, such as digital fingerprints, which are used in E-documents to provide verification, credibility, and nonrepudiation. However, for the specifications of an E-qualification certificate, it has crucial security gaps and missed functions: for example, it uses the keys to validate the alteration of the record, but doesn't initiate the validation of the public key certificates' status immediately.

This can result in a forgery being accepted if the key has been compromised. Furthermore, also the signer's public key credential has been authenticated, but the signed paper itself hasn't. In our case with an e-qualification certificate, the signed form itself is also a certificate, and could have a legitimate duration (e.g. the problem we are grappling with is a (certificate) matter, hence, a simple digital signature of the document alone doesn't fix the problem.

Digital Certificate Digital certificate which adopts digital signature technology, presents to the user by the authority to validate the user himself in the digital fields used to confirm a user's identity and access authorization to the network resources. Digital certificates can be extended to e-commerce operations on the internet and e-government activities, whose domain get interested in application of identity verification and data protection, like conventional financial, manufacturing, retail online purchases, public services etc.

Blockchain is the fundamental era underlying the rising crypto currencies along with Bitcoin. the key gain of blockchain is extensively taken into consideration to be decentralization, and it is able to assist set up disintermediary peer-to-peer (P2P) transactions, coordination, and cooperation in distributed systems without mutual believe and centralized control amongst character nodes, based on such strategies as information encryption, time-

stamping, disbursed consensus algorithms, and monetary incentive mechanisms. As such, blockchain can offer a unique solution to the longstanding issues of high operation expenses, low performance and potential protection risks of statistics garage in conventional centralized structures.

This literature survey article's second section is devoted to a literature review that assesses prior research, and part three makes recommendations for more study.

II RELATED WORKS

[1] Suprateek Sarker et al describe corruption, whether systemic or petty, and related fraud still remains in the global shipping industry, but the mechanisms to effectively fight it are emerging. Historically, anti- corruption bodies and organizations have relied upon policies and legal framework to battle corruption. However, with digital technologies in general and blockchain in particular, anti-corruption actors have new resource at their disposal. We see how blockchain can fight both process and document-related corruption on a global scale across continents and economies, bringing to attention the misuse of funds for improper gift giving, kick backs, or inappropriate social activities, in the same way that an enterprise resource planning (ERP) system provided transparency for internal business procsses and activities. In particular, institutional entrepreneurs, whether individuals or organizations, have drawn upon these new emerging resources such as blockchain and social enablers such as policies and laws in their quest to change the world..

[2] S. CHOUDAIAH et al introduced aimed to provide a cost-effective remedy to the document management difficulties connected with Colombia's embargo procedure by implementing the solution. Data scalability, availability, and integrity are all improved using blockchain technology, which is a new technology that allows for transparency at the transaction level. Instead of using a big database stored in an extremely powerful server, the solution provided allows users to access their data through a point-to-point network in which all participants are responsible for controlling and supervising the data

[3] Sakshi Jha et al proposes a framework for developing a secure, tamper-resistant paradigm for keeping research records in a distributed file system with no single point of control. The metadata information collected from the distributed file system is likewise stored on the blockchain. The blockchain provides an indelible record of events since it is a distributed ledger system that records all transactions and cannot be changed or altered. As a result, malicious alterations to the blockchain's metadata information are prevented.

[4] P. Kang et al explain the combination of blockchain technology and NDN network involved in this article is applied to the fields of le forwarding, and data storage and protection and innovatively solves the problems of low performance and forwarding efficiency of traditional forwarding networks, difficulty in tracing the history of le transfer and document authenticity. Challenging to guarantee and other issues, the two technologies play a complementary role in this scenario. routing node is not responsible for the acquired data, it is also considered unsafe for confidential content data to be arbitrarily forwarded and received. Therefore, this paper uses the characteristics of smart contract rules to make judgments after the NDN network forwarding strategy. On the one hand, it limits the scope of le forwarding that is not allowed, and on the other hand, it also ensures that confidential les are not arbitrarily obtained.

[5] Yeboah-Ofori et al describe blockchain technology can bolster cloud security. We explored how decentralization, immutability, and transparency principles can enhance data privacy and integrity in the cloud. Our study demonstrated that integrating AES encryption, cloud storage, and Ethereum smart contracts could preserve the confidentiality and integrity of data. The encouraging results highlight that AES encryption and decryption procedures efficiently secure the data, while AWS S3 provides a robust cloud storage environment. Simultaneously, our Ethereum smart contract provides a transparent and unchangeable record of data access and updates. However, some limitations need acknowledgment. The seamless integration of AWS, Ethereum, and AES encryption poses inherent challenges, and vulnerabilities in these platforms may compromise the system's security.

[6] Ms. Sanskriti Punde et al explain in this study has found that there are a lot of institutes that are not able to manage documents in an effective manner and secure manner so we are proposing a solution that will help them to solve this issue. With the help of this application, the institute or department will be able to manage applications such as leave applications, approvals, and circulars effectively and will be able

to keep documents secure from various cyber security threats. DocMan is a secure, scalable, and easy-to use web application which is customizable and can be used effectively to manage the department's application process digitally at high speeds and transparency. We are providing a tracking feature to help understand where the application is right now and what its status is.

[7] Maria José Sousa et al introduced this study provides insights into the dimensions of Blockchain technology that experts find of higher or lower importance, shedding light on the underlying reasons. Notably, issues like regulatory risks, data ownership, and data availability emerged as prevalent concerns among respondents. By conducting a literature review and employing a specific methodology, this research collected and analyzed feedback from 173 specialists, aiming to unravel the advantages and drawbacks of implementing blockchain technology in public organizations. The results offer valuable insights for researchers and practitioners, helping them understand the varying levels of complexity associated with different dimensions of block chain when applied in public sector contexts.

[8] Olivier Rikken et al narrate DAOs provide a new form of governance, and there is limited knowledge about how DAOs should be designed to be viable in the long-term. Providing insights into the effect of governance elements' impact on the long-term viability of DAOs helps pol icy-makers and decision-makers in choosing the right setup of these elements when they want to use DAOs to achieve higher levels of transparency, inclusiveness, and accountability. Based on our in-depth analysis of 220 out of 6,000þ DAOs, we find that a number of governance elements can influence the long-term viability of DAOs.

[9] Mohammad Mustafa Ibrahimya et al describe blockchains, including their subset technologies, such as smart contracts, Web 3.0, and DAOs, have the potential to enable governments to combat corruption and improve transparency by minimizing physical interactions between citizens and public servants. In our research, we focus on existing blockchain-based models, examining their fundamental components and characteristics. We also delve into the role of token economies in eliminating intermediaries and discuss the effects of blockchains and their subset technologies, along with multifactor SSI authentication, within the public sector. Through an exhaustive systematic review of the literature that includes 242 peer-reviewed journals, proceedings, and book chapters published between 2012 and 2023, we identify seven blockchain-based governance models that emphasize improving governance and transparency in the public sector.

[10] Jaymin S Chandaria et al., The article discusses the potential of implementing a blockchain storage project for vehicle documents in the transportation sector. The use of blockchain technology is expected to offer benefits such as enhanced security, privacy, and streamlined verification processes. The inherent immutability and tamper resistance of blockchain technology ensure the integrity of vehicle documents, reducing the risk of fraud and identity theft.

[11] Gauri Yogeshwar Wankhade et al introduced our software offers a promising solution to the persistent hurdles encountered by the legal sector in managing documents through decentralized peer to peer data storage. Digital signatures are employed to validate the authenticity of uploaded data, with each sender assuming full accountability for the content they upload. Utilizing encryption enhances the security measures of our system. The use of randomly generated encryption keys guarantees that each file possesses a unique key, significantly diminishing the vulnerability to attacks.

[12] Prathmesh Doni et al explain that research culminated in the development of "Secure Cloud File Sharing System," a novel blockchain-based file sharing system. This innovative platform addresses the critical concerns of data privacy and control in today's digital landscape. This system leverages the power of Ethereum blockchain and IPFS to create a decentralized architecture that prioritizes data security. Encryption safeguards user data confidentiality, while the immutability of the blockchain ensures the integrity of file-sharing activities.

[13] Yash Ashok Gokakkar et al introduced a novel decentralized storage system that leverages blockchain technology to address the shortcomings of centralized storage systems. The implementation, in the form of a user-friendly website developed with React.js and tailwindcss, coupled with a robust backend using MySQL and IPFS, provides a secure and efficient platform for document management. The key features of the system, such as secure document storage on IPFS, user-centric document management, and blockchain-based access control, contribute to enhanced security, transparency, and accountability in document sharing.

III. SUMMARY OF RELATED WORK

Research Paper Title	Focus Area	Identified Gaps
1.Improving Security: Blockchain-Based IoT Solutions for Healthcare	IoT & Healthcare Security	Limited exploration of interoperability between different IoT devices
2.An Implementation of Secure Storage Using Blockchain Technology on Cloud Environment	Cloud Storage Security	Lacks scalability analysis and real-world performance benchmarks
3.Blockchain-Based Trust Management in Cloud Computing Systems: A Taxonomy, Review, and Future Directions	Cloud Computing & Trust Management	Needs more empirical studies to validate the proposed taxonomy.
4.Blockchain-Based Data Security and Access Control System Using Cloud	Data Security & Access Control in Cloud	Does not address the potential performance overhead and latency issues.
5. Unlocking the Power of Blockchain in Education: An Overview of Innovations and Outcomes	Blockchain in Education	Limited empirical data on the long-term impacts and adoption challenges in the educational sector
6. Implementing Blockchain-Assisted Public Key Encryption	Encryption & Blockchain	Needs further exploration of the integration challenges with existing cryptographic systems.
7. The Key Security Management Scheme of Cloud Storage Based on Blockchain and Digital Twins	Cloud Security & Digital Twins	Limited real-world applicability and lack of performance evaluations in diverse cloud environments.
8.Cloud Computing Access Control Using Blockchain	Cloud Access Control	Does not sufficiently address the scalability and privacy issues in large-scale cloud environments.
9. Blockchain Document Forwarding and Proof Method Based on NDN Network	Document Management & Blockchain	Lack of focus on potential network latency and bandwidth consumption issues.
10. Blockchain-Enabled Framework for Transparent Land Lease and Mortgage Management	Land Management & Blockchain	Limited discussion on regulatory compliance and integration with existing legal frameworks.

IV. PROPOSED SYSTEM

The proposed system for securing college documents through blockchain in the cloud aims to enhance the security, integrity, and authenticity of academic records. The system begins with the user (student or administrator) submitting a document, such as an academic certificate or transcript. The document is then converted into byte data, preparing it for digital processing. This byte data is used to form the body of a block in the blockchain, which is a decentralized and immutable ledger. Along with the block body, a block head is created, which contains metadata such as timestamps and references to the previous block, ensuring the chronological and linked nature of the blockchain.

Once the block is fully formed, it is added to the blockchain, securing the document in a tamper-proof, distributed system. A terminal key is generated to enhance the document's security, which plays a crucial role in encryption and verification. Additionally, the system employs bilinear pairing, a cryptographic technique, to further secure the document and ensure that it remains unaltered throughout its lifecycle. This process guarantees the integrity of the document, confirming that it has not been tampered with and is authentic.

After these cryptographic measures are applied, the system verifies the integrity of the document, ensuring its authenticity. A final report is generated,

which confirms the successful encryption, verification, and storage of the document on the blockchain. This report acts as a proof of authenticity that can be used by students, administrators, or third parties for verification purposes. By leveraging blockchain technology and cryptographic methods, the proposed system offers a secure, transparent, and efficient way to manage and safeguard college documents in the cloud.

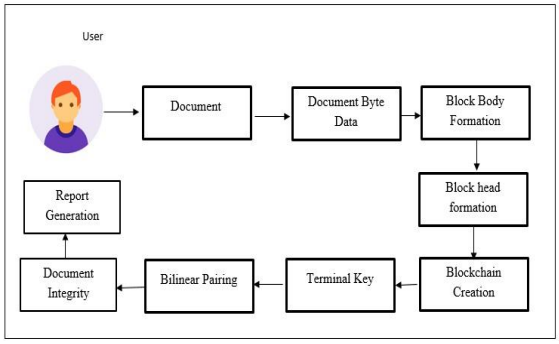

Fig. System Architecture

1.User (Student or Administrator): The user begins the process by submitting a document, which can be an academic record, certification, or any other college-related document.

2. Document: The submitted document is taken as input, which will go through a process to ensure its security and integrity.

3. Document Byte Data: The document is converted into byte data, representing it in a digital format that can be processed for blockchain storage.

4. Block Body Formation: The byte data from the document is used to create the body of a block, which is a crucial element in the blockchain. This block will hold the actual document data.

5. Block Head Formation: Along with the block body, a block head is formed, which typically includes metadata such as a timestamp, previous block hash, and other necessary information required to link it with other blocks in the blockchain.

6. Blockchain Creation: The newly created block (with both body and head) is then added to the existing blockchain. Each block is linked with the previous one, ensuring an immutable, secure, and tamper-proof chain of records.

7. Terminal Key: A terminal key is generated to ensure the security of the document and to verify its authenticity. The key acts as a security mechanism that helps in encryption and validation of the data.

8. Bilinear Pairing: Bilinear pairing is applied as a cryptographic technique. It is used for encryption and verification of the document, ensuring its integrity and preventing unauthorized alterations.

9. Document Integrity: This step ensures that the integrity of the document is preserved. Using cryptographic methods (like bilinear pairing), the system checks whether the document remains unaltered and maintains its authenticity.

10. Report Generation: Finally, a report is generated after all processes are complete, confirming the document's integrity, authenticity, and successful addition to the blockchain. This report serves as proof for verification purposes.

V .CONCLUSION AND FUTURE SCOPE

Document Storage is one of the applications of blockchain. There are many ways to store it using blockchain. But what matters here is the size of the document. The data in the block can only be a string or anything which is in kilobytes. As the size of the documents or files will be in megabytes, it is not logically correct to store the documents directly in the blocks. Hence, the documents can be stored in an off-chain storage systems like the local machine or any distributed file system. In the present work, a blockchain network is created for storing the documents. Incidents that allow the graduation certificate to be falsified are also discovered owing to the unavailability of a competent storage medium. Despite the fact that security issues still exist, digital accreditation solutions have been used to solve this issue. One of the most existing technology that may be utilized for information security is blockchain. The block chain's inescapable nature aids in the prevention of document counterfeiting.

For the purpose of future research directions this Project can be extends with the below mentioned points

✓ Future research might focus on integrating the Educational Certificate Management Using Blockchain technique into the mobile application

design, allowing any smartphone user to access their certificates securely.

REFERENCES

[1] Suprateek Sarker, Stefan Henningsson, Thomas Jensen & Jonas Hedman (2021) The Use Of Blockchain As A Resource For Combating Corruption In Global Shipping: An Interpretive Case Study, Journal of Management Information Systems, 38:2, 338-373, DOI: 10.1080/07421222.2021.1912919

[2] S. Choudaiah, u. Chandraselhar et al., "block chain based document management system," Vol 12, Issue 08, August/2021 ISSN NO:0377-9254.

[3] Sakshi Jha, Govind Dhingra, Gagan Mittal, Harsh Vardan, "Secured Document Storing Using Blockchain," 2022 IJRTI | Volume 7, Issue 5 | ISSN: 2456-3315

[4] P. Kang, Y. Wenzhong and T. Ding, "Blockchain Document Forwarding and Proof Method Based on NDN Network," in IEEE Access, vol. 10, pp. 75312-75322, 2022, doi: 10.1109/ACCESS.2022.3178992.

[5] Yeboah-Ofori, Abel ORCID: https://orcid.org/0000-0001-8055-9274, Sadat, Sayed Kashif and Darvishi, Iman (2023) Blockchain Security Encryption to Preserve Data Privacy and Integrity in Cloud Environment. In: EEE 2023 10th International Conference on Future Internet of Things and Cloud (FICloud), 14-16 August 2023, Marrakesh, Morocco.

[6] Ms. Sanskriti Punde, Mr. Kartikey Yadav, Mr. Chakradhar Ghute, Ms. Namrata Shinde, "Document Management System using Blockchain," Volume 3, Issue 13, May 2023, DOI: 10.48175/568

[7] Maria José Sousa (2023) Blockchain as a driver for transformations in the public sector, Policy Design and Practice, 6:4, 415-432, DOI: 10.1080/25741292.2023.2267864

[8] Olivier Rikken, Marijn Janssen & Zenlin Kwee (2023) Governance impacts of blockchain-based decentralized autonomous organizations: an empirical analysis, Policy Design and Practice, 6:4, 465-487, DOI: 10.1080/25741292.2023.2270220

[9] Mohammad Mustafa Ibrahimya, Alex Nortab,Peeter Normak , "Blockchain-based governance models supporting corruption-transparency: A systematic literature review,"https://doi.org/10.1016/j.bcra.2023.100186

[10] Jaymin S Chandaria, Keerthi Sai Adithiya, Harsh Mehta, Sterlin Minish T N, "MyDeed – A Blockchain Based Storage Solution for Official Documents," International Journal of Research Publication and Reviews, Vol 5, no 1, pp 1600-1612, January 2024

[11] Gauri Yogeshwar Wankhade, Shantanu Rawade, Harshal Lokhande, Anish Bhalerao, "Blockchain-Based eVault for Legal Documents," ISSN: 2454-132X ,Impact Factor: 6.078 (Volume 10, Issue 1 - V10I1-1289), Available online at: https://www.ijariit.com

[12] Prathmesh Doni, Kaustubh Gade, Yashraj Gaikwad, Swapnil Badal, " Blockchain Based Secure Cloud File Sharing System, " International Journal of Research Publication and Reviews, Vol (5), Issue (5), May (2024).

[13] Yash Ashok Gokakkar, Shriniket Kulkarni, Ashutosh Raj Gupta, Suyash Dighe, Viraj Sonagra, "Blockchain based Decentralized Storage System," IJRASET, ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 12 Issue III Mar 2024- Available at www.ijraset.com