paper

by Pratheek .

A Blockchain-Based Framework for Secure Management of Government and Law Enforcement Records

Himanshu S Shetty
Dept. of Computer Science and Engineering
Sahyadri College of Engineering & Management
Mangalore, India
himanshushettykt03@gmail.com

Pratheek G Shetty
Dept. of Computer Science and Engineering
Sahyadri College of Engineering & Management
Mangalore, India
pratheekshetty934@gmail.com

M Imaad Iqbal
Dept. of Computer Science and Engineering
Sahyadri College of Engineering & Management
Mangalore, India
mohdimadiqbal@gmail.com

Shifali Florine Lobo
Dept. of Computer Science and Engineering
Sahyadri College of Engineering and Management
Mangalore, India
shifalilobo9@gmail.com

Dr Mustafa Basthikodi
Dept. of Computer Science and Engineering
Sahyadri College of Engineering and Management
Mangalore, India
mbasthik@gmail.com

***Abstract*—The integrity, security, and accessibility of government and law enforcement records are fundamental to public trust. Yet, traditional centralized databases remain vulnerable to data manipulation, cyberattacks, and systemic inefficiencies that can compromise sensitive legal documents and undermine judicial processes. Blockchain technology offers a paradigm shift toward decentralized trust and cryptographic assurance. This paper presents a robust framework designed using Hyperledger Fabric to secure government legal records and enhance law enforcement procedures. We focus on the practical application of a permissioned blockchain, which is better suited for government use than public, cryptocurrency-based models. The architecture integrates smart contracts to automate legal documentation workflows and employs a hybrid on-chain/off-chain storage model to ensure scalability. Our results demonstrate a functionally complete, tamper-proof system that improves efficiency and provides a fully auditable trail for all record interactions. This work validates the feasibility of blockchain as a foundational technology for next-generation digital governance.**

***Index Terms*—Blockchain, Hyperledger, Legal Records, Law Enforcement, Smart Contracts, Data Security, Government Applications, Tamper-Proof Systems, Judicial Data, Auditability.**

I. INTRODUCTION

In the era of digital governance, public institutions are tasked with a monumental challenge: safeguarding the sanctity of official records while making them accessible. As governments transition from paper-based archives to digital infrastructures, they expose themselves to a new class of threats, including sophisticated data breaches, unauthorized tampering, and systemic failures [5], [8]. Within the legal and law enforcement sectors, the consequences of these vulnerabilities are particularly dire. A compromised chain of evidence or a manipulated judicial record can erode due to process, obstruct justice, and catastrophically damage public confidence in the rule of law. Legacy systems are often ill-equipped to counter these modern threats, making the shift to a more resilient and accountable digital infrastructure not just a technological upgrade, but a fundamental necessity for governmental legitimacy [10].

This paper advances a solution built on blockchain technology, a decentralized ledger system that offers security and transparency by design. By moving beyond the cryptocurrency origins of blockchain [2], we leverage an enterprise-grade, permissioned framework—Hyperledger Fabric—which is engineered for the specific privacy and governance needs of institutions [3]. The core architectural principles of blockchain, namely its immutable ledger and decentralized consensus, provide a powerful defense against data manipulation. Furthermore, by integrating smart contracts, we can automate and enforce legal and administrative protocols, which drastically reduces the potential for fraud and human error while streamlining complex workflows [16], [18]. This approach promises to build a new foundation of trust in our judicial processes.

The operational advantages extend beyond mere security. A blockchain-based system creates a fully auditable, transparent, and chronological trail of every transaction or data interaction, a feature of immense value in legal proceedings and internal audits [1]. Pioneering real-world implementations have already validated this potential. Estonia, for example, has successfully integrated blockchain into its e-governance services to secure public records, while Georgia deployed a similar solution for its land registry to reduce fraud [6], [7].

Despite this promise, a significant gap remains between conceptual frameworks and comprehensive, scalable solutions tailored to the demands of the legal and law enforcement sectors. Much of the existing literature either remains theoretical or focuses on narrow applications, failing to address the requirements of a unified judicial record management system [11], [15].

This study addresses this gap directly. We present a secure, tamper-proof blockchain architecture for government legal records, designed and implemented using the Hyperledger Fabric framework. We detail the development of smart contracts that automate key judicial procedures, provide a critical analysis of the system's performance, and discuss the tangible benefits and challenges of deploying such a framework. Specifically, our primary contribution is the validation of a hybrid on-chain/off-chain architectural model that solves the scalability problem of storing large legal files, combined with robust, role-based smart contract logic to automate judicial access control.

II. RELATED WORKS

Our research builds upon a rich body of work spanning foundational blockchain theory, pioneering government pilot programs, and architectural solutions from parallel domains. Blockchain's theoretical groundwork is well-established. Technical overviews, such as Zheng et al. [4], catalog the architectures and consensus protocols. While invaluable for their strategic vision, these foundational works primarily out- line the "why" rather than the technical "how" for public sector implementation

A. Pioneering Implementations in the Public Sector

Several governments have moved beyond theory, offering practical case studies. Estonia's pioneering e-governance model uses blockchain to ensure national data integrity [6]. Similarly, Georgia's Ministry of Justice deployed a blockchain land registry to increase transparency and combat fraud [7]. Dubai has also launched ambitious initiatives, highlighting both operational benefits and legal hurdles [24]. These significant projects are nonetheless confined to specific domains like property or identity. They do not address the complex data flows inherent in the judicial and law enforcement ecosystem.

B. Applying Designs from Other Areas

Many of the technical challenges in our project—such as data privacy, auditability, and interoperability—have been addressed in other fields. Extensive research into blockchain for healthcare data management, for instance, provides robust models for securing sensitive patient records that can be adapted for legal evidence [20], [22]. Likewise, frameworks for user-controlled data sovereignty [17], verifiable digital credentials [18], and secure identity verification [26] offer proven patterns for managing access rights among different legal stakeholders. These architectural blueprints provide essential components, but they require significant adaptation to meet the unique evidentiary rules and procedural constraints of the judicial sector.

C. Identifying the Research Gap

The collective literature confirms a strong consensus on blockchain's capacity to bring unprecedented security and efficiency to government operations [1], [23], [29]. However, a critical gap persists between this potential and its comprehensive application within the legal and law enforcement domains. Much of the existing work remains either at a high conceptual level [9], is validated only within narrow, non-judicial pilots [6], [7], or lacks the empirical evidence that comes from a live, integrated deployment [25]. Our research directly addresses this deficiency by designing, implementing, and validating a holistic blockchain framework specifically engineered to meet the stringent requirements of a modern judicial system.

D. Positioning Our Framework

While pioneering implementations in Estonia and Georgia validate blockchain for public records , they often focus on specific domains like identity or land registry. Similarly, frameworks from other sectors like healthcare provide robust patterns for privacy , but they are not tailored for the unique chain-of-custody rules and complex, multi-actor access policies required by the judicial system (e.g., judge, prosecutor, defense). Our framework addresses this gap by providing a holistic solution that specifically combines an immutable on-chain ledger for metadata with a scalable, encrypted off-chain storage model for large evidence files , all governed by smart contracts explicitly designed to automate these complex legal workflows.

III. SYSTEM DESIGN AND IMPLEMENTATION

This section details the architecture and technical protocols of our proposed system. Our methodology was guided by the core requirements of judicial data management: creating a secure, tamper-proof, and efficient environment that is both auditable and scalable. To achieve this, we integrated a permissioned blockchain, decentralized storage, and robust cryptographic techniques.

A. System Architecture

We designed a hybrid architecture combining Hyperledger Fabric for the permissioned ledger and the InterPlanetary File System (IPFS) for decentralized storage. Hyperledger Fabric provides a controlled, auditable environment for immutable metadata and access rights—critical for government systems—while IPFS offers a resilient, efficient solution for storing large data objects, like evidence files, off-chain.

Hyperledger Fabric was chosen over other enterprise platforms, such as Quorum or Corda, due to its permissioned nature, modular architecture, and robust support for 'channels.' This feature allows for private transactions between specific organizations (e.g., a prosecutor's office and a courthouse), aligning perfectly with judicial confidentiality requirements. This separation ensures the blockchain remains lightweight and performant. The overall architecture is depicted in Fig.1.

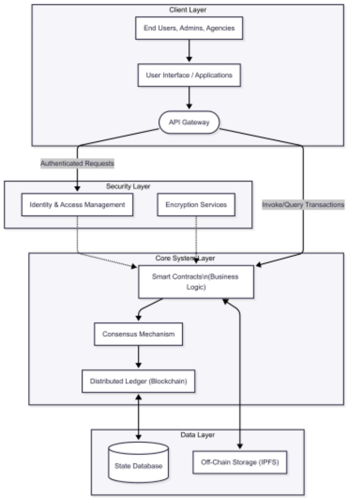

Fig. 1. System architecture detailing the Client, Security, Core, and Data components.

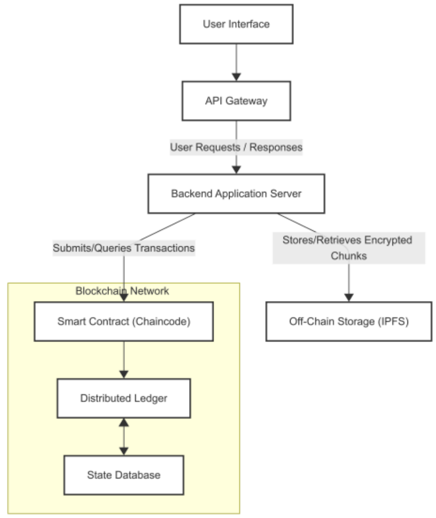

Fig. 2. The end-to-end workflow for data ingestion, from the initial user request to the final blockchain transaction.

B. Secure Data Ingestion and Retrieval Workflow

The system's end-to-end process flow, illustrated in Fig. 2. The workflow begins at the User Interface. Requests are routed via an API Gateway to the central Backend Application Server, which acts as the orchestrator. The backend manages two distinct operations: it stores large, encrypted file chunks in Off-Chain Storage (IPFS) and submits the corresponding metadata as a transaction to the Blockchain Network. Within the network, the Smart Contract (Chaincode) validates and commits the transaction to the immutable Distributed Ledger, whose current state is maintained in the State Database. This architecture cleanly separates large file storage from immutable verification, ensuring both scalability and integrity.

A cornerstone of this framework is the secure, multi-step process for handling legal records, which guarantees confidentiality, integrity, and availability. The protocol, outlined in Table I, is executed by the backend server. It first generates a unique SHA-256 hash of the file for integrity verification and then encrypts the file using AES. The encrypted file is split into smaller chunks and uploaded to the decentralized storage (IPFS), which returns a verifiable Content Identifier (CID) for each chunk.

By storing only lightweight metadata on-chain, the blockchain remains efficient while providing a tamper-proof and auditable record of every file. Retrieving a file is the reverse process: the metadata is fetched from the ledger, the CIDs are used to retrieve the encrypted chunks from IPFS, and the file is reassembled and decrypted using the stored key.

TABLE I
SECURE DATA INGESTION AND STORAGE PROTOCOL

Step	Description
File Hashing	A unique SHA-256 hash is generated to create a digital fingerprint of the file, enabling future integrity verification.
File Encryption	The file is encrypted using AES with a unique key and Initialization Vector (IV) to ensure confidentiality.
File Chunking	The encrypted file is split into smaller chunks to facilitate efficient and reliable distributed storage on IPFS.
Decentralized Storage	Encrypted chunks are uploaded to IPFS, where each receives a verifiable Content Identifier (CID).
Metadata Transaction	The file's metadata (including its hash, AES key, IV, and the list of CIDs) is recorded as an immutable transaction on the Hyperledger Fabric ledger.

C. Multi-Layered Security Model

The framework implements a multi-layered security strategy. For authentication, we employ a stateless JWT system. Upon login, the backend issues an authToken that must be submitted as a bearer token for all subsequent requests. A dedicated middleware validates this token's signature on every request, rejecting any tampered or invalid tokens.

Authorization is managed via a strict Role-Based Access Control (RBAC) policy, enforced at the middleware level of the backend server. This ensures users only perform actions permitted by their assigned role. The Hyperledger Fabric network itself is architecturally isolated and not directly exposed; only the trusted backend server is permitted to initiate communication with it. As a permissioned blockchain, all operations occur within a secure, private "channel," ensuring transaction data is visible only to authorized organizations. This model positions the blockchain not as the primary enforcer of access control, but as the ultimate, immutable auditor of all actions authorized by the centralized server.

D. Automated Governance via Smart Contracts

Access to legal records is governed by smart contracts (chaincode) deployed on the Hyperledger Fabric network. These contracts function as self-executing digital agreements that autonomously enforce predefined access control policies.

Lst. 1 shows a simplified JavaScript implementation of our `EvidenceContract`, which inherits from the base Fabric `Contract` class. This chaincode is responsible for the final interaction with the ledger. Functions like `storeEvidence` and `getEvidence` are the core of this process. The `storeEvidence` function takes a stringified JSON object containing the evidence metadata and uses the `putState` command to write it to the ledger, keyed by its hash. Conversely, `getEvidence` retrieves the record using its ID.

```
'use strict';
const { Contract } = require('fabric-contract-api');

class EvidenceContract extends Contract {
    async initLedger(ctx) {
        console.info('Chaincode instantiated');
    }

    async storeEvidence(ctx, evdString) {
        const {hash} = JSON.parse(evdString);
        await ctx.stub.putState(hash, Buffer.from(
    evdString));
        return {success:true, hash:hash};
    }

    async getEvidence(ctx, evID) {
        const evBytes = await ctx.stub.getState(evID
    );
        if (!evBytes || evBytes.length === 0) {
            throw new Error(`Evidence ${evID} does
    not exist`);
        }
        return JSON.parse(evBytes.toString());
    }
}
module.exports = EvidenceContract;
```

Listing 1. Simplified JavaScript snippet of the Hyperledger Fabric chaincode

It is important to note that this chaincode is intentionally simple, as it represents the final, trusted step in the workflow. The primary security, including user authentication (JWT) and Role-Based Access Control (RBAC), is enforced by the backend server's `submissionController` *before* it invokes this chaincode. When a user requests a document, the backend first validates their permissions, and only then triggers the smart contract to execute the more granular validation logic detailed in Table II.

TABLE II
SMART CONTRACT ACCESS CONTROL LOGIC

Process Step	**Description**
Identity Verification	The contract confirms the cryptographic identity of the requesting user against the network's trusted member list.
Permission Validation	The contract queries the ledger to verify the user's assigned role and permissions for the specific record being requested.
Rule Execution	The contract enforces any situational rules, such as time-based access restrictions or requirements for multi-party approval.

Access is granted only upon successful validation by the smart contract. Crucially, every access attempt—whether successful or denied—is recorded as an immutable transaction on the blockchain, creating a comprehensive and undeniable audit trail. This automated enforcement minimizes the risk of human error or malicious circumvention of policies.

IV. RESULTS AND DISCUSSION

Our implemented prototype successfully demonstrates the feasibility of a decentralized, tamper-resistant platform that enhances data security and provides complete auditability.

A. Achieving Data Immutability and Verifiable Integrity

A primary achievement is the framework's ability to guarantee the integrity of legal records. By hashing all files and anchoring their metadata on the Hyperledger Fabric ledger, we have created a system where any unauthorized modification to a file becomes immediately detectable. This cryptographic chain-of-custody is essential for legal proceedings, ensuring that digital evidence remains verifiable.

B. Streamlining Processes with Smart Contract Automation

Our system leverages JavaScript-based chaincode (smart contracts) to automate the registration, validation, and access control of forensic and legal data. These smart contracts enforce business logic at the protocol level, which significantly reduces the reliance on manual oversight and minimizes opportunities for human error or malicious activity. This automation demonstrably accelerates traditionally time-consuming workflows, such as evidence verification, while ensuring strict adherence to predefined policies.

C. Performance Evaluation and Analysis

All performance benchmarks were conducted on a modest hardware setup, comprising an Intel Core i3-7100U CPU, 16GB of RAM, and an M.2 SSD, to establish a baseline performance profile. The results demonstrate the system's efficiency even on non-server-grade equipment, suggesting significant potential for enhanced performance in a production environment with enterprise-grade hardware.

The performance evaluation first confirmed the efficiency of our hybrid architecture for individual operations. As shown in Fig. 3, processing times for data ingestion and retrieval scale linearly with file size. This result is critical as it validates our design choice to store large files off-chain, preventing the blockchain ledger itself from becoming a performance bottleneck. The higher computational overhead of the ingestion process—which includes hashing, encryption, and consensus—naturally results in longer response times for the POST /upload endpoint compared to the simpler GET /getfile operation, as detailed in the API metrics in Fig. 4. This predictable performance trade-off is justified by the system's foundational advantage: a tamper-proof, immutable audit trail for every record.

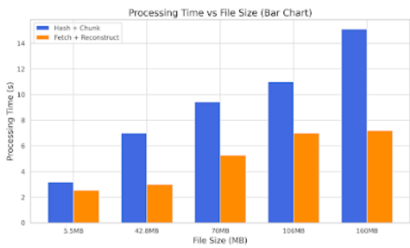

Fig. 3. System processing time for handling files of various sizes, demonstrating a linear performance scaling that supports large files.

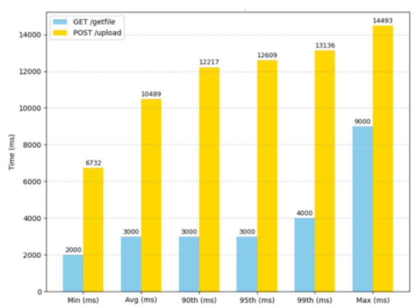

Fig. 4. A comparison of API response times, showing the higher latency of the ingestion process due to cryptographic and consensus overhead.

To assess the system's behavior under realistic conditions, we conducted scalability tests with concurrent users on the file retrieval route (Fig. 5). The results show a characteristic performance curve: as the number of virtual users increases from 20 to 50, the system's throughput (requests/sec) gradually decreases from a peak of approximately 1.2 to 0.6. Concurrently, the average and percentile response times rise, peaking at 30-40 users before stabilizing. This indicates the system is reaching its saturation point, where additional load increases queuing time without improving throughput. The test confirms that the system remains stable under pressure but highlights a clear performance ceiling, providing a valuable benchmark for resource allocation and capacity planning in a production environment.

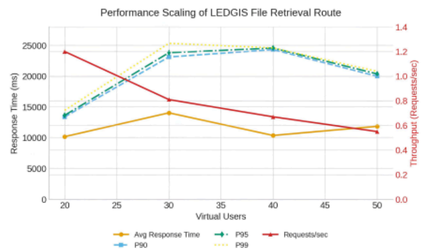

Fig. 5. System performance under concurrent load, illustrating the relationship between throughput and response time as user load increases.

V. CONCLUSION

The challenge of managing legal and law enforcement records in a secure and trustworthy manner is a critical hurdle for modern governments. Traditional centralized databases, with their inherent vulnerabilities to tampering and their lack of transparent auditability, are no longer sufficient. This project demonstrates that a blockchain-based solution, built on a permissioned framework like Hyperledger Fabric, offers a robust alternative.

Our implemented system successfully creates a decentralized, transparent, and efficient environment for legal records. By integrating smart contracts, we have shown how key administrative processes can be automated, reducing both manual overhead and the potential for error or fraud. The immutable, time-stamped audit logs produced by the system guarantee that every interaction is recorded and verifiable, fostering unprecedented accountability. Furthermore, our hybrid architecture, which combines on-chain metadata with off-chain storage, strikes a crucial balance between security and scalability, confirming that the system is not just technically sound but practically deployable.

Ultimately, this work moves beyond theoretical discussion to provide a functional blueprint for a next-generation government service. By ensuring that critical legal data is tamper-proof, auditable, and efficiently managed, blockchain-based infrastructures like the one proposed here can fundamentally enhance institutional integrity and rebuild public trust. With continued development and supportive policy, such systems are poised to become a cornerstone of digital transformation in the public sector.

REFERENCES

[1] S. Liu and Q. Zheng, "A study of a blockchain-based judicial evidence preservation scheme," Blockchain: Research and Applications, vol. 5, 2024, Art. no. 100192. [Online]. Available: https://doi.org/10.1016/j.bcra.2024.100192

[2] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3] Hyperledger Foundation, "Hyperledger Blockchain Frameworks for Business and Government." [Online]. Available: https://www.hyperledger.org

[4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. IEEE Int. Congr. Big Data, 2017. [Online]. Available: https://doi.org/10.1109/BigDataCongress.2017.85

[5] D. Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin Random House, 2016. [Online]. Available: https://books.google.co.in/books/about/Blockchain_Revolution.html?id=NqBiCgAAQBAJ

[6] Government of Estonia, "Estonia's Digital Government and Blockchain Implementation." [Online]. Available: https://e-estonia.com

[7] Ministry of Justice, Georgia, "Blockchain for Land Registry: A Case Study on Secure Government Records," 2017. [Online]. Available: https://gov.ge/blockchain-land-registry

[8] M. Risius and K. Spohrer, "A blockchain research framework: What we (don't) know, where we go from here, and how we will get there," Business Inf. Syst. Eng., vol. 59, no. 6, pp. 385–409, 2017. [Online]. Available: https://link.springer.com/article/10.1007/s12599-017-0506-0

[9] M. Atzori, "Blockchain technology and decentralized governance: Is the state still necessary?," J. Governance Regul., vol. 6, no. 1, pp. 45–62, 2017. [Online]. Available: http://dx.doi.org/10.22495/jgr_v6_i1_p5

[10] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," Telecommunications Policy, vol. 42, no. 4, pp. 335–344, 2018. [Online]. Available: https://doi.org/10.1016/j.telpol.2017.09.003

[11] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," NIST, 2018. [Online]. Available: https://doi.org/10.6028/NIST.IR.8202

[12] M. Swan, Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015. [Online]. Available: https://books.google.co.in/books/about/Blockchain.html?id=ygzcrQEACAAJ

[13] J. Sun, J. Yan, and K. Z. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," Financial Innovation, vol. 2, no. 26, 2016. [Online]. Available: http://dx.doi.org/10.1186/s40854-016-0040-y

[14] M. Pilkington, "Blockchain technology: Principles and applications," in Research Handbook on Digital Transformations, Edward Elgar Publishing, 2016. [Online]. Available: https://doi.org/10.4337/9781784717766

[15] European Commission, "Blockchain for Digital Government: A European Perspective," 2019. [Online]. Available: https://ec.europa.eu/digital-strategy

[16] L. W. Cong and Z. He, "Blockchain disruption and smart contracts," Rev. Financ. Stud., vol. 32, no. 5, pp. 1754–1797, 2019. [Online]. Available: https://doi.org/10.1093/rfs/hhz007

[17] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in IEEE Security and Privacy Workshops, pp. 180–184, 2015. [Online]. Available: https://doi.org/10.1109/SPW.2015.27

[18] N. D. Bhaskar and D. L. K. Chuen, Blockchain and Smart Contract for Digital Certification. Springer, 2017. [Online]. Available: http://dx.doi.org/10.1007/978-3-031-22835-3

[19] T. Saito and T. Yamada, "What's so different about blockchain? Decentralized trust and the future of digital transactions," Harvard Business Review, 2016. [Online]. Available: https://hbr.org/2017/01/the-truth-about-blockchain

[20] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: A blockchain-based secure data exchange architecture for healthcare information systems," J. Med. Syst., vol. 40, no. 10, Art. no. 218, 2016. [Online]. Available: https://doi.org/10.1016/j.jnca.2023.103633

[21] M. Kassen, "Blockchain and public service delivery: a lifetime cross-referenced model for e-government," Information Polity, 2024. [Online]. Available: https://doi.org/10.1080/17517575.2024.2317175

[22] A. Al Mamun, S. Azam, and C. Gritti, "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction," IEEE Access, 2022. [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3141079

[23] M. J. Sousa, "Blockchain as a driver for transformations in the public sector," J. Innov. Entrepreneurship, 2023. [Online]. Available: https://doi.org/10.1080/25741292.2023.2267864

[24] S. Khan, M. Shael, M. Majdalawieh, N. Nizamuddin, and M. Nicho, "Blockchain for Governments: The Case of the Dubai Government," Sustainability, vol. 14, no. 11, p. 6576, 2022. [Online]. Available: https://doi.org/10.3390/su14116576

[25] E. Tan, S. Mahula, and J. Crompvoets, "Blockchain governance in the public sector: A conceptual framework for public management," Gov. Inf. Q., vol. 39, no. 1, p. 101625, 2022. [Online]. Available: https://doi.org/10.1016/j.giq.2021.101625

[26] T.-H. Kim, G. Kumar, R. Saha, M. K. Rai, W. J. Buchanan, and R. Thomas, "A Privacy Preserving Distributed Ledger Framework for Global Human Resource Record Management: The Blockchain Aspect," IEEE Access, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.2995481

[27] C. Piao, Y. Hao, J. Yan, and X. Jiang, "Privacy preserving in blockchain-based government data sharing: A Service-On-Chain (SOC) approach," Inf. Process. Manage., vol. 58, no. 5, p. 1026, 2021. [Online]. Available: https://doi.org/10.1016/j.ipm.2021.1026

[28] N. Elisa, L. Yang, F. Chao, N. Naik, and T. Boongoen, "A Secure and Privacy-Preserving E-Government Framework Using Blockchain and Artificial Immunity," IEEE Access, 2023. [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3239814

[29] J. Mahlaba, A. K. Mishra, D. Puthal, and P. K. Sharma, "Blockchain-Based Sensitive Document Storage to Mitigate Corruptions," IEEE Trans. Eng. Manage., 2022. [Online]. Available: https://doi.org/10.1109/TEM.2022.3183867

[30] F. Wang, Y. Gai, and H. Zhang, "Blockchain user digital identity big data and information security process protection based on network trust," J. King Saud Univ. - Comput. Inf. Sci., 2024. [Online]. Available: https://doi.org/10.1016/j.jksuci.2024.102031

paper

ORIGINALITY REPORT

7%	6%	5%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Pushpalatha K, Ananthanarayana V S. "Multimedia Document Mining using Sequential Multimedia Feature Patterns", 2020 IEEE Sixth International Conference on Multimedia Big Data (BigMM), 2020 Publication	1%
2	www.coursehero.com Internet Source	1%
3	dokumen.pub Internet Source	1%
4	lists.hyperledger.org Internet Source	1%
5	Arif Perdana, S Vijayakumar Bharathi, Ridoan Karim, Saru Arifin, Aashish Srivastava. "Digital Strategy and Governance in Transformative Technologies", CRC Press, 2025 Publication	1%
6	digitalcommons.kennesaw.edu Internet Source	1%
7	Muthu Ramachandran. "Blockchain Engineering", Springer Science and Business Media LLC, 2025 Publication	<1%
8	link.springer.com Internet Source	<1%
9	hal.science Internet Source	<1%
10	repositorio.uloyola.es Internet Source	<1%

11	www.nature.com Internet Source	<1 %
12	Al-Barami, Said Musallam. "Assessing Information Security in Omani Ministries: Data Storage, International Standards Compliance, and Blockchain Potential", Sultan Qaboos University (Oman), 2025 Publication	<1 %
13	Jie Ma, Bin Qi, Kewei Lv. "BSA: Enabling Biometric-Based Storage and Authorization on Blockchain", 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2021 Publication	<1 %
14	core.ac.uk Internet Source	<1 %
15	download.bibis.ir Internet Source	<1 %
16	journalofcloudcomputing.springeropen.com Internet Source	<1 %
17	Md. Ahsan Habib, Md. Motaleb Hossen Manik. " : A Blockchain-Based Framework for Secure Medical Data Sharing and Monetisation ", IET Blockchain, 2025 Publication	<1 %

Exclude quotes	On	Exclude matches	< 3 words
Exclude bibliography	On		