JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DEVELOPING A BLOCKCHAIN BASED EVAULT FOR LEGAL RECORDS

[1]Swetha R, [2] Viswanath V, [3]Vijay G, [4]Sanjay S

[1]Assistant Professor, Department of Computer Science and Engineering,

[2,3,4] UG Students, Department of Computer Science and Engineering,

Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College

Abstract: This project focuses on developing a blockchain-based eVault tailored for the secure storage and management of legal records. In response to the increasing demand for trustworthy digital record-keeping solutions, the proposed eVault leverages blockchain technology to ensure data integrity, authenticity, and accessibility. Utilizing smart contracts and cryptographic methods, the system automates verification, access control, and auditing processes, aiming to streamline operations and enhance security. The eVault's decentralized architecture and immutable ledger provide a robust framework for storing, managing, and sharing legal records while adhering to compliance standards and legal requirements. Utilizing blockchain's audit trail capabilities to provide a transparent and auditable record of all transactions and modifications to legal records, ensuring accountability and compliance with regulatory requirements.

IndexTerms-LegalRecords,BlockchainTechnology,eVault,Security,Transparency,Compliance,Efficiency, Decentralization

I. INTRODUCTION

The legal sector is changing quickly in the current digital era, depending more and more on electronic documents to improve accessibility and streamline procedures. But maintaining these documents' accessibility, security, and integrity continues to be a difficult task. By utilizing blockchain technology, the "eVault for Legal Records using Blockchain" initiative seeks to resolve these problems. Blockchain is a popular technology for securely maintaining sensitive legal documents because of its decentralized and irreversible record. By placing a strong emphasis on efficiency, security, and openness while adhering to strict legal and regulatory requirements, this effort aims to revolutionize legal document management. The project intends to transform the way legal professionals, clients, and authorities interact with and protect important documentation by creating a blockchain-based eVault for legal records. This would ultimately simplify legal procedures going forward.

II. LITERATURE SURVEY:

In [1], Verma and Ashwin introduced NyaYa, an Electronic Law (EL) management system using blockchain. It features phases such as stakeholder and case registration, updates across agencies, and settlement via smart contracts. Simulation shows NyaYa surpasses traditional EL storage in mining cost, query time, and trust probability, enhancing digital evidence management efficiency securely.

The authors of [2] The article by Victoria L. Lemieux examines Blockchain, a revolutionary distributed ledger technology utilized in industries such as finance, real estate, and healthcare. Through transaction blocks that are cryptographically chained, it guarantees transparent and safe recordkeeping. Public-private key pairs are used in asset token transfers in blockchain transactions. Although there are benefits in terms of identifying changes and improving privacy, issues like scalability and legal ramifications still exist.

The authors of [3] A blockchain-based system was introduced by Maisha Afrida Tasnim, Abdullah Al Omar, Mohammad Shahriar Rahman, and Md Zakirul Alam Bhuiyan for the safe management and archiving of criminal data. In an effort to stop manipulation and improve data security, it incorporates records into blockchain technology and uses peer-to-peer cloud networks for decentralization. Digital signatures, blockchain technology, and encryption enable law enforcement and other authorized users to effectively maintain and access documents while guaranteeing their legitimacy and integrity.

In [4]. Kamshad Mohsin explores blockchain's intersection with legal frameworks, focusing on contracts, intellectual property, and personal data protection. It discusses both enabling and prohibitive legislation, highlighting Blockchain Law's emergence and the necessity to align technology with evolving global legal standards. Regulatory sandboxes' role in fostering blockchain innovation is also examined.

III. RESEARCH METHOD:

There are several important issues that need to be resolved in order to establish a blockchain-based eVault for legal data. First and foremost, preserving the authenticity and integrity of legal data is a serious concern because conventional digital storage techniques are susceptible to manipulation and illegal access. Given the hazards associated with centralized databases that are vulnerable to insider threats and cyberattacks, security is still of the utmost importance. Furthermore, inefficient data retrieval and accessibility in many existing systems is made worse by cumbersome authentication procedures and ineffective sharing protocols. Complying with various legal standards adds to the complexity, necessitating observance of strict data protection regulations and cross-jurisdictional evidential requirements. Another obstacle is user authorization and authentication, which calls for strong methods to safely handle and authenticate user identities.

.

Another obstacle is user authorization and authentication, which calls for strong methods to safely handle and authenticate user identities. To enable smooth operation under current regulatory frameworks, technological obstacles including scalability concerns and high transaction costs associated with blockchain integration must also be addressed. Designing an eVault system based on blockchain technology that improves security, transparency, and efficiency in the efficient management of legal records requires a thorough understanding of these complex issues.

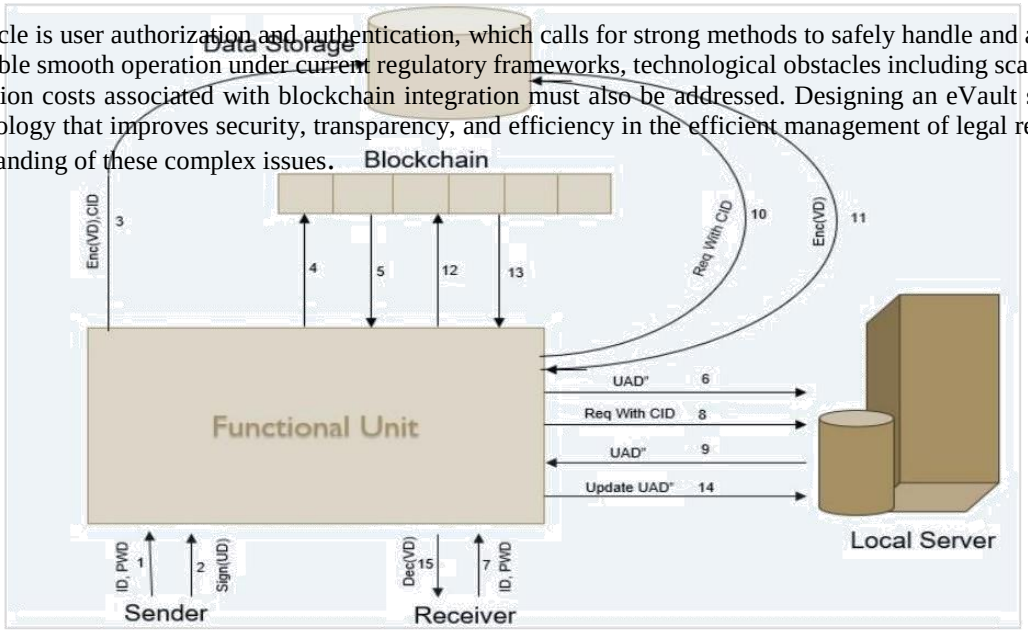


Figure1. Block Diagram

Security and Privacy Considerations:

When creating an eVault for legal data based on blockchain technology, security and privacy are of the highest priority. Encryption is essential for maintaining data secrecy. It uses strong symmetric and asymmetric encryption methods to protect private data kept in the eVault. Digital signatures, role-based access controls (RBAC), and multi-factor authentication (MFA) are used as access control measures to make sure that only authorized users, like law enforcement and legal experts, can access and handle legal records. The unchangeable ledger of the blockchain ensures the accuracy and verifiability of data, offering an impenetrable archive that amplifies accountability and transparency.

Zero-knowledge proofs and pseudonymous transactions are used to improve privacy, and data minimization and anonymization techniques are used to preserve compliance with data protection laws like the GDPR. Decentralized storage networks reduce the hazards associated with centralized data repositories by improving data redundancy and resilience. Proactive vulnerability detection and mitigation are ensured by regular security audits, penetration tests, and continuous monitoring, which are supported by strong incident response and disaster recovery strategies. The blockchain-based eVault seeks to transform how legal records are safely maintained and accessed in accordance with changing legal and regulatory standards by solving these extensive security and privacy concerns.

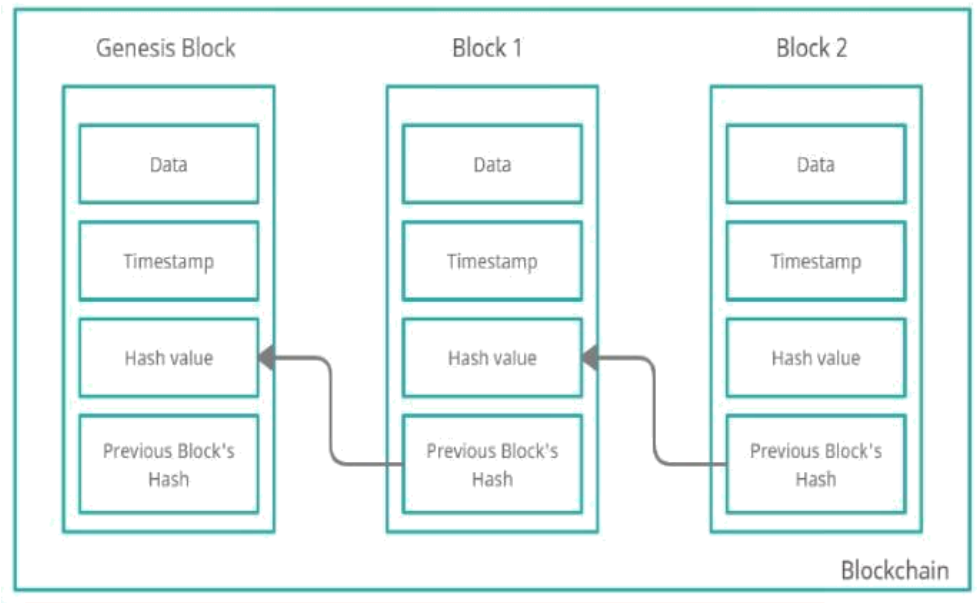


Figure 2.Proposed System

IMPLEMENTATION:

An eVault for legal records built on blockchain technology transforms data security and accessibility in the legal sector by guaranteeing transparent record management and tamper-proof storage."

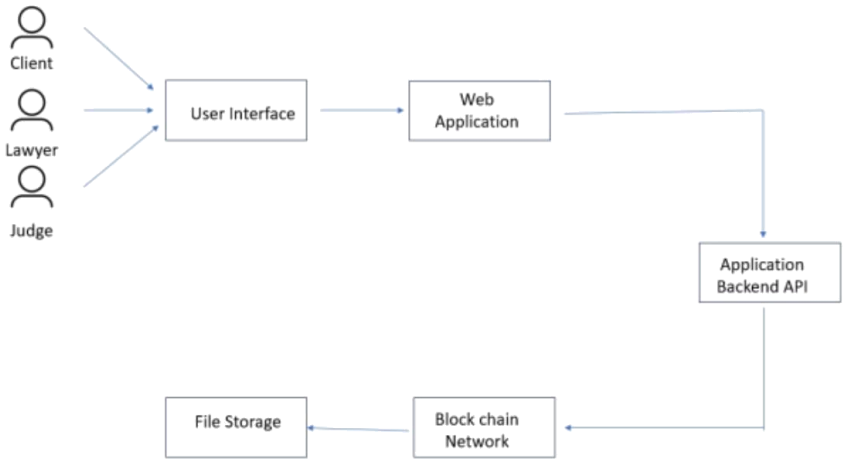


Figure 4.Model Diagram

Client/Lawyer/Judge:The end users or legal professionals who engage with the system are the client, lawyer, or judge. They may be people or organizations engaged in court proceedings, including Judges supervising legal matters, attorneys offering legal assistance, and people in need of legal services.

User Interface: The graphical or user-friendly interface that the client, attorney, or judge uses to communicate with the system is this component. It offers a platform where users can enter information, get information, and carry out different legal-related tasks.

Web Application:The program that runs on a web server and displays the user interface is known as a web application. It manages user authentication, responds to user queries, and interacts with the application backend API to carry out a number of legal services-related tasks, including communication, document management, case tracking, and more.

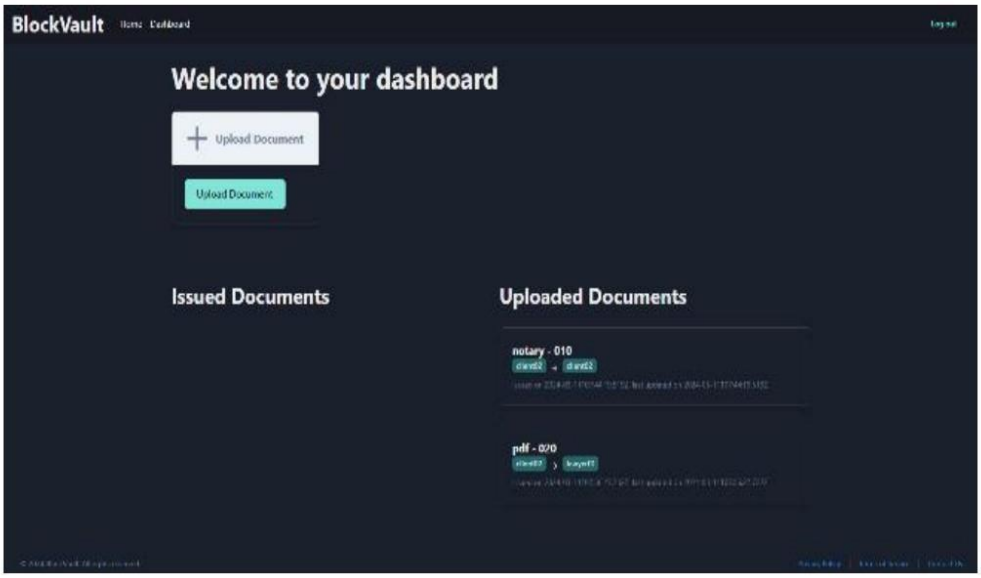
Application Backend API:This section of the system is in charge of communicating with other parts and handling requests from the online application. It operates a number of tasks, including data retrieval and storage, business logic execution, and data storage interface with the blockchain network.

Blockchain Network:A kind of distributed and decentralized ledger technology is the blockchain network. It is employed for data storage that is both safe and impenetrable. Within this architectural design, Contracts, legal documents, and other private information are kept there. Because blockchain technology guarantees data integrity and immutability, it can be used in legal contexts where data security and authenticity are essential.

File Storage:This part is an integrated storage system that is part of the blockchain network. It is employed for the long-term preservation of case files, legal papers, and additional files. Cryptographically encrypted files kept on the blockchain are easily retrievable when needed.

Algorithm:File Encryption Algorithm: To secure file content, use symmetric and asymmetric encryption techniques like AES and RSA. SHA-256 is one of the hash functions used to create file checksums. Role-based access control (RBAC) algorithms are used to manage user permissions through access control algorithms. Fine-grained access control using attribute-based access control techniques. Accord Algorithm: This algorithm consists of: Depending on the blockchain platform selected, blockchain consensus can be achieved by Proof-of-Work or Proof-of-Stake. Merkle trees are an effective way to represent and verify the integrity of data on the blockchain, according to the Blockchain Data Management Algorithm. Data compression techniques, like zlib, are used to maximize storage effectiveness. File Chunking Algorithm: To facilitate effective storage and retrieval, files are first divided into smaller chunks before encryption. algorithms for determining chunk boundaries, such as Rabin's fingerprinting algorithm. Decentralized Storage Algorithms: The distributed storage protocols of Filecoin or the Interplanetary File System (IPFS)fully connected layers are responsible for classifying color types using a collection of visual features previously extracted from
convolutional layers.

The Ganache-built blockchain-based legal record system functions similarly to an extremely safe digital filing cabinet reserved for the storage of crucial legal papers. Think of it as a high-tech safe deposit box where judges, attorneys, and clients may securely store and retrieve court documents without fear of them being altered or misplaced. This system makes use of private keys that function as digital locks, guaranteeing that only authorized users can access the saved documents, are created using specialized tools like MetaMask and Ganache. It functions similarly to having a virtual safe deposit box of your own where all of your legal documents are kept secure. With the help of this system, every document kept in the digital vault is safeguarded by cutting-edge encryption technology, ensuring that only authorized users may access or alter them.

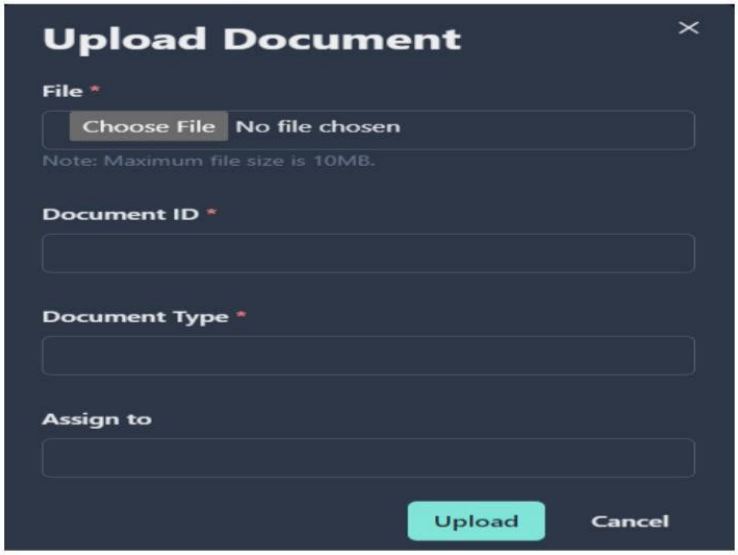


Additionally, the use of a blockchain-based legal record system improves the legal industry's data transparency and integrity. Append-only feeds and sophisticated encryption prevent unauthorized access to or alteration of legal documents kept on a decentralized ledger. Smart contract technology streamlines administrative duties and transactional work for attorneys, cutting down on hours of manual labor and related expenses. This system transforms the way legal documents are managed by providing a safe and effective.

Blockchain technology offers improved security, transparency, and efficiency, revolutionizing the handling of legal

documents. Due to robust access controls and encryption, legal papers are safeguarded by the intrinsic security characteristics of blockchain, shielding sensitive information from alteration or unwanted access. By establishing a Blockchain, a decentralized and unchangeable ledger, promotes confidence and transparency in document exchanges by enabling the integrity and authenticity of each document to be verified and validated. In addition to improving accountability, this transparency boosts trust in the legal system among those involved and guarantees the dependability of document management procedures.

Additionally, blockchain technology reduces costs and improves operational efficiency by doing away with the necessity for third parties to act as middlemen in the handling of legal documents. Because blockchain technology is decentralized, all players will have equal access to information while data security and integrity are preserved. The use of granular access controls, businesses can safely distribute documents to those who are allowed, reducing the possibility of data breaches or illegal access. Blockchain's auditability and monitoring characteristics let businesses keep an open record of all document-related operations, complying with internal and regulatory regulations and efficiently optimizing document management procedures.



There are various procedures involved in uploading documents to a blockchain network. Initially, a file input window allows the user to choose the files they wish to upload. After processing the chosen files, the metadata is taken out. The files themselves are hashed and stored on the blockchain along with this metadata. The hash functions as a distinct identification for the document, verifying its validity and existence without disclosing the information itself. The user uses their private, digital signature—which is only known to them—to guarantee security while signing the document. Anyone can confirm with this signature that the document was really delivered by the correct individual. The route from sender to receiver is recorded in an audit log that is kept on the blockchain, generating a secure system.

RESULT:

There are many benefits to employing blockchain technology to implement an eVault for legal records. The decentralized and unchangeable ledger of blockchain technology guarantees the accuracy of data, protecting it from manipulation or unwanted access. Blockchain's use of cryptographic algorithms improves security by protecting the privacy of critical legal data. All stakeholders have the capacity to confirm the authenticity of records and follow their history thanks to the inherent properties of transparency and traceability. Using smart contracts to automate jobs and digitize record-keeping procedures, firms can increase productivity, cut down on administrative costs, and simplify operations. Additionally, because blockchain-based eVaults provide a safe and auditable record-keeping solution, they make regulatory compliance easier. oversight. Blockchain's worldwide reach facilitates easy access to legal documents from any location, fostering efficiency and cooperation amongst geographically separated teams. Although the benefits seem promising, careful consideration of elements like interoperability, data protection, and regulatory compliance is necessary for a successful implementation. However, blockchain-based eVaults have the ability to completely transform the handling of legal records, providing a reliable and long-lasting option for businesses looking to update existing procedures.

CONCLUSION:

Our platform provides decentralized peer-to-peer data storage, which presents a possible answer to the ongoing challenges faced by the legal industry in handling documents. Each sender is fully responsible for the content they submit, and digital signatures are used to verify the validity of the data. Encryption strengthens our system's security protocols. By guaranteeing that every file has a unique key, randomly generated encryption keys greatly reduce the vulnerability to assaults. The blockchain and data storage components of the cloud are not available to individual users. This thorough strategy addresses probable software/hardware failures and guarantees data confidentiality and precise provenance monitoring. Our platform ensures that papers stored within the system are secure by utilizing the immutability of blockchain technology and decentralizing control.

REFERENCES:

[1] Verma, A., Bhattacharya, P., Saraswat, D., & Tanwar, S. (2021). NyaYa: Blockchain-based electronic law record management scheme for judicial investigations. Journal of Information Security and Applications, 63, 103025.

[2] Lemieux, V. L. (2021). Blockchain and Recordkeeping. Computers, 10(11), 135.

[3]Tasnim, M. A., Omar, A. A., Rahman, M. S., & Bhuiyan, M. Z. A. (2018). Crab: Blockchain based criminal record management system. In Security, Privacy, and Anonymity in Computation, Communication, and Storage: 11th International Conference and Satellite Workshops, SpaCCS 2018, Melbourne, NSW, Australia, December 11-13, 2018, Proceedings 11 (pp. 294-303). Springer International Publishing.

[4] Ali, S., Wang, G., White, B., & Cottrell, R. L. (2018, August). A blockchain-based decentralized data storage and access framework for pinger. In 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE) (pp. 1303-1308). IEEE

[5] Malomo, O., Rawat, D., & Garuba, M. (2020). Security through block vault in a blockchain enabled federated cloud framework. Applied Network Science, 5(1), 1-18.

[6] Storer, M. W., Greenan, K., Long, D. D., & Miller, E. L. (2008, October). Secure data deduplication. In Proceedings of the 4th ACM international workshop on Storage security and survivability (pp. 1- 10).

[7] Batista, D., Mangeth, A. L., Frajhof, I., Alves, P. H., Nasser, R., Robichez, G., ... & Miranda, F. P. D. (2023). Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. Journal of Risk and Financial Management, 16(8), 360

[8] Mohsin, K. (2021). Blockchain Law: A New Beginning. Available at SSRN 3840220.

[9]Lemieux, V., Hofman, D., Batista, D., & Joo, A. (2019). Blockchain technology & recordkeeping. ARMA International Educational Foundation

[10] G. Li and H. Sato, “A privacy-preserving and fully decentralized storage and sharing system on the blockchain,” in Proceedings of the 2019 IEEE 43rd Annual Computer Software and Applications Conference, pp. 694–699, IEEE, Milwaukee, WI, USA, July 2019.

[11] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

[12] Wood, G. (2014). Ethereum: A secure decentralized generalized transaction ledger. Ethereum Project Yellow Paper, 151, 1-32.

[13] Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561

[14] Shovon Niverd Pereira, Noshin Tasnim, Rabius Sunny Rizon, Muhammad Nazrul Islam "Blockchain-Based Digital Record-Keeping in Land Administration System", "Proceedings of International Joint Conference on Advances in Computational Intelligence", 2021, pp.431-443

[15] R.C. Suganthe, N. Shanthi, R.S. Latha, K. Gowtham, S. Deepakkumar, R. Elango, "Blockchain enabled Digitization of Land Registration", " 2021 International Conference on Computer Communication and Informatics (ICCCI)", 2021, DOI:

10.1109/ICCCI50826.2021.9402469

[16] Heng Xu, Nan Zhang, "Privacy implications ofblockchain systems: a datamanagement perspective", "Published in Organizational Cybersecurity Journal: Practice, Process and People", Vol 03, 2023, DOI:10.1108/OCJ-01- 2023-0003

[17] ALHAJ HOSSEN, MD. MAHEDI HASAN, TAHMID AHMED, MD. ANWAR HUSSEN WADUD, "A BLOCKCHAIN-BASED SECURED LAND RECORD SYSTEM USING HYPERLEDGER FABRIC", "THE FOURTH INDUSTRIAL REVOLUTION AND BEYOND", 2023, DOI: 10.1007/978-981-19-8032-9_1

[18] Pinata: IPFS Pinning Service. https://www.pinata.cloud 8] Buterin, V. (2013). "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." Ethereum Whitepaper. [Link to Ethereum Whitepaper]

[19] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." Proceedings of IEEE International Congress on Big Data.

[20] G. Li and H. Sato, “A privacy-preserving and fully decentralized storage and sharing system on the blockchain,” in Proceedings of the 2019 IEEE 43rd Annual Computer Software and Applications Conference, pp. 694–699, IEEE, Milwaukee, WI, USA, July 2019

.