Journal of Social Sciences *Vol. VIII, no. 4 (2025), pp. 202 - 212*
Fascicle *Social Science* *ISSN 2587-3490*
Topic *Sociology* *eISSN 2587-3504*

https://doi.org/10.52326/jss.utm.2025.8(4).13
CZU 351.077:004.7:004.056.5

DATA GOVERNANCE IN THE PUBLIC SECTOR WITH LEXCHAIN: A HYBRID BLOCKCHAIN-CLOUD ARCHITECTURE PROPOSAL

Anatolie Alexei *, ORCID: 0000-0002-0570-4854,
Victor Moraru, ORCID: 0000-0002-5454-8341,
Arina Alexei, ORCID: 0000-0003-4138-957X,
Stefan Bistritchi, ORCID: 0009-0006-4640-5494,
Adrian Manole, ORCID: 0009-0000-9540-3512

Technical University of Moldova, 168, Stefan cel Mare Blvd., Chisinau, Republic of Moldova
* Corresponding author: Anatolie Alexei, *anatolie.alexei@adm.utm.md*

Received: 11. 21. 2025
Accepted: 12. 22. 2025

Abstract. As public administrations at the EU, national, regional, and municipal levels increasingly rely on digital systems to deliver public services, the need for secure, interoperable, and policy-compliant data exchange becomes critical. This paper presents LexChain, a decentralized data-sharing framework designed to address the technical and governance challenges of multi-level e-Governance. Built on a permissioned Ethereum-based blockchain, LexChain combines smart contracts, a decentralized identity system (LexID), and client-side encryption with data fragmentation to enable secure, auditable, and autonomous collaboration between institutions. By storing encrypted file fragments across public cloud providers and recording all metadata and access events on-chain, LexChain ensures that public sector entities can exchange information with full control, without relying on central intermediaries. The system supports interoperability across administrative levels while preserving compliance with privacy and audit requirements. This contribution demonstrates how blockchain-based architectures can strengthen digital trust, transparency, and coordination across multi-tier governance structures.

Keywords: *blockchain, decentralized identity, e-Government, interoperability, public sector innovation, smart contracts.*

Rezumat. Pe măsură ce administrațiile publice la nivel european, național, regional și municipal se bazează tot mai mult pe sisteme digitale pentru a furniza servicii publice, necesitatea unor mecanisme de schimb de date sigure, interoperabile și conforme cu politicile devine esențială. Această lucrare prezintă LexChain, un cadru descentralizat pentru partajarea datelor, proiectat pentru a aborda provocările tehnice și de guvernanță specifice e-Guvernării de tip multi-nivel. Dezvoltat pe un blockchain permisiv bazat pe Ethereum, LexChain combină contracte inteligente, un sistem de identitate descentralizat (LexID) și criptare la nivelul clientului împreună cu fragmentarea datelor, pentru a permite o colaborare sigură, auditabilă și autonomă între instituții. Prin stocarea fragmentelor criptate ale fișierelor la furnizori de cloud public și înregistrarea pe blockchain a tuturor meta-datelor și

evenimentelor de acces, LexChain asigură că entitățile din sectorul public pot schimba informații cu control deplin, fără a depinde de intermediari centrali. Sistemul sprijină interoperabilitatea între nivelurile administrative, menținând în același timp conformitatea cu cerințele de confidențialitate și audit. Această contribuție demonstrează modul în care arhitecturile bazate pe blockchain pot consolida încrederea digitală, transparența și coordonarea în structurile de guvernanță multi-nivel.

Cuvinte-cheie: *blockchain, contracte inteligente, e-Guvernare, identitate descentralizată, inovație în sectorul public, interoperabilitate.*

1. Introduction

The digital transformation of government services is no longer a distant objective but a present-day reality. The platforms, systems, and technologies employed for data management and service delivery enable convenient access from any location, significantly reducing both time and operational costs.

From an operational standpoint, digitalization offers numerous advantages; however, it also significantly increases the risks associated with the security of governmental data. Such data frequently includes sensitive information, most notably citizens' personal data, which requires enhanced protection measures.

Ensuring the security of digital platforms is fundamental to effective e-Governance, as it safeguards the confidentiality, integrity, and dependability of the electronic systems responsible for managing and delivering public services [1]. Similar concerns regarding increased cyber exposure have been documented in educational and public-sector environments, where the rapid transition to digital platforms significantly expanded the attack surface and required new governance measures [2,3].

Within this context, the notion of multi-level governance (MLG) is particularly relevant, as it denotes a distributed model of authority in which responsibilities are allocated both vertically—across local, regional, national, and supranational levels—and horizontally, engaging actors from the public sector, private markets, and civil society [4]. Consequently, interoperability emerges as a critical enabler of effective e-Governance. In this interconnected environment, security is no longer confined to individual standalone systems but extends to the entire network of platforms involved in data exchange. While each system may have distinct security requirements, their interconnection amplifies the overall exposure, thereby exponentially increasing the need for integrated and coordinated security measures. Interoperability in digital governance denotes the capacity of diverse information systems and applications employed within public administration to seamlessly communicate, share data, and operate collaboratively in a consistent and efficient manner [5].

Significant security challenges arise in relation to all three core principles of cybersecurity—confidentiality, integrity, and availability—particularly when it comes to the protection of governmental data. Previous studies on cybersecurity governance in Moldova have highlighted the fragmentation of security controls across sectors and the lack of robust data-sharing mechanisms, which reinforces the need for integrated architectures such as LexChain [6,7].

Confidentiality is essential to ensure that data is accessible exclusively to authorized users. This encompasses not only data encryption but also access control mechanisms, which are fundamental components of data governance. Ensuring the confidentiality of data exchanged during digital transactions remains a critical concern [8], particularly when

sensitive or personal information is involved. Similar challenges were observed in Moldovan higher education and public-sector institutions, where confidentiality breaches and weak governance policies were among the most frequently identified risks [9,10]. Access control models in governmental contexts range from the least restrictive—Discretionary Access Control, where individuals, as clients of government platforms, voluntarily grant access to their personal data—to the most stringent form, Mandatory Access Control, typically applied to the handling of classified information, such as secret or top-secret documents, managed by governmental entities and organizations.

Equally important in this context is data integrity, which ensures that documents remain unaltered by unauthorized or accidental modifications. The maintenance and assurance of data accuracy and consistency throughout a system's entire lifecycle are fundamental aspects of data integrity. Prior work on public-sector governance demonstrates that adopting structured frameworks such as ISO 27001 greatly improves consistency, auditability, and lifecycle management of sensitive data [3]. Given the probability of such events occurring in complex digital ecosystems, preserving integrity is essential for sustaining trust in public administration and ensuring both legal compliance and procedural transparency [11].

Additionally, data must remain accessible to both citizens and governmental authorities at the moment of request. If data is to be useful, it must be available to the right stakeholders at the right time [12]. Thus, availability constitutes a critical pillar of cybersecurity in digital governance. Ensuring high availability depends on factors such as system robustness, data redundancy, and minimal latency. Prior studies have shown that service availability issues remain among the most disruptive problems for public institutions and Small and Medium-sized Enterprises (SMEs), often caused by inadequate infrastructure segmentation and insufficient monitoring [13,14]. Any delays in accessing or exchanging information within these systems can result in significant disadvantages, undermining the efficiency and responsiveness of public services.

Therefore, placing security at the core of the design and deployment of digital governance infrastructures is imperative to guarantee secure, reliable, and interoperable data exchange across administrative entities [15].

In light of these security imperatives, it becomes essential to critically assess the underlying platforms and infrastructures employed in public sector governance, particularly those responsible for storing, processing, and exchanging sensitive data.

Digital platforms, in general, can be classified into centralized, distributed, and decentralized architectures, each offering distinct advantages and trade-offs in terms of control, scalability, fault tolerance, and security. Centralized platforms commonly employed to disseminate information across various locations, governmental entities, and end-users are predominantly based on cloud infrastructure [16].

Centralized cloud platforms are widely adopted in public administration due to their scalability, cost efficiency, and simplified infrastructure management. They offer built-in redundancy and robust compliance support. However, their centralized nature introduces risks such as vendor lock-in, limited transparency, and reduced control over data localization and access policies [17]. These limitations become especially problematic in multi-level governance, where fine-grained control and auditability are essential. Similar structural limitations were observed in the management of information systems within Moldovan SMEs, where centralized infrastructures lacked resilience and fine-grained control [13].

Distributed systems offer improved fault tolerance, scalability, and data locality, making them attractive for public sector applications where reliability and resilience are essential [18]. By decentralizing processing and storage, these systems reduce single points of failure and allow local governance units to retain control over their data. While distributed models enhance resilience and local autonomy in digital governance, they also introduce new governance challenges. These include increased coordination complexity, fragmented accountability structures, and the need for robust interoperability standards [19].

Although decentralized platforms, such as blockchain-based systems, provide benefits like immutable audit trails and reduced dependence on central authorities, they also face important limitations—including scalability issues, regulatory challenges, and limited interoperability with existing governmental infrastructures [20].

To address these limitations, this paper proposes LexChain—a hybrid decentralized platform that combines blockchain-based metadata governance with adaptive encrypted cloud storage, specifically tailored for secure and interoperable data sharing in multi-level digital governance.

The next section reviews relevant literature and existing approaches related to secure and interoperable data sharing in digital governance. This is followed by the presentation of our proposed solution, LexChain, along with its architectural design and implementation details.

2. Related Work

Recent research in digital governance emphasizes the importance of secure, interoperable frameworks capable of ensuring data confidentiality, integrity, and availability across institutional and jurisdictional boundaries. In this context, blockchain technology has emerged as a promising enabler for decentralized and tamper-resistant record management, while cryptographic and AI-based methods increasingly support privacy preservation and intrusion detection.

In contrast to conventional centralized e-Government systems, which are prone to privacy breaches and single points of failure, the framework proposed by Elisa et al. [21] introduces a decentralized architecture that integrates blockchain for secure data handling and an artificial immune system (AIS) for adaptive threat detection. The AIS module enhances the resilience of blockchain transactions by mitigating both insider and external attacks, while the blockchain ensures encryption, validation, and immutability.

Malik et al. [1] proposed a secure platform for digital governance interoperability and data exchange by integrating blockchain with deep learning techniques. Their model combines a Bonobo optimization algorithm for trust scoring and data source authentication, a lightweight Feistel structure for dual-layer privacy preservation, and a deep reinforcement learning (DRL) model for intrusion detection.

To address the challenges of privacy and security in open government data (OGD) sharing, a federated learning-based framework was proposed by Xingsen Zhang [22] that models the OGD ecosystem through four distinct participant roles: data providers, collectors, operators, and users. The framework incorporates horizontal, vertical, and transfer federated learning schemes to enable collaborative analytics without direct data exposure. Applied to real-world scenarios, the approach effectively mitigates information leakage risks and enhances model security, offering a scalable solution for secure and privacy-preserving government data governance.

To address persistent shortcomings in integrating interoperability, secure data exchange, and adaptive risk governance in digital public services, the Government Adaptive

Unified Cybersecurity Holistic Orchestration framework was proposed in [23]. This comprehensive model combines an adaptive risk management methodology based on Metodología de Análisis y Gestión de Riesgos de Seguridad de la Información (MARISMA), providing a structured and standards-aligned approach to evaluating and mitigating security risks, an X-Road-inspired secure interoperability layer, and a strategic cybersecurity governance component. The framework aims to protect e-Government ecosystems holistically, with a focus on citizen-centric design, sustainability, and regulatory compliance.

To address the limitations of traditional IT risk assessment methods in the context of cyber-physical systems (CPSs), a novel technique named MARISMA-CPS was proposed in [24]. Built upon the MARISMA security management methodology and the eMARISMA cloud-based environment, the approach introduces a reusable and adaptable risk assessment pattern tailored specifically for CPSs. The pattern aligns with leading frameworks such as NIST and ENISA and supports dynamic risk analysis across various CPS domains. By enabling modular adaptation to systems like smart hospitals, the method ensures broad applicability and scalability for critical infrastructures with tightly coupled cyber and physical components.

An illustrative example of blockchain-supported interoperability is presented by Ren et al. [25], where the authors propose a data-sharing mechanism for the mineral resource sector. The framework addresses the fragmentation of data sources and the lack of trust between stakeholders by enabling verifiable, decentralized data exchange. Compared to conventional sharing models, it improves data quality assurance, secures intellectual property, and facilitates cooperation among independent entities. This approach demonstrates how blockchain can be leveraged to establish interoperable environments across siloed institutional systems.

A blockchain-based proxy re-encryption framework for e-healthcare data sharing is introduced in [26], addressing the limitations of existing conditional proxy re-encryption (CPRE) schemes. The proposed solution enables fine-grained, condition-based data access control while hiding the condition itself from the proxy, preserving privacy. In addition, smart contracts are employed to validate the completeness and correctness of the re-encryption results, ensuring trustworthy data exchange across institutions. This architecture exemplifies how blockchain and cryptographic enforcement mechanisms can support inter-institutional interoperability without compromising data confidentiality.

The system further [27] enhances trust by combining CPRE with smart contract enforcement, ensuring that access conditions remain confidential and that the proxy cannot infer sensitive attributes. Unlike traditional CPRE models, this approach supports condition invisibility, thus preventing leakage of access logic or policy. The use of blockchain not only enables auditable ciphertext searching but also guarantees result integrity through verifiable execution. Such integration of privacy-preserving re-encryption and decentralized validation illustrates a compelling method for secure, cross-organizational data interoperability, particularly in sensitive domains like healthcare.

Building on similar efforts to secure e-healthcare data through blockchain-enabled re-encryption, another approach [28] introduces a proxy re-encryption-based Electronic Health Record (EHR) management system that decouples the re-encryption server from the blockchain infrastructure. Unlike the condition-invisible CPRE scheme discussed earlier, which focused on fine-grained access with hidden policies, this model emphasizes architectural separation to prevent outsourced blockchain service providers from accessing sensitive health records. Here, the proxy server operates strictly between file servers,

enabling efficient ciphertext transformation without exposing plaintext to untrusted infrastructure. Access control is enforced through smart contracts on-chain, ensuring that data-sharing remains both secure and auditable. Taken together, these solutions demonstrate a growing convergence around re-encryption, decentralization, and contract-based policy enforcement as foundational design principles for secure and interoperable data ecosystems.

Overall, the surveyed frameworks converge on several key architectural principles: the use of blockchain as a decentralized trust anchor, the incorporation of cryptographic primitives for fine-grained and privacy-preserving access control (e.g., Conditional Proxy Re-Encryption, Ciphertext-Policy Attribute-Based Encryption CP-ABE), and the reliance on smart contracts for verifiable policy enforcement. Whether addressing public governance, healthcare, or critical infrastructure, these solutions aim to reconcile interoperability with security, each proposing domain-specific adaptations such as federated learning for OGD, multi-authority control in CP-ABE, or proxy isolation for outsourced blockchain infrastructures.

However, despite this progress, few frameworks succeed in unifying cross-institutional interoperability, scalable data access control, and auditability within a single cohesive architecture applicable to multi-level government ecosystems. This gap is addressed by LexChain, which introduces a hybrid blockchain–cloud architecture featuring adaptive data fragmentation, end-to-end encryption using Ethereum-derived keys, and smart-contract-based permission management. In contrast to existing sector-specific solutions, LexChain is designed explicitly for secure data sharing across administrative boundaries, supporting both horizontal (intra-level) and vertical (inter-level) collaboration through decentralized identity (LexID), re-encryption per recipient, and transparent access history anchored on a permissioned blockchain. As such, LexChain contributes a generalized yet operationally grounded model for secure and interoperable digital governance.

None of the reviewed frameworks fully address interoperability and policy-driven access control and cloud-scalability and blockchain auditability in a single unified architecture.

3. Proposed Framework

Building on the limitations identified in previous frameworks and guided by requirements specific to multi-level governance environments, we propose LexChain—a hybrid, permissioned blockchain-based system that enables secure, auditable, and fine-grained data sharing across institutional boundaries.

3.1. Overview of System Design

LexChain is a hybrid and permissioned platform designed to enable secure and interoperable data exchange across different administrative levels. It integrates a private Ethereum-based blockchain, using the IBFT2 consensus protocol, to ensure tamper-proof metadata registration and auditable access control. In parallel, encrypted file fragments are stored in public cloud infrastructures such as Google Drive or OneDrive, enabling scalable and distributed storage.

The use of a private Ethereum network is justified by its demonstrated capabilities to support smart contract automation, data integrity assurance, and chain-of-custody preservation, as shown in both digital governance solutions [1] and blockchain-based forensic systems [29]. These features are fundamental for building trustworthy data-sharing

frameworks in e-Government environments, where legal compliance, transparency, and auditability are essential.

LexChain consists of four core modules:

- the LexUser interface, which includes a browser and digital wallet (LexID),
- a client-side SecureFileManager responsible for local processing,
- the LexChain blockchain for immutable recordkeeping,
- and a smart contract layer that governs access control and permissions.

The interaction between these components is illustrated in Figure 1, which presents the general architecture of the platform and the logic of secure document sharing.

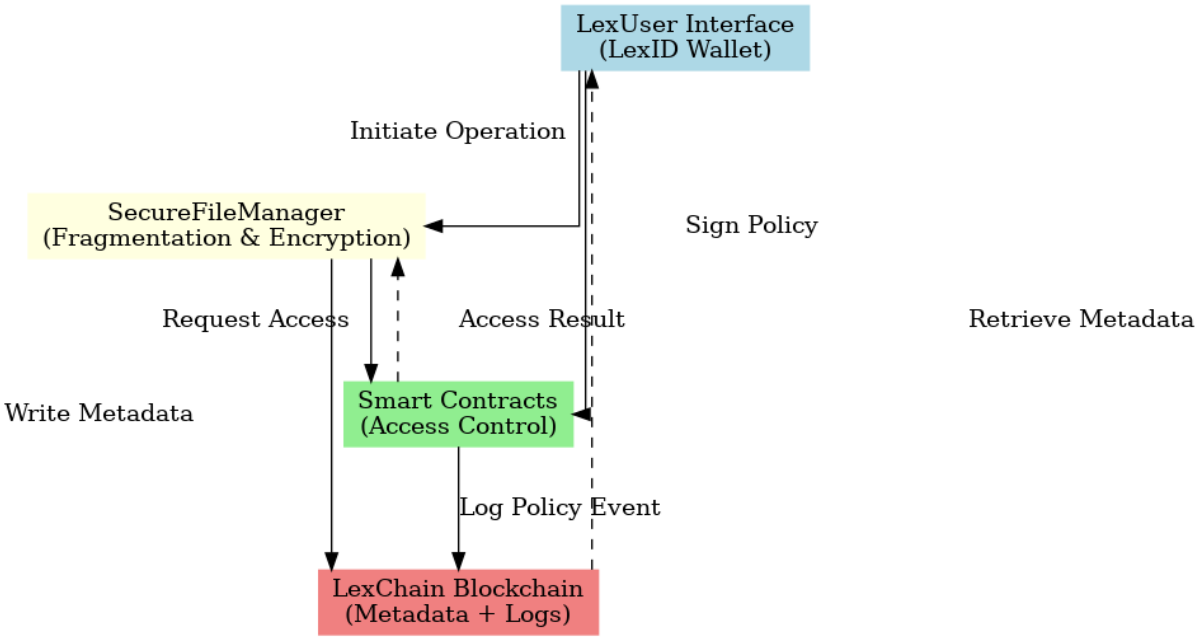

Figure 1. Component interaction in the LexChain architecture.

3.2. Data Fragmentation and Encryption

In LexChain, sensitive documents are protected through a two-step process that takes place entirely on the user's device, before any data is uploaded to external systems. First, each file is divided into smaller, manageable fragments. This fragmentation allows for more flexible storage across multiple cloud services and reduces the impact of potential data breaches. Kapusta and Memmi identify fragmentation as a fundamental architectural requirement, combined with encryption and dispersion, to protect sensitive information even when the underlying infrastructure is compromised [30]. Moreover, a recently validated algorithm in multi-cloud environments demonstrates that fragmentation provides a robust level of security against unauthorized access [31].

Next, every fragment is individually encrypted using a secure and widely adopted encryption method (AES-256). The encryption key is not stored anywhere; instead, it is derived from the user's digital identity (LexID). LexID can be regarded as a practical implementation of a Decentralized Identifier (DID) within a permissioned blockchain ecosystem, offering support for smart contract-based policy enforcement and trustless authentication. By eliminating reliance on centralized identity providers, LexID enables secure and verifiable interactions across institutional boundaries while preserving user autonomy and cryptographic integrity. This approach ensures that only the rightful user can access the data, without relying on central authorities or key distribution services.

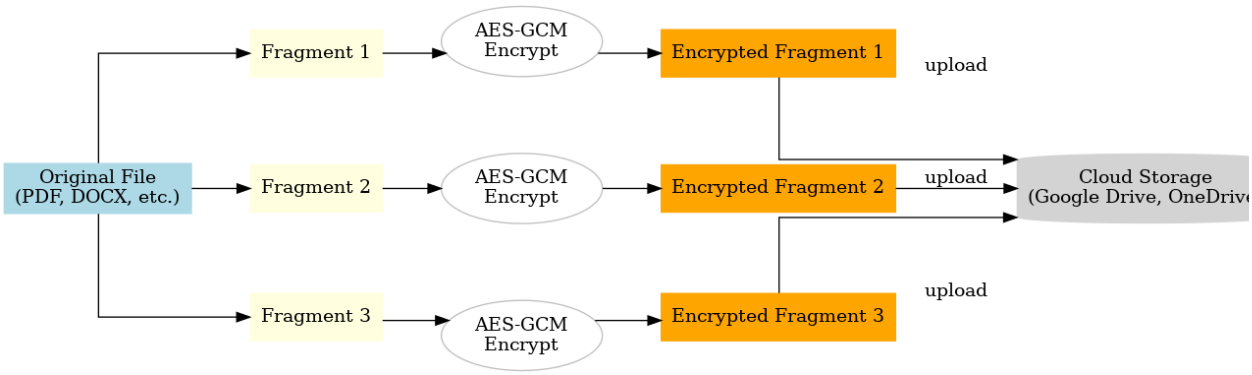

Figure 1. Fragmentation and encryption process in LexChain.

By combining fragmentation, encryption, and decentralized identity, LexChain ensures that:

- Cloud providers cannot read or reconstruct the original data;
- Access remains under the user's control, even after sharing;
- Public institutions can confidently store and exchange information, knowing it remains protected end-to-end.

This method aligns with the principles of zero-trust architecture and enables secure, scalable, and privacy-respecting data sharing across administrative levels.

4. Identity Management and Policy Enforcement

At the core of LexChain's decentralized access model lies LexID, a self-sovereign identity mechanism implemented as a browser-based wallet. Each user is uniquely identified by their Ethereum-compatible public address, which serves as both an access token and a cryptographic anchor for operations such as encryption, decryption, and transaction signing. LexID aligns with the W3C Decentralized Identifier (DID) model, where an entity can prove control over a self-issued identifier without relying on a centralized authority. DIDs are typically anchored to distributed ledgers, enabling tamper-proof and publicly verifiable identity references. Moreover, governance policies over DIDs can be deployed via smart contracts, as shown by recent research emphasizing the critical role of distributed authorization mechanisms in cross-domain deployments [32].

LexID eliminates the need for centralized identity providers, placing control directly in the hands of the user. The private key associated with each LexID remains strictly local, while the public key is used on-chain to validate access and permission transactions. This setup enables privacy-preserving authentication and non-repudiable audit trails without revealing personal information.

Access control and policy enforcement are handled through a suite of smart contracts deployed on the LexChain blockchain. These contracts govern who can access a file, under what conditions, and ensure that every transaction is auditable and verifiable.

The high-level identity and access workflow is illustrated in Figure 3. A LexUser encrypts and fragments files locally, uploads them to cloud storage, and registers metadata and policies on-chain. Smart contracts enforce access control rules, while authorized recipients (also identified via LexID) can request access. The blockchain verifies the policy and grants decryption rights accordingly.

Every operation—whether uploading a document, sharing it with another institution, or accessing a shared resource—is immutably recorded via smart contracts. These contracts not only enforce permission logic but also act as an auditable ledger of all data-sharing activities.

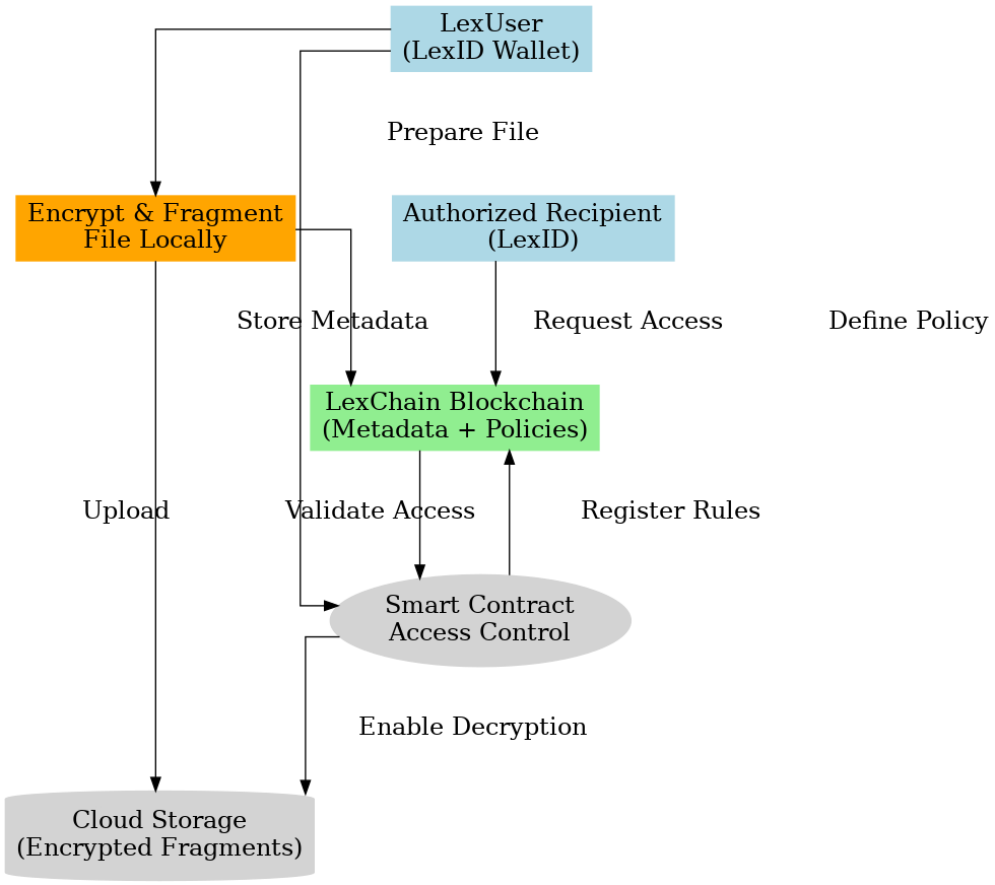

Figure 2. Workflow of identity-based access control and policy enforcement using LexID and smart contracts in LexChain.

The integration of emerging technologies such as Blockchain 3.0 and Artificial Intelligence (AI) is transforming how governments deliver secure, transparent, and citizen-centric services. As highlighted by recent studies, smart contracts on blockchain platforms enable authenticity, auditability, and scalability in critical sectors such as energy and healthcare, where AI agents and blockchain logic interact to automate and validate service transactions [33].

Together, LexID and smart contracts form the foundation of LexChain's security and interoperability model, enabling traceable, rule-based collaboration between stakeholders in a multi-level e-Governance ecosystem.

5. Conclusions

This paper presented LexChain, a decentralized framework tailored for secure and auditable data sharing across public institutions in multi-level governance settings. By combining a private Ethereum-based blockchain, decentralized identity (LexID), and smart contract–driven access control, LexChain addresses critical requirements such as confidentiality, interoperability, and traceability.

The architecture allows institutions to retain full control over encrypted data, while smart contracts enforce sharing policies transparently and verifiably. This enables trusted collaboration between local, regional, and national administrations—without relying on central intermediaries.

LexChain demonstrates how blockchain technologies can be effectively applied beyond financial use cases, supporting secure public data exchange aligned with EU digital governance principles and data sovereignty goals.

Further work will explore deployment scenarios in justice, digital archives, and cross-border services, as well as integration with national eID systems.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Malik, V.; Mittal, R.; Mavaluru, D.; Narapureddy, B.R.; Goyal, S.B.; Martin, R.J.; Srinivasan, K.; Mittal, A. Building a Secure Platform for Digital Governance Interoperability and Data Exchange Using Blockchain and Deep Learning-Based Frameworks. *IEEE Access* 2023, 11, pp. 70110–70131. https://doi.org/10.1109/ACCESS.2023.3293529.
2. Alexei, A.; Alexei, A. Cyber security threat analysis in higher education institutions as a result of distance learning. *Int. J. Sci. Technol. Res.* 2021, 10(3), pp. 128-133.
3. Alexei, A. Ensuring information security in public organizations in the Republic of Moldova through the ISO 27001 standard. *J. Soc. Sci.* 2021, 4(1), 11. https://doi.org/10.52326/jss.utm.2021.4(1).11.
4. Daniell, K.A.; Kay, A. Multi-Level Governance: An Introduction. In: *Multi-Level Governance: Conceptual Challenges and Case Studies from Australia*. ANU Press, Canberra, Australia, 2017, pp. 3–32. https://doi.org/10.22459/MG.11.2017.01.
5. Jimenez, C.E.; Criado, J.I.; Gasco, M. Technological e-Government Interoperability: An Analysis of IberoAmerican Countries. *IEEE Lat. Am. Trans.* 2011, 9(7), pp. 1112–1117. https://doi.org/10.1109/TLA.2011.6129711.
6. Alexei, A.; Nistiriuc, P.; Alexei, A. The holistic approach to cybersecurity in academia. In: *Proceedings of the Central and Eastern European e|Dem and e|Gov Days 2022* (CEE eGov 2022). Budapest, Hungary, 22–23 September 2022; ACM, New York, USA, 2022, pp. 106–111. https://doi.org/10.1145/3551504.3551516.
7. Alexei, A. Design and development of a cybersecurity conceptual framework for higher education institutions in the Republic of Moldova. *Sci. Pract. Cyber Secur. J. (SPCSJ)* 2022, 6(1), pp. 35–52.
8. Posch, R.; Leitold, H. Identification and Confidentiality for E-Government. In: *Communications and Multimedia Security*; Katsikas, S.K.; Gritzalis, D.; Preneel, B., Eds. Springer, Boston, MA, USA, 2003, pp. 267–279. https://doi.org/10.1007/978-0-387-35696-9_17.
9. Alexei, A.; Nistiriuc, P.; Alexei, A. Empirical study of cyber security threats in Moldovan higher education institutions. In: *Proceedings of the 12th International Conference on Electronics, Communications and Computing (ICECCO 2021)*, Technical University of Moldova, Chisinau, Moldova, 2021, pp. 1–6.
10. Alexei, A.; Alexei, A. The difference between cyber security vs information security. *J. Eng. Sci.* 2022, 29(4), pp. 72–83. https://doi.org/10.52326/jes.utm.2022.29(4).08.
11. Santhosh Kumar, B. Introductory Chapter: Data Integrity and Data Governance. In *Data Integrity and Data Governance*. IntechOpen, London, UK, 2023. https://doi.org/10.5772/intechopen.110399.
12. Walsh, M.J.; McAvoy, J.; Sammon, D. The Data Governance Journey in Practice: Insights from Case Study Research. *Inf. Syst. Manag.* 2025, 42(3), pp. 471–488. https://doi.org/10.1080/10580530.2025.2477459.
13. Alexei, A.; Alexei, A. The problem of information systems security in SME. In: *Proceedings of the Central and Eastern European e|Dem and e|Gov Days 2023*. ACM, New York, USA, 2023, pp. 101–105. https://doi.org/10.1145/3603304.3603346.
14. Alexei, A.; Moraru, V.; Alexei, A. Securing Moldovan small and medium-sized businesses: Strategies based on IT infrastructure domains. *J. Eng. Sci.* 2025, 32(2), pp. 75–86. https://doi.org/10.52326/jes.utm.2025.32(2).07.
15. Kumar, P.; Gupta, G.P.; Tripathi, R. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for Sustainable Smart Cities by Leveraging Blockchain and Machine Learning. *J. Syst. Archit.* 2021, 115, 101954. https://doi.org/10.1016/j.sysarc.2020.101954.
16. Brzozowska-Rup, K.; Nowakowska, M.; Zdradzisz, M. Cloud Computing in the Polish Public Administration: Current State and Development Prospects. *Technol. Forecast. Soc. Change* 2024, 205, 123500. https://doi.org/10.1016/j.techfore.2024.123500.
17. Assaf, A.; IisHamsir, A.W.; Muhammad, M. Benefits and Risks of Cloud Computing in E-Government Tasks: A Systematic Review. *E3S Web Conf.* 2021, 328, 04005. https://doi.org/10.1051/e3sconf/202132804005.
18. van Steen, M.; Tanenbaum, A.S. A Brief Introduction to Distributed Systems. *Computing* 2016, 98(10), pp. 967–1009. https://doi.org/10.1007/s00607-016-0508-7.
19. Vergne, J. Decentralized vs. Distributed Organization: Blockchain, Machine Learning and the Future of the Digital Platform. Organ. *Theory* 2020, 1(4). https://doi.org/10.1177/2631787720977052.

20. Kassen, M. Blockchain and E-Government Innovation: Automation of Public Information Processes. *Inf. Syst.* 2022, 103, 101862. https://doi.org/10.1016/j.is.2021.101862.
21. Elisa, N.; Yang, L.; Chao, F.; Naik, N.; Boongoen, T. A Secure and Privacy-Preserving E-Government Framework Using Blockchain and Artificial Immunity. *IEEE Access* 2023, 11, pp. 8773–8789. https://doi.org/10.1109/ACCESS.2023.3239814.
22. Zhang, X. A More Secure Framework for Open Government Data Sharing Based on Federated Learning. *Gov. Inf. Q.* 2024, 41(4), 101981. https://doi.org/10.1016/j.giq.2024.101981.
23. Figueroa, V.; Sánchez Crespo, L.E.; Santos-Olmo, A.; Rosado, D.G.; Fernández-Medina, E. Building a Holistic Cybersecurity Framework for E-Government Based on a Systematic Analysis of Proposals. *Int. J. Inf. Secur.* 2025, 24(3), 121. https://doi.org/10.1007/s10207-025-01024.
24. Rosado, D.G.; Caballero, I.; Gutiérrez, C.; et al. Managing Cybersecurity Risks of Cyber-Physical Systems: The MARISMA-CPS Pattern. *Comput. Ind.* 2022, 142, 103715. https://doi.org/10.1016/j.compind.2022.103715.
25. Ren, Y.; Liang, J.; Su, J.; Cao, G.; Liu, H. Data Sharing Mechanism of Various Mineral Resources Based on Blockchain. *Front. Eng. Manag.* 2020, 7(4), pp. 592–604. https://doi.org/10.1007/s42524-020-0132-2.
26. Lin, G.; Wang, H.; Wan, J.; Zhang, L.; Huang, J. A Blockchain-Based Fine-Grained Data Sharing Scheme for E-Healthcare System. *J. Syst. Archit.* 2022, 132, 102731. https://doi.org/10.1016/j.sysarc.2022.102731.
27. Zhang, X.; Du, W.; Moshayedi, A.J. A Traceable and Revocable Multi-Authority Attribute-Based Access Control Scheme for Mineral Industry Data Secure Storage in Blockchain. *J. Supercomput.* 2023, 79(13), pp. 14743–14779. https://doi.org/10.1007/s11227-023-05222-2.
28. Park, Y.-H.; Kim, Y.; Lee, S.-O.; Ko, K. Secure Outsourced Blockchain-Based Medical Data Sharing System Using Proxy Re-Encryption. *Appl. Sci.* 2021, 11(20), 9422. https://doi.org/10.3390/app11209422.
29. Zarpala, L.; Casino, F. A Blockchain-Based Forensic Model for Financial Crime Investigation: The Embezzlement Scenario. *Digit. Finance* 2021, 3(3–4), pp. 301–332. https://doi.org/10.1007/s42521-021-00035-5.
30. Kapusta, K.; Memmi, G. Data Protection by Means of Fragmentation in Various Different Distributed Storage Systems: A Survey. arXiv preprint 2017, arXiv:1706.05719.
31. Nabawy, R.M.; Hassanin, M.; Ibrahim, M.H.; Kaseb, M.R. Mixed Fragmentation Technique for Securing Structured Data Using Multi-Cloud Environment (MFT-SSD). *Ad Hoc Netw.* 2024, 164, 103625. https://doi.org/10.1016/j.adhoc.2024.103625.
32. Garzon, S.R.; Segat, C.; Küpper, A. Governance of Ledger-Anchored Decentralized Identifiers. In: *Proceedings of the 2025 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, IEEE, NY, USA, 2025.
33. Terzi, S.; Votis, K.; Tzovaras, D.; Stamelos, I.; Cooper, K. Blockchain 3.0 Smart Contracts in E-Government 3.0 Applications. In: *Proceedings of the 2019 IEEE International Conference on Computer, Information and Telecommunication Systems (CITS)*, IEEE, Beijing, China, 2019.

Citation: Alexei, A.; Moraru, V.; Alexei, A.; Bistritchi, S.; Manole, A. Data governance in the public sector with lexchain: a hybrid blockchain-cloud architecture proposal. Journal of Social Sciences, 8 (4), pp. 202-212. https://doi.org/10.52326/jss.utm.2025.8(4).13.

Submission of manuscripts: *jes@meridian.utm.md*