VIVA-TECH IJRI
ANNUAL RESEARCH JOURNAL

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

A Review on Blockchain based Legal Vault

Dhruv Dutkar[1], Neha Kadam[2], Ansh Poojari[3], Prof. Bhavika Thakur[4]
[1]*(Department of Computer Engineering, Mumbai University, MUMBAI)*
[2]*(Department of Computer Engineering, Mumbai University, MUMBAI)*
[3]*(Department of Computer Engineering, Mumbai University, MUMBAI)*
[4]*(Professor, Department of Computer Engineering, Mumbai University, MUMBAI)*

Abstract: *In today's digital age, the legal industry is experiencing a transformative shift towards efficient, secure, and transparent record-keeping solutions. This project introduces a pioneering Blockchain-Based eVault designed to revolutionize the management and preservation of legal records. Leveraging the power of blockchain technology, this system provides an immutable, tamper-proof, and easily accessible repository for legal documents, ensuring the integrity, authenticity, and privacy of sensitive information. By harnessing the capabilities of blockchain technology, the Blockchain-Based eVault for Legal Records addresses the pressing need for secure, transparent, and efficient legal record management. It offers a solution that can significantly reduce the risk of document fraud, errors, and data breaches while simplifying complex legal processes. This project represents a promising step towards the modernization of the legal industry and sets a precedent for the adoption of blockchain-based solutions in other sectors reliant on secure data management and transparency.*

Keywords *– authenticity, eVault, immutable, integrity, legal records, transparent.*

I. Introduction

In an era marked by technological advancements and the increasing need for secure, transparent, and efficient legal record management, we present the Legal Records Evault. Our mission is to harness the power of block chain technology and smart contracts to revolutionize the way legal records are stored, managed, and shared. With a strong focus on security, accessibility, and interoperability. The importance of immutable evidence cannot be overstated in a legal context, where disputes and cases often hinge on the credibility and authenticity of presented facts. Physical documents, or digital files that are susceptible to manipulation or accidental loss. Traditionally, the preservation and protection of evidence have relied heavily on paper records, however, the Legal Vault concept leverages advanced technology and cryptographic techniques to create a digital fortress for crucial legal evidence, making it virtually invulnerable to tampering while maintaining the accessibility.

II. Review Of Literature Survey

The following chapter is a literature survey of the previous research papers and research which gives the detailed information about the earlier system along with its pros and cons.

Sonali Patil, Sarika Kadam, Jayashree Katti [1] explores the utilization of blockchain technology is deemed more suitable for establishing a transparent system with the immutability of forensic evidence. Blockchain facilitates the transfer of assets or evidence reports within a transparent environment without the need for a central authority. Through this proposed system, tampering with forensic evidence can be readily traced at any stage by any party within the forensic chain. By leveraging the Ethereum platform, the security enhancement of forensic evidence is achieved, ensuring high integrity, traceability, and immutability. In today's digital era, data holds paramount importance in various domains. It is imperative to ensure the security of data storage and processing across different formats due to the potential for tampering. With the escalating instances of cybercrime, malicious actors often target crucial information for organizations, posing a significant threat to the reliability and provenance of digital evidence required for forensic investigations. Therefore, maintaining the integrity and provenance of digital evidence as it traverses through different stages of forensic investigation is essential.

Shivansh Kumar, Aman Kumar Bharti, Ruhul Amin [2] analysis delves into existing solutions and their architecture, aiming to pave the way for future research and development in emerging IPFS and Blockchain technologies. Currently, numerous hospitals store their patients' data locally, with some lacking backup storage altogether. This scenario poses a significant risk of data loss or corruption. Although many healthcare institutions are transitioning to cloud storage, these platforms harbor their own threat vectors. The recent surge in ransomware and Distributed Denial of Service (DDoS) attacks during the COVID-19 outbreak targeted various healthcare providers, resulting in the disruption of essential services and leaving hundreds of thousands without access to healthcare. Furthermore, traditional database practices often lead to the misplacement or mixing of patient data, exacerbating complications. To address these challenges, numerous researchers are actively engaged in leveraging IPFS and Blockchain technologies to enhance the storage of medical records.

Abdullah ayub khan, Mueen uddin, aftab ahmed shaikh, Asif ali laghari, adil e. rajput [3] proposes a digital forensic investigation architecture called MF-Ledger, which leverages blockchain technology, particularly Hyperledger Sawtooth, to ensure security and transparency in the investigation process. In this architecture, participating stakeholders form a private network where they can exchange information and reach consensus on various investigation activities before recording them on the blockchain ledger. One of the key components of this architecture is the use of smart contracts, which are digital contracts implemented using sequence diagrams. These smart contracts facilitate secure interaction among stakeholders throughout the investigation process. The primary goal of MF-Ledger is to provide a robust mechanism for ensuring the integrity, prevention, and preservation of evidence, commonly referred to as the chain of custody, in a private permissioned encrypted blockchain ledger. By utilizing blockchain technology, the architecture ensures that once information is recorded on the ledger, it becomes permanently and immutably stored, thereby maintaining the integrity of the investigation process. The paper emphasizes the importance of addressing the challenges posed by the increasing globalization and connectivity, particularly in the context of multimedia data exchange over the Internet.

Meng Li a, Chhagan Lal b, Mauro Conti c, Donghui Hu [4] tell that the lawful evidence management in digital forensics is critical for ensuring the integrity and privacy of evidence throughout its lifecycle, from collection during police investigations to presentation in court trials. Existing approaches often lack robust security models and fail to adequately address key privacy concerns, such as protecting witness and juror privacy. In this paper, we propose LEChain, a blockchain-based lawful evidence management scheme designed to supervise the entire evidence flow and court data, including evidence collection, access, and court proceedings. Fine-grained access control based on ciphertext-policy attribute-based encryption is employed to regulate evidence access. A secure voting method is developed to protect juror privacy during court trials. Additionally, we establish a consortium blockchain to record evidence transactions, ensuring transparency, immutability, and auditability.

Dr. Ch. Rupa, Senior Member, Dr.Divya Midhunchakkaravarthy [5] proposes a novel approach to tackle the issue of forgery in medical evidence by leveraging advanced features of blockchain technology. In this model, a regulatory body authorizes healthcare centers (hospitals) to issue medical certificates in a decentralized manner. Smart contracts are employed to facilitate the verification of certificate authenticity by any authorized party worldwide. The key strength of this paper lies in its utilization of blockchain-based solutions to address the challenges associated with proving the authenticity of medical evidence. By employing blockchain technology, the model ensures transparency, immutability, reliability, and decentralization, which are crucial properties for securing medical certificates effectively. To protect sensitive and critical data across various application domains such as communication systems, healthcare, education, and the financial sector, advanced privacy preservation techniques are implemented. However, the focus of this paper is primarily on healthcare, where the issuance and verification of medical certificates play a significant role.

Zhihong Tiana, Mohan Li a, Meikang Qiub, Yanbin Suna, Shen Su [6] introduces Block-DEF, a secure Digital Evidence Framework utilizing blockchain technology (Block-DEF). Block-DEF employs a loosely coupled structure wherein evidence and evidence information are managed separately. Specifically, only evidence information is stored on the blockchain, while the evidence itself resides on a trusted storage platform. To mitigate blockchain bloat, Block-DEF proposes a lightweight blockchain featuring a mixed block structure and an optimized name-based Practical Byzantine Fault Tolerance (PBFT) consensus mechanism. Analytical and experimental evaluations demonstrate Block-DEF's scalability, integrity, and validity assurance for evidence, effectively balancing privacy and traceability. A robust digital evidence system must prevent tampering with evidence and safeguard against information leakage.

Yu Xiong, Jiang Du [7]. introduce an electronic evidence preservation model founded on blockchain technology. Blockchain, renowned for its decentralized and immutable nature, offers a promising solution for ensuring the safety and reliability of data. By leveraging blockchain, this model aims to establish a robust framework for preserving electronic evidence in a secure and tamper-proof manner. The proposed model operates on the principles of decentralization, cryptographic hashing, and consensus mechanisms inherent to blockchain technology. Through distributed ledger technology, electronic evidence can be stored across a network of nodes, eliminating the vulnerabilities associated with centralized databases. Moreover, cryptographic hashing techniques are employed to create unique fingerprints for each piece of evidence, facilitating easy verification and detecting any alterations or tampering attempts.

Jingjing Guo, Xuliang Wei, Yuling Zhang, Jianfeng Ma,Huamin Gao,Libo Wang , Zhiquan Liu [8] proposes a solution to address the critical issue of evidence tampering and ensure the integrity, consistency, and nonrepudiation of evidence transfer records in China's judicial system. To achieve this, the authors propose the use of a consortium blockchain network. This network would record evidence transfer events among different departments within the judicial system. By utilizing blockchain technology, which offers immutability and transparency, the system aims to provide a secure and tamper-proof way of documenting evidence transfer. The proposed solution outlines the format of transactions and blocks within the blockchain network. Additionally, smart contracts for three types of transactions are designed to automate and enforce rules governing evidence transfer. The authors adopt the Raft consensus algorithm to achieve consensus among network participants. Consensus mechanisms are crucial in ensuring that all parties agree on the state of the blockchain, thereby maintaining the integrity and consistency of recorded data.

Revathy Sathyaprakasan, Pratheeksha Govindan, Samina Alvi, Lipsa Sadath, Sharon Philip, Nrashant Singh [9] tells that the forensic science heavily relies on the management of evidence to ensure the integrity and admissibility of evidence in court proceedings. The process of maintaining the Chain of Custody is crucial in preserving the integrity of evidence. Inadequate preservation of the Chain of Custody can render evidence inadmissible, leading to case dismissal. With the increasing need for digitalization in forensic evidence management, blockchain technology presents a promising solution. Blockchains are digitally distributed ledgers that offer transparency, immutability, and security through cryptographic techniques. Hyperledger Fabric, a consortium blockchain framework, is particularly suitable for enterprise-level applications. This paper proposes a framework leveraging Hyperledger Fabric to digitalize forensic evidence management and maintain the Chain of Custody. Additionally, an algorithm is presented to implement blockchain technology in this domain, ensuring the integrity and admissibility of forensic evidence.

Donghyo Kim, Sun-Young Ihm, Yunsik Son [10] proposes a novel approach to managing digital evidence in criminal investigations. This system involves the use of two separate blockchains, referred to as the hot and cold blockchains, to handle different types of digital evidence. The hot blockchain is designed to store information that frequently changes, while the cold blockchain is utilized for storing immutable data such as videos. This two-level architecture aims to optimize the storage and retrieval of digital evidence, thereby enhancing the efficiency of the criminal investigation process. To evaluate the effectiveness of the proposed system, the authors conducted performance measurements focusing on the storage and inquiry processing of digital crime evidence videos across various capacities within the two-level blockchain system. This evaluation likely involved assessing factors such as storage capacity, data retrieval speed, scalability, and overall system responsiveness.

P. Rajitha Nair, Dr. D. Ramya Dorai [11] the article aims to conduct a comprehensive review of current literature and consolidate study findings to evaluate the performance of two methodologies: Proof of Stake and Proof of Work, for implementing Blockchain technology in data storage. By assessing performance metrics and security features of both methodologies, the goal is to identify a secure and high-performing blended Blockchain approach with broad practical application across industries. Storing data in Blockchain has gained popularity in the technical and communication industry, attracting participation from major players. Two primary methodologies facilitating Blockchain implementation are "Proof of Work" and "Proof of Stake." Proof of Work involves members solving complex problems without a specific need for the solution, aside from serving as evidence, which consumes significant resources. On the other hand, Proof of Stake requires fewer resources to ensure secure data storage in Blockchain.

Sotirios Brotsis, Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles, Dimitris Kavallieros, Emanuele Bellini, Clement Pavu ´ e [12] proposes a blockchain-based solution tailored for the Smart home domain, focusing on the collection and preservation of digital forensic evidence. The system incorporates a private forensic evidence database for storing captured evidence, complemented by a permissioned blockchain for providing security services such as integrity, authentication, and non-repudiation, ensuring the admissibility of evidence in legal proceedings. The blockchain records metadata associated with the evidence, essential for facilitating the aforementioned security services, and employs smart contracts to interact with various entities involved in the investigation process, including Internet service providers, law enforcement agencies, and prosecutors. This solution aims to address the challenges posed by cyber-attacks in IoT networks, enhancing the security and reliability of forensic evidence management.

Muhammad Imran Sarwar 1, Muhammad Waseem Iqbal 2, Tahir Alyas 3, Abdallah NAMOUN 4, Ahmed Alrehaili 4, Ali Tufail 5 [13] tells that the data vaults for Blockchain-Empowered Accounting Information Systems represent an innovative approach to securely storing and managing financial data within blockchain networks. These vaults function as highly secure repositories for accounting information, capitalizing on the decentralized and immutable characteristics of blockchain technology. Through the application of cryptographic techniques, data stored within these vaults is encrypted, guaranteeing confidentiality and integrity. Blockchain's distributed ledger technology plays a pivotal role in ensuring transparency and trust by recording all transactions in an immutable manner. This tamper-evident feature significantly diminishes the risk of fraud or data manipulation, as any unauthorized alterations would be immediately detected. Moreover, the decentralized nature of blockchain networks eliminates the necessity for intermediaries, thus streamlining processes and reducing the costs associated with traditional accounting systems. In essence, Data Vaults for Blockchain-Empowered Accounting Information Systems offer enhanced security, transparency, and efficiency, making them an appealing choice for organizations seeking to modernize their accounting practices.

Xiaoling Zhu 1 and Chenglong Cao 2 [14] propose a robust solution for conducting exams online while enhancing security and integrity. This framework integrates biometric authentication and blockchain technology to ensure the authenticity of exam takers and the integrity of exam results. Biometric authentication methods such as fingerprint or facial recognition are employed to verify the identity of individuals, thereby mitigating the risk of impersonation or cheating. By leveraging these biometric markers, the system can reliably authenticate users before allowing them to participate in an exam, significantly reducing the possibility of fraudulent activity. Furthermore, the utilization of blockchain technology offers a tamper-proof and transparent record of exam activities throughout the entire examination process, including registration, submission, and grading. Each transaction related to the exam is securely recorded on the blockchain, ensuring immutability and preventing unauthorized alterations to exam data. This transparency enhances the integrity of the examination process and fosters trust among stakeholders.

Philipp Paech [15] examines the interplay between liquidity and legal certainty within the realm of blockchain technology, particularly in the context of securities trading. The advent of blockchain platforms for securities trading has revolutionized liquidity by offering decentralized avenues for faster and more efficient transactions. However, this enhanced liquidity poses challenges concerning legal certainty, given the decentralized nature of blockchain, which raises pertinent questions regarding regulatory compliance and investor protection. The paper delves into the intricate balance required between these two factors, emphasizing the necessity for regulatory frameworks capable of adapting to the dynamic landscape of blockchain-based securities trading. Such frameworks should aim to uphold investor confidence and ensure legal compliance while accommodating the innovative potential of blockchain technology. By exploring the trade-offs inherent in this balance, this paper contributes to a deeper understanding of the challenges and opportunities presented by blockchain in the securities trading domain.

III. Analysis

Analysis table summarizes the research papers on the IV-Drip Monitoring and Controlling. Below is a detailed description of various algorithms used in research papers.

Table 1: Analysis Table

Title	Summary	Advantages	TechStack
Security Enhancement of Forensic Evidences Using Blockchain [1]	In this approach, there is a forensic chain in which generated report passes through various levels or intermediaries such as pathology laboratory, doctor etc.	Remove intermediaries and thereby to minimize transaction cost and frauds with central authority.	Privacy and Confidentiality, Regulatory and Legal Framework.
Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions [2]	It presents a detailed study of the IPFS and Blockchain based Healthcare secure storage solutions.	Provides proper authentication of data using different authentication processes and collects real-time data, which are very for patient predictive health analysis.	For prototype implementation and for logical model systems, adding different technology with IPFS and Blockchain is the choice of many researchers.
MF-Ledger: Blockchain Hyperledger Sawtooth-Enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture[3]	This paper bridges this gap by enabling a secure and transparent digital forensic investigations process using blockchain technology.	Case investigation is shared among potentially untrusted stakeholders.	Data Integrity, Regulatory Compliance.
LEChain: A blockchain-based lawful evidence management	Propose LEChain, a blockchain based lawful evidence	Blockchain's immutable ledger ensures that once data is recorded, it	To enhance LEChain's practicality by integrating it with real-world investigation.

scheme for digital forensics [4]	management scheme to supervise the entire evidence flow and all of the court data.	cannot be altered or deleted.	
Preserve Security to Medical Evidences using Blockchain Technology [5]	The regulatory body will authorize the Health care centers to issue medical certificates to the required persons in adecentralized approach.	Blockchain allows for easy and secure access to medical evidence from anywhere in the world	Multi signature scheme is to be used in future.
Block-DEF: A secure Digital evidence Framework using blockchain [6]	Secure digital evidence Framework using blockchain (Block-DEF) with a loose coupling structure.	Block-DEF can provide a secure and auditable chain of custody for digital evidence.	Block-DEF can be employed for secure Identity verification and authentication processes.
Electronic evidence preservation model based on blockchain [7]	This paper discusses the growing significance of electronic data in legal cases due to the internet's development.	This immutability ensures that electronic evidence, once stored on the blockchain.	Blockchain technology will bring great changes to the field of electronic data preservation in the future.
Antitampering Scheme of Evidence Transfer Information in Judicial System Based on Blockchain [8]	Consortium blockchain network is suggested to record evidence transfer events within China's judicial system.	By utilizing blockchain technology, the system ensures the integrity of evidencetransfer records. Once data is recorded, it becomes immutable, reducing the risk of tampering.	Blockchain technology is continuously evolving. Staying up to date with the latest advancements and ensuring the proposed system remains secure and efficient may require ongoing development efforts.
An Implementation of Blockchain Technology in Forensic Evidence Management [9]	The study proposes the use of Blockchain Technology, inspired by Hyperledger Fabric, to create a digitalized forensic evidence management system.	The chronological recording of evidence handling on a blockchain maintains the Chain of Custody, making it airtight and admissible in court.	Maintaining the privacy of sensitive forensic data while ensuring transparency is a delicate balance that needs to be addressed.
Two-Level Blockchain System for Digital Crime Evidence Management [10]	The study evaluated the system's storage and inquiry processing performance for digital crime evidence videos under various capacities.	Separating data into hot and cold blockchains optimizes performance, as only frequently changing information is processed in the hot blockchain, reducing the computational load.	Implementing and maintaining a blockchain system can be resource-intensive.
Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain [11]	This involves two main approaches: "Proof of Work" and "Proof of Stake." Proof of Work involves solving complex problems,	Miners are rewarded with cryptocurrency, motivating them to maintain the network.	It requires specialized and expensive hardware, which can exclude smaller players.

	consuming significant resources, mainly for evidence.		
Blockchain Solutions for Forensic Evidence Preservation in IoT Environments [12]	This paper introduces a blockchain-based solution for the smart home domain to address cyber-attacks and digital forensic evidence preservation in IoT networks.	Blockchain's data preservation capabilities ensure that evidence Remains accessible and Intact for an extended period.	Ensuring data recovery and backup solutions in case of blockchain failure or data loss is essential.
Data Vaults for Blockchain-Empowered Accounting Information Systems [13]	In this research, a hybrid solution is proposed to ensure AIS data integrity against any deliberate attempt or mala-fide intention for alteration or deletion from the database that can be verified at any later stage.	Transparency and Trust and Cost Efficiency.	Blockchain Platforms: Ethereum, Hyperledger Fabric, Corda, etc., provide the underlying blockchain infrastructure for data storage and transaction processing.
Secure Online Examination with Biometric Authentication and Blockchain-Based Framework [14]	It propose a novel biometric authentication and blockchain-based online examination scheme examination data are encrypted to store in a distributed system, which can be obtained only if the user satisfies decryption policy.	Biometric authentication ensures the identity of exam takers, reducing the risk of impersonation or cheating.	Node.js, Django, or Flask for developing the backend logic and APIs for exam management and data processing.
Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty [15]	This article shows what the new international legal framework could look like in the light of experience gained from earlier developments.	By eliminating intermediaries and streamlining processes, blockchain-based securities trading can significantly reduce transaction costs associated with traditional securities markets, benefiting both issuers and investors.	Software wallets or hardware wallets allow users to securely store and manage their digital securities tokens, providing access to their assets while maintaining control over private keys.

IV. CONCLUSION

The concept of Legal Vaults, designed to ensure the immutability of evidence, presents a groundbreaking opportunity to transform the way we handle legal information and evidence in the digital age. Through our exploration of this project topic, it has become evident that the implementation of Legal Vaults has the potential to significantly enhance the integrity and credibility of legal proceedings. These digital fortresses for evidence can substantially reduce the risk of tampering and provide a secure platform for preserving information vital to the pursuit of justice. In conclusion, the Legal Vault concept represents a promising path forward in the legal field. With continued research, development, and collaboration among legal experts, technologists, and ethicists, we can harness the full potential of Legal Vaults while safeguarding the rights and interests of individuals involved in legal proceedings.

References

[1] S. Patil, S. Kadam and J. Katti, "Security Enhancement of Forensic Evidences Using Blockchain," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 263-268, doi: 10.1109/ICICV50876.2021.938.

[2] Kumar, Shivansh & Bharti, Aman & Amin, Ruhul. (2021). Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions. Security and Privacy. 4. 10.1002/spy2.162.

[3] A. A. Khan, M. Uddin, A. A. Shaikh, A. A. Laghari and A. E. Rajput, "MF-Ledger: Blockchain Hyperledger Sawtooth-Enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture," in IEEE Access, vol. 9, pp. 103637-103650, 2021, doi: 10.1109/ACCESS.2021.3099037.

[4] Meng Li, Chhagan Lal, Mauro Conti, Donghui Hu, LEChain: A blockchain-based lawful evidencemanagement scheme for digital forensics, Future Generation Computer Systems, Volume 115,2021,Pages406-420,ISSN0167-739X, https://doi.org/10.1016/j.future.2020.09.038.(https://www.sciencedirect.com/science/article/pii/S0 1 67739X1933167X).

[5] C. Rupa and D. Midhunchakkaravarthy, "Preserve Security to Medical Evidences using BlockchainTechnology," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2020, pp. 438-443, doi: 10.1109/ICICCS48265.2020.9120948.

[6] Alam M., Lee Z.C., Nicopoulos C., Lee K.H., Kim J., Lee J., SBBox: A tamper-resistant digital archiving system, Int. J. Cyber-Secur. Digit. Forensics 5 (3) (2016) 122–131.

[7] Yu Xiong and Jiang Du. 2019. Electronic evidence preservation model based on blockchain. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (ICCSP).

[8] Jingjing Guo, Xuliang Wei, Yuling Zhang, Jianfeng Ma, Huamin Gao, Libo Wang, Zhiquan Liu, "Antitampering Scheme of Evidence Transfer Information in Judicial System Based on Blockchain", Security and Communication Networks, vol. 2022, Article ID 5804109, 19 pages, 2022. https://doi.org/10.1155/2022/5804109.

[9] R. Sathyaprakasan, P. Govindan, S. Alvi, L. Sadath, S. Philip and N. Singh, "An Implementation of Blockchain Technology in Forensic Evidence Management," 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 2021, pp. 208-212, doi: 10.1109/ICCIKE51210.2021.9410791.

[10] Kim D, Ihm SY, Son Y. Two-Level Blockchain System for Digital Crime Evidence Management. Sensors (Basel). 2021 Apr 27;21(9):3051. doi: 10.3390/s21093051. PMID: 33925538;PMCID: PMC8123771.

[11] P. R. Nair and D. R. Dorai, "Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 279-283, doi: 10.1109/ICICV50876.2021.9388487.

[12] S. Brotsis et al., "Blockchain Solutions for Forensic Evidence Preservation in IoT Environments," 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, 2019, pp. 110-114, doi: 10.1109/NETSOFT.2019.8806675. keywords: {Forensics;Blockchain;Intrusion detection;Smart phones;Smart homes;Internet of Things;Blockchain;Cyber-security;Forensic evidence;Intrusion detection;Internet of things}.

[13] M. I. Sarwar et al., "Data Vaults for Blockchain-Empowered Accounting Information Systems," in IEEE Access, vol. 9, pp. 117306-117324, 2021, doi: 10.1109/ACCESS.2021.3107484.

[14] Xiaoling Zhu, Chenglong Cao, "Secure Online Examination with Biometric Authentication and Blockchain-Based Framework", Mathematical Problems in Engineering, vol. 2021, Article ID 5058780, 12 pages, 2021. https://doi.org/10.1155/2021/5058780

[15] Paech, Philipp, Securities, Intermediation and the Blockchain - An Inevitable Choice between Liquidity and Legal Certainty? (December 22, 2015). LSE Legal Studies Working Paper 20/2015 (update June 2016), Uniform Law Review (2016) 21 (4), Available at SSRN: https://ssrn.com/abstract=2697718 or http://dx.doi.org/10.2139/ssrn.2697718