applied sciences

MDPI

Article

Transparent Digital Governance: A Blockchain-Based Workflow Audit Application

Constantin Viorel Marian, Dan Alexandru Mitrea, Dinu Stefan Rusu and Andrei Vasilateanu *

Department of Engineering in Foreign Languages, National University of Science and Technology Politehnica Bucuresti, RO-060042 Bucharest, Romania; constantin.marian@upb.ro (C.V.M.); alexandru.mitrea@upb.ro (D.A.M.); dinu_stefan.rusu@upb.ro (D.S.R.)
* Correspondence: andrei.vasilateanu@upb.ro

Featured Application

An innovative blockchain-based software system for monitoring document flows in central and local administration, with a focus on legislative process.

Abstract

Digital governance requires transparent, auditable, and secure mechanisms for document circulation across public institutions. Existing workflow management and e-government systems, especially in the legislative field, often lack end-to-end auditability, leaving gaps in accountability and verification. This article introduces a blockchain-based workflow audit application designed to ensure integrity, traceability, and transparency of document exchanges and transitions in central and local administrations. This article presents a solution that oversees the auditing and monitoring of document circulation between different public institutions or within a single institution. The system is based on blockchain technology that stores data and preserves history, making every action traceable and auditable. The process of document creation involves the encryption, timestamping and addition of the document to the blockchain, the access to which is restricted only to authorised stakeholders. The system aims to enhance transparency and accuracy in the presentation of legislative process documents for public consultation. The preliminary prototype was subjected to a validation process by an end-user from the parliamentary legislative authority in Romania.

Keywords: blockchain; distributed ledger technology; digital governance; verifiable credentials

check for updates

Academic Editor: Gianluca Lax

Received: 25 September 2025
Revised: 23 October 2025
Accepted: 29 October 2025
Published: 1 November 2025

Citation: Marian, C.V.; Mitrea, D.A.; Rusu, D.S.; Vasilateanu, A. Transparent Digital Governance: A Blockchain-Based Workflow Audit Application. *Appl. Sci.* **2025**, *15*, 11694. https://doi.org/10.3390/app152111694

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

E-government can be seen as a collection of individuals, processing tools and procedures, communication subsystems, software applications, and user and/or organization data. This set of diverse information is used under strict policies to gather, retrieve, process, and distribute information inside and outside any organization, which is seen as a closed information system. It is important to mention the specific and precise order of interaction between any information system elements [1]. Electronic government (e-government) is the utilization of digital technologies and online platforms to improve the exchange of information, to enhance the delivery of government services, and foster engagement with citizens, businesses, and other stakeholders. It includes a wide range of digital and web-based programs aimed at improving the effectiveness, accessibility, and openness of

government functions [2,3]. The objective of e-government is twofold: to enhance accessibility to government services for citizens and to optimize operational procedures. Thus, government services are improved through transparent access to public data [4]. The ultimate goal of these efforts is to foster a more engaged and informed society.

E-government encompasses a number of key elements that are concurrently being developed. The concept of Digital Service Delivery enables citizens to access a range of government services and information online, including the ability to apply for permits, pay taxes, or access healthcare services. Online portals and websites represent a significant aspect of e-government. Governments provide centralized online portals that enable citizens to access information, submit forms, and interact with government agencies. Digital identity and authentication are an essential aspect of e-government and they include digital identity systems for secure authentication when accessing government services online. Digital identity systems provide valid, secure and reliable information, replacing human identities with digital data [5]. The concept of Open Data and Transparency encompasses the act of making government data accessible to the public in formats that are open and readily available. Digital Communication and Engagement, on the other hand, refers to the utilization of digital platforms for the purpose of engaging with citizens and eliciting feedback on policies and services. E-Government Infrastructure, in turn, represents the technological frameworks that facilitate the delivery of online services, including secure networks and cloud computing platforms. Finally, the domain of Cybersecurity and Data Protection is concerned with the protection of sensitive information and the mitigation of cyber threats [6,7]. The use of cryptographic systems with public keys is now pervasive in digital signatures, despite the system's limitations [8].

Open Data and Transparency, a common practice for e-government initiatives, includes the release of government datasets to the public. Such transparency fosters accountability and enables citizens, researchers, and private entities to utilize the data for a multitude of purposes, including the development of applications or the conduct of analyses. Digital Communication and Engagement through digital platforms facilitate communication between the government and the general public. These may include social media platforms, forums and feedback tools which enable direct interaction and allow governments to gather input on proposed policies and initiatives.

An overview of the legislative process in Romania will be presented to understand how a software system based on blockchain technology can be implemented to support it. For a law to be adopted, several steps must be completed:

1. Legislative Initiative: The process begins with the legislative initiative, which can be proposed by the Government, members of Parliament (deputies or senators), or by at least 100,000 citizens with voting rights.
2. Submission to Parliament: The proposed bill is submitted to the Parliament. It is first reviewed by the chamber that has primary jurisdiction over the subject matter, which could be either the Senate or the Chamber of Deputies.
3. Committee Review: The bill is assigned to relevant parliamentary committees for detailed examination. These committees analyze the bill, hold hearings, and may suggest amendments.
4. Debate and Voting in the First Chamber: The bill is debated in the first chamber (either the Senate or the Chamber of Deputies). Members discuss the bill and vote on it. If the bill is approved, it will proceed to the other chamber.
5. Review by the Second Chamber: The second chamber reviews the bill, following a similar process of committee review, debate, and voting. Both chambers must approve the bill in the same form.

6. Conference Committee: If there are differences between the versions passed by each chamber, a conference committee made up of members from both chambers works to reconcile the differences. Subsequently, the revised bill is transmitted back to both chambers for final approval. After that, the amended bill is returned to both chambers where the bill is discussed before the final voting session and approval.
7. Promulgation by the President: Once both chambers pass the final version of the bill, it is sent to the President of Romania for promulgation. The President can sign the bill into law, request a review, or send it back to Parliament for reconsideration.
8. Publication: After the President signs the bill, it is published in the Official Journal/Gazette of Romania and becomes law.

This process ensures that proposed laws are thoroughly reviewed and debated before being enacted. Taking into consideration existing research, such as [9], blockchain technology is a transformative force in the domain of auditing, thereby facilitating greater transparency, security, and efficiency. It provides auditors with the means to manage the digital environment and conduct high quality audits.

This paper introduces an innovative software system built on distributed ledger technology (DLT), designed for deployment within the public sector, particularly in central and local public administrations (e.g., county councils, city halls, government bodies). The system provides a comprehensive solution for auditing and monitoring document circulation both within and between public institutions. It also supports interoperability with private institutions, even when differing document workflows are involved. The platform operates on a unified blockchain that records only the final versions of documents, while maintaining a complete history to ensure full traceability and auditability. Each document is encrypted, timestamped, and added to the blockchain, with access restricted to authorized users. Key features include real-time auditing and external accessibility for verifying the authenticity of legislative documents, thereby enhancing transparency and precision in presenting legal texts for public consultation. Additionally, the system is well-suited for use in legal offices and professional legal environments.

The study investigates three research questions: (RQ1) how a blockchain-based audit layer can be designed to ensure end-to-end traceability of legislative document workflows, including intermediate drafts, while maintaining compliance with existing workflows, (RQ2) how a blockchain-enabled web application can be designed to deliver verifiable, real-time insights into legislative processes and (RQ3) how smart contracts that govern workflow events can be subjected to verification and validation to guarantee functional correctness and adherence to legislative process constraints. The answers to these questions form the foundation of our proposed system and highlight its novelty within the field of blockchain-based governance applications. This study follows the Design Science Research (DSR) methodology as outlined in [10], which is particularly suitable for projects that aim to create and evaluate innovative IT artifacts. The DSR paradigm ensures that the development of the artifact is both relevant to a real-world problem and rigorously evaluated in a scientifically defensible manner. The choice of DSR is motivated by the need to address a concrete problem in public governance—insufficient traceability and transparency in legislative processes—through the design of a novel blockchain-based audit system, while ensuring that the resulting artifact is systematically validated against technical, legal, and usability criteria. The research process followed the six activities of DSR:

1. Identify problem and motivate: The research identified areas in the Romanian legislative process that could benefit from increased transparency, such as capturing comments from commissions at each phase. Existing publication practices, such as the Official Journal, only provide final versions without verifiable histories or real-time visibility.

2. Define Objectives of a Solution: Objectives were derived from domain analysis and stakeholder needs: ensuring end-to-end traceability of legislative documents, including intermediate drafts and providing real-time, verifiable transparency for external monitoring organizations. These objectives were constrained by respecting the existing workflow in the Parliament.
3. Design and Development: The artifact consists of a blockchain audit layer built on Ethereum, a monitoring interface, and a suite of smart contracts for storing intermediate stages of the laws.
4. Demonstration: The system was deployed and tested in a simulated Romanian parliamentary workflow scenario, going through all the stages in the first chamber. Observers could access real-time audit data through the monitoring interface, demonstrating the transparency mechanism in practice.
5. Evaluation: Functional and usability assessment was done by domain experts from the Parliament, interviewed for the study. Smart contract validation-workflow logic was tested using automated unit tests in Hardhat, runtime event inspection via Chainlens, and static code analysis to ensure security and correctness.
6. Communication: Results are communicated to both academic and practitioner communities through this article.

By following DSR, the research not only produces a functional system but also delivers a rigorously validated contribution to the body of knowledge on blockchain applications in legislative processes.

Two prototypes are developed for this study. An initial prototype showcases a general document workflow using distributed ledger technologies, particularized for a journalist accreditation use case. A second, more complex system, is developed for supporting the legislative process workflow in Romanian Parliament.

A benefit of our system lies in the integration of a role-aware access control framework—combining Keycloak-based institutional authentication with smart-contract–level authorization—within a permissioned blockchain that remains publicly auditable. This dual-layer design ensures that only verified institutional actors can record or attest legislative actions, while any external observer can transparently verify their integrity through the public audit interface.

The structure of the paper is as follows: Section 2 presents an overview of existing research and implementations in the use of DLT in administration; Section 3 presents the general document workflow customized for a particular use case; Section 4 presents the design and implementation using DLT of the application; Section 5 evaluates the results, from a performance point of view; Section 6 highlights the next stage of the implementation, involving a real legislative process in the Romanian Parliament; and Section 7 presents the conclusions.

2. Related Work

The backbone of e-government is information exchange, which provides a platform for secure data sharing and improved communication [11]. In the context of e-government, the most important benefits are those related to digital identity management, which includes the secure identification of individuals. The decentralized and immutable method of storing and verifying digital identities provided by blockchain reduces the risk of identity theft and fraud. In the context of the legislative process, the blockchain technology offers a more transparent and auditable means of accessing services. The blockchain facilitates the comprehensive and immutable documentation of all document transitions, thereby ensuring the integrity and verifiability of the process. Blockchain can enhance the efficiency, transparency, and security of various e-government functions. For our system we have

analyzed four different Blockchain technologies: Ethereum, Hyperledger Fabric, Exonum, and Corda. Ethereum was chosen as it is the chosen implementation for the European Blockchain Services Infrastructure (EBSI) [12] embraced by blockchain initiatives in Romania at Government level [13]. Moreover, Ethereum has an active community, allowing for easier integration with the Web 3.0 ecosystem and high security due to the distributed consensus mechanism. Hyperledger Fabric was also taken into consideration as it is frequently used in e-government use cases [14].

2.1. Blockchain Use Cases and Applications

Blockchain technology has started to find its place in the most important industries by improving traditional practices. By facilitating secure data exchange, blockchain technology supports the principles of the circular economy, which ultimately increases organizational efficiency [15]. Among the most important cutting-edge applications and trends are [16]: Digital Identity Management, Land Registry, Voting Systems, Supply Chain Management, Public Records, Taxation and Financial Management. The management of digital identities is a crucial aspect of modern digital governance. Governments are employing DLT to establish secure and verifiable digital identities for citizens. A unified infrastructure for verifiable credentials and decentralized identifiers deployed at scale depends on the interoperability of digital systems, institutional integration and compatibility with existing European strategies [17]. This facilitates the reduction of fraud and the streamlining of access to public services [18]. Blockchain technology is being employed to maintain land records that are resistant to alteration. Such measures guarantee transparency and mitigate the occurrence of disputes pertaining to land ownership [19]. Blockchain-based land registry, which integrates digital identities, simplifies acquisition processes and reduces the risk of fraud [20]. Blockchain-based voting systems are currently being tested to ensure secure, transparent, and tamper-proof elections [21,22]. Public administrations are employing DLT to monitor the supply chain of goods and services, thereby enhancing transparency and reducing corruption [23]. An example of a supply-chain management system is the monitoring of stamps produced and used to limit the release of counterfeit stamps into circulation [24]. The maintenance of public records, including birth and death certificates, marriage licenses, and other important documents, is being facilitated by the use of blockchain technology. This ensures the security and accessibility of these records, which are of significant importance to individuals and governments alike [25]. DLT has the potential to streamline tax collection and management, thereby reducing errors and increasing efficiency [26]. Using decentralized finance platforms, it is easier to access user data to estimate default risk more accurately than classical models [27].

In the public domain, the majority of extant blockchain deployments are related to citizen services, recordkeeping, or pilot voting—rather than direct legislative drafting or voting. Switzerland conducted one of the earliest municipal blockchain-based e-voting pilots in 2018, where residents could cast votes via mobile using a distributed system rather than a central server, increasing perceived simplicity and security [28]. In the U.S. (the state of West Virginia), a mobile app, leveraging blockchain and biometrics, was used to allow military personnel voting from abroad to submit votes securely, with no security breaches reported [29]. European Parliament passed a resolution highlighting the potential of Distributed Ledger Technologies to reduce bureaucracy, decentralize governance, and improve transparency in public registries and cross-border services [30]. Even so, the legislative process is deeply rooted in tradition, with legal, procedural, and technological barriers making blockchain integration more complex. To genuinely observe the implementation of blockchain technology in the realm of lawmaking—for instance, in the compilation of legislative drafts, the verification of official texts, or even the execution of parliamentary

votes on blockchain—a greater number of pilot projects, legal experiments, or specialist committees would be required to thoroughly assess the practical capabilities of blockchain tools. At present, this subject has not yet been the focus of widespread attention.

2.2. Benefits for the Legislative Processes Tracking and Audit Using Blockchain

Blockchain technology can be employed to create secure and verifiable digital identities, which can facilitate the streamlining of processes such as the registration of members of Parliament acting as voters for a bill. The aforementioned use cases illustrate the manner in which blockchain technology can facilitate enhanced transparency, security, and efficiency within the legislative process [31]. Blockchain technology presents a number of advantages for the field of auditing:

- Trust and transparency: Blockchain technology offers an immutable and transparent ledger where transactions are recorded in a decentralized manner. This provides auditors with the ability to verify the integrity of data without relying on a central authority, thereby enhancing trust in statements and audit reports [32].
- Prevention of frauds: The transparency that is characteristic of blockchain technology has been shown to act as a deterrent to fraudulent activities. The transparency characteristic of blockchain technology has been demonstrated to have the effect of reducing the likelihood of financial fraud. This is due to the fact that auditors are able to identify irregularities with greater efficacy [33].
- Enhanced Data Modification Prevention (sometimes referred as Security): Blockchain's cryptographic techniques guarantee the secure storage of data and prevent any unauthorized alterations. Furthermore, auditors can rely on the accuracy and consistency of the information stored on the blockchain [34].
- Transaction monitoring: Blockchain technology facilitates the real-time monitoring of financial transactions, enabling auditors to continuously observe and assess activities. This transition from a retrospective examination approach to an ongoing monitoring strategy has been shown to enhance the effectiveness of audits.
- Increased efficiency through automation: The automation of predefined audit procedures through the use of smart contracts reduces the necessity for manual effort. This allows auditors to direct their attention toward exceptions and anomalies, thereby enhancing efficiency and reducing the overall duration of the audit process.

In the literature frameworks, limitations and technological challenges of using blockchain-based smart contracts in the legislative process are presented, but without providing an implemented and tested software solution. Palmirani et al. [35] explores how blockchain technology can improve the efficiency of the legislative process, without affecting the separation of powers in the state. A multi-level architecture is presented that maintains the independence of the participating institutions, while allowing for the traceability and secure verification of legislative documents. The conceptual framework proposed by Tan et al. [36] evaluates decision-making options and their impact on the design and implementation of blockchain solutions by classifying governance decisions according to three levels of analysis. Noe et al. [37] propose a prototype that solves interoperability problems between government institutions, yet further research and testing in real-world scenarios are needed before this system can be fully implemented. Many of the applications are still in the pilot project stage, but the success of blockchain adoption in the public sector depends not just on the technology but also on institutional capacity, infrastructure, trust in the government, and a suitable legal framework that facilitates decentralized innovation [38].

Some countries have integrated blockchain technology into their traditional systems to improve government services, but this adoption remains fragmented. The Philippine

government [39] has implemented a blockchain solution based on the Polygon network to verify official budget documents. These documents are converted into non-fungible tokens and recorded on the blockchain. The data model maintains the confidentiality of the data by keeping document hashes without disclosing private information. Since the network is semi-public, users can scan QR (Quick Response) codes or access a public portal to confirm the user's identity. The system was developed on the Polygon network, which uses the Proof-of-Stake consensus mechanism.

Another legislative system is that of Estonia [40], which is based on the Keyless Signature Infrastructure (KSI) blockchain technology. To generate a cryptographic audit trail, KSI uses hashes and hash trees instead of smart contracts. The information is not copied to the blockchain, but remains stored in the government systems. Users can access and verify information through transparent audit mechanisms. In addition, KSI complies with data protection requirements because only fingerprints of the data are stored, without compromising the identity or content of the data.

Another government use case is the National Agency of Public Registry (NAPR) in Georgia [41], which leverages blockchain technology to ensure the integrity of land ownership records. The system, developed in collaboration with Bitfury, anchors cryptographic hashes of property transactions onto a permissioned blockchain based on the Exonum framework. Unlike a fully decentralized ledger, NAPR retains operational control through government nodes and periodically anchors its internal blockchain to a public network for additional immutability guarantees. The approach provides tamper-evidence and traceability while keeping the detailed registry data within governmental databases. Personal and property information remain off-chain, and only minimal identifiers and content hashes are written to the blockchain, ensuring compliance with data protection regulations.

A further notable initiative is ARCHANGEL [42], a pilot project conducted by The National Archives of the United Kingdom, which explores the use of blockchain for long-term digital preservation. ARCHANGEL employs smart contracts on a public Ethereum network to register and verify content fingerprints of archived documents, ensuring their authenticity and provenance over time. Each fingerprint is stored together with metadata describing the hashing algorithm and version history, enabling independent verification of fixity. The design supports public verifiability through blockchain explorers and a dedicated verification interface, while the actual document content remains in archival repositories. Privacy and compliance are maintained by storing only hash digests and non-identifiable metadata on-chain.

Unlike prior implemented systems that (i) provide general hash anchoring (Estonia KSI, Georgia NAPR) or (ii) pilot archival fixity (ARCHANGEL), our platform delivers a domain-specific smart-contract layer for legislative workflows: it models state transitions of bills/acts, voting, and a public verifiability gateway. Technically, the combination of permissioned blockchain for institutional governance, a minimal on-chain data model aligned with GDPR-by-design (hashes + metadata only), and a role-based dApp for parliamentary users is, to our knowledge, the first end-to-end proposal tailored to Romanian legislative units rather than a generic integrity anchor. A key aspect of our system lies in the integration of a role-aware access control framework—combining Keycloak-based institutional authentication with smart-contract-level authorization—within a permissioned blockchain that remains publicly auditable. This dual-layer design ensures that only verified institutional actors can record or attest legislative actions, while any external observer can transparently verify their integrity through the public audit interface.

Our objective is not merely to protect the content; there are other centralized solutions available for that purpose. Instead, we urge policymakers to give due consideration to all comments and observations, including those originating from both within parliament

and from Non-Governmental Organizations (NGOs). Furthermore, the observations must possess unalterable traceability, particularly with regard to order and, notably, timing. According to Law No. 544 of 12 October 2001, which governs the right of access to public information, specific deadlines are established for public institutions to formulate responses to requests. The utilization of blockchain technology establishes a framework that renders the modification of timestamps and subsequent alteration of content impossible.

To validate our DLT-based implementation, we target two use cases, first a simpler workflow, for journalist accreditation in a public institution, then a more complex and realistic workflow, validated in a public institution, that follows the lifecycle of a draft proposal that becomes adopted law in Romanian Parliament. A key aspect is supporting transparency in all stages of the legislative process by using DLT. Also, this implementation can be the starting point of other use cases as the ones presented above. This validated work can serve as a good practice for any other areas of government process.

3. Document Workflow

In order to illustrate the integration of blockchain technology into a document management system utilized in the legislative process, we first employed a fundamental four-step workflow (Figure 1) that outlines the procedure for obtaining accreditation as a journalist. The use case of journalist accreditation is a frequent and common procedure in the Romanian Parliament. It should be noted that the workflow can be adapted for any other use cases. For these reasons, we started from this common procedure and developed a four-step workflow:

- Creation: The accreditation application is generated and the necessary documents are submitted.
- Review and validation: The application form, its content, and submitted documents are analyzed and validated.
- Approval: The journalist's application for accreditation is either approved or rejected.
- Distribution: The necessary documents are sent to the departments involved in implementing the security check and issuing access permits.

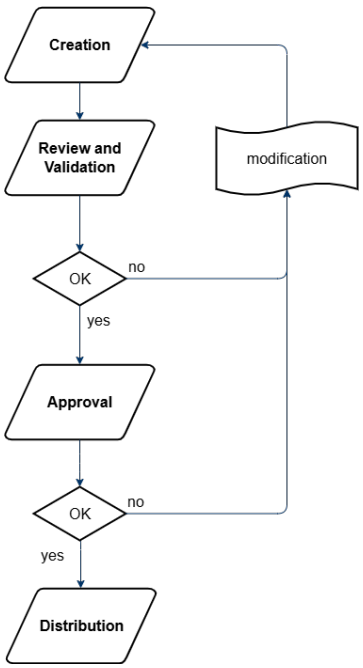


Figure 1. Simplified workflow procedure for obtaining journalist accreditation.

Accredited journalists are issued a verifiable credential, stored on their digital wallet. The other use case will be the workflow of a draft becoming an adopted law.

4. Methods and Implementation

4.1. Blockchain Platform

To develop our document management system, we considered different Blockchain technologies: Ethereum, Hyperledger Fabric, Exonum, and Corda. Based on related work in e-government domain, the final choice was between Ethereum and Hyperledger Fabric. It is influenced by several factors, including specific requirements for privacy, scalability and governance. Hyperledger Fabric is open source backed by the Linux Foundation, which provides a significant level of assurance to potential users. Additionally, Hyperledger Fabric allows:

1. Privacy: Hyperledger Fabric is designed for private, permissioned networks, making it an optimal choice for enterprise use where data privacy and controlled access are paramount. The issue of confidentiality is important in this context; only authorized participants are able to view transactions, thus ensuring the highest levels of confidentiality.
2. Scalability and Performance: Hyperledger Fabric is capable of processing a considerable number of transactions per second due to its modular architecture. It does not rely on a native cryptocurrency, which can facilitate reducing transaction costs.
3. Governance and Flexibility: Hyperledger Fabric's modular architecture allows users to customize the blockchain to align with their specific requirements. This flexibility is a key advantage of Hyperledger Fabric, as it enables users to adapt the blockchain to their unique needs. Moreover, Hyperledger Fabric has strong support from major enterprises and a robust development community, further enhancing its credibility and potential for success.

Ethereum is a decentralized blockchain that allows the development of applications and smart contracts. It is distinguished by the following properties:

- Decentralized and public: The Ethereum network is a public, non-restricted network, meaning that anyone (individual or company) is permitted to join and engage in the activities conducted on the network. The network is characterized by a high degree of transparency, whereby all transactions are publicly visible and accessible for review. All transactions are transparent and accessible for viewing by any interested party, which may not be optimal for the management of sensitive documents.
- Smart Contracts: Ethereum is a highly effective platform for the execution of smart contracts and the construction of decentralized applications. It offers a robust foundation for the implementation of sophisticated logic and automation. The Hardhat Development Environment is a system that facilitates the process of constructing, testing, and deploying smart contracts in a streamlined manner, centered around Ethereum Virtual Machine based blockchains by providing a set of tools and features like Smart Contract Development, Local Testing, Debugging.
- Community and Ecosystem: The Ethereum platform boasts a substantial and dynamic developer community, offering a valuable resource for locating necessary resources and assistance. As a highly utilized blockchain system, Ethereum provides superior interoperability with other blockchain implementation's services.

In qualitative terms, based on the aforementioned criteria, it can be stated that Hyperledger Fabric represents a superior option for a document management system that adheres to rigorous privacy and permissioning standards. This assertion is predicated on the system's private and permissioned nature, high scalability, and robust enterprise sup-

port. Conversely, for a system that necessitates the extensive utilisation of smart contracts and a preference for a public, decentralised networks, Ethereum with Hardhat may prove a more optimal choice. The final decision was to use Ethereum taking also into consideration future interoperability with the National Blockchain in Romania which is centered on Ethereum technology and connected to European Blockchain Services Infrastructure.

4.2. Components

We have developed a document management system integrated with blockchain technology with a focus on security, transparency, and efficiency. The document management system, as seen in the information model, (Figure 2) has four states for documents: Creation, Review and validation, Approval, Distribution/archived. Each state transition is recorded on the blockchain to ensure transparency, immutability, and security.

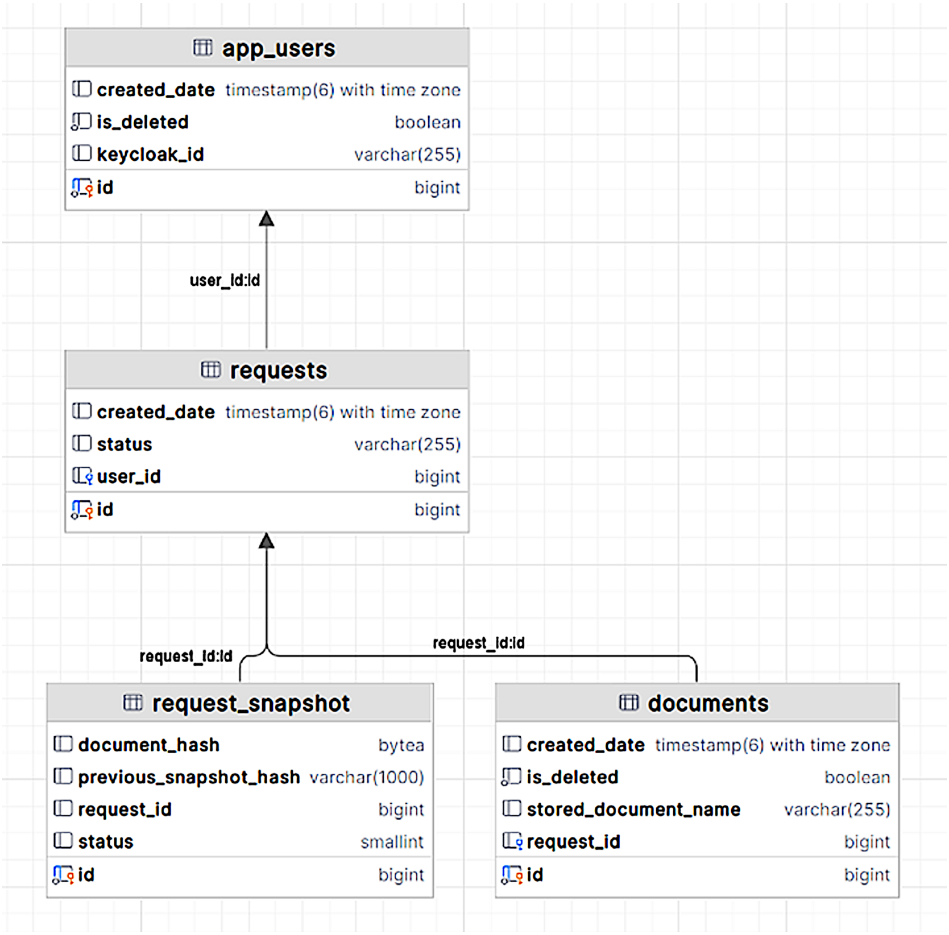


Figure 2. Information model for document requests.

4.2.1. Frontend

The front-end of the application is built using React with the Vite development tooling and two user-interface UI Libraries: shadcn for customizable components and tailwind for styling components. Vite is a modern JavaScript build tool and development server which leverages native ECMAScript (ES) modules during development, therefore making it a fast development server. It also has features like hot module replacement which allows for the code to be reloaded without needing for a complete restart of the app. Shadcn/ui is a collection of reusable React components, which allowed us to have a greater flexibility and customization for the elements. The web-based interface allows users to upload, view, and manage documents. The user authentication and authorization is handled with the help of Keycloak. The additional data is the list of documents, each having an unique

identifier. To ensure secure access, OAuth was integrated into the authentication and authorization process.

4.2.2. Backend

The smart contract automates the execution of the terms of an agreement on a blockchain network. The Ethereum smart contracts are used to manage state transitions and store document metadata. Hardhat is a versatile tool that can be utilized for both development and deployment. PostgreSQL stores document contents and metadata that are not stored on the blockchain. Besides the blockchain, the additional data stored on a traditional database helps the application to speed up the verification process. Node.js is used on the server-side to handle requests from the front-end. Express.js is used to interact with the blockchain and the database.

4.2.3. Blockchain Layer

For the prototype we have used a private Ethereum network with PoA consensus mechanism in which a full Ethereum node is used to interact with the blockchain. Full nodes store all blockchain data and validate blocks, providing complete control over participation in the Ethereum blockchain. Hardhat Ethereum Node is used for local development and testing. Smart Contracts are deployed on a private Ethereum blockchain to handle document state transitions and ensure immutability. We have used Slither, which is an open-source static analysis framework for Solidity that runs locally to audit the Ethereum contracts for the application. After analyzing the contracts with all the 80 detectors, it has not found any vulnerabilities. The –exclude-informational flag is used to filter out the informational outputs like the ones related to variable naming (e.g., mixedCase).

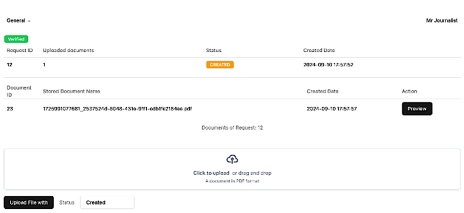
4.3. Document Workflow

Improving document workflows has been achieved by digitizing existing manual processes, thus reducing repetitive tasks, reducing time and minimizing errors in the workflow.

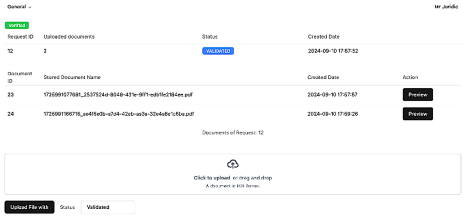
1. Document Upload (Figure 3a):
   - User uploads a document through the UI.
   - Application Programming Interface (API) Server receives the document and stores it in the database.
   - Smart Contract is called to record the document's initial state (Creation) on the blockchain.
2. State Transitions (Figure 3b):
   - User requests a state transition (e.g., from Creation to Review).
   - API Server validates the request and calls the smart contract to update the document's state on the blockchain.
   - Smart Contract updates the state and logs the transition.
3. Document Retrieval:
   - User requests to view a document.
   - API Server retrieves the document from the database and its state from the blockchain.
   - UI displays the document along with its current state.

The final step is document approval or denial (Figure 3c,d).

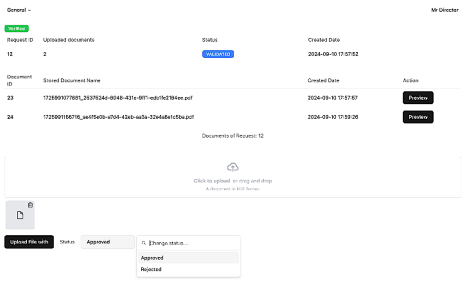
To provide insight into the document workflow, each document has a status attached. The status of each document is presented to the first user who created it. The document has a timestamp created to facilitate auditing and can be opened by the user (Figure 3e).



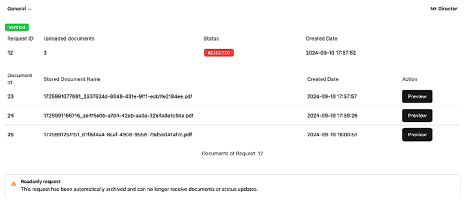
(**a**) Document creation.



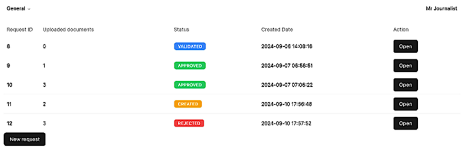
(**b**) Document validation.



(**c**) Document approval.



(**d**) Document denial.



(**e**) Document status.

Figure 3. Document lifecycle.

4.4. Audit

Through the use of smart contracts, legislative processes are automated, thus each legislative document will be tagged, secured and registered on the blockchain with the aim of being immutable and auditable. Permissioned access to the blockchain ensures that authorized parties, such as auditors, can verify the legitimacy and integrity of legislative actions. In order to ascertain the structure of the DLT, we employed the services of *Chainlens* [43]. A blockchain explorer such as Chainlens serves as a browser for whole chain, offering comprehensive insights into pertinent data such as blocks and transactions (Figure 4), as well as an analytics platform for Ethereum Virtual Machine compatible networks. It allows for gathering insights regarding on-chain activity, allowing users to view and analyze tokens and smart contracts.

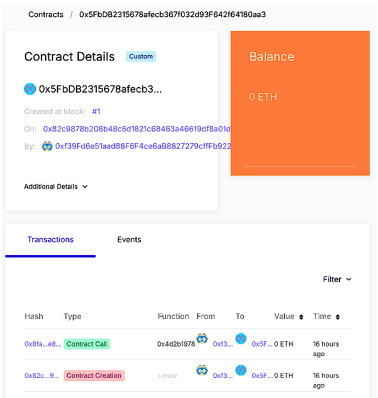


Figure 4. Blockchain explorer.

4.5. Verification and Access

In order to reduce costs, the access control is implemented as a mobile application (for the security officer or as an automated checkpoint).

1. Accreditation Requirement: For a valid access, the journalists are required to have valid accreditation, which is provided as a QR code stored in their digital wallet (Figure 5). The verifiable credential is based on W3C Verifiable Credentials Data Model 2.0 [44].
2. Verification Process: At the entry point, the journalist presents their QR code to the security officer (can be a human or automated reader) who scan it using a physical scanner device (in case of a human) or mobile app to reduce costs (using an automated reader).
3. Authentication: The scanned QR code links to the application that verifies the journalist's credentials in real time. The scanned QR code triggers a query to the blockchain network via smart contract. If the information matches the valid accreditation document, the system approves access (Figure 6).
4. Access Decision: If the verification is successful, the access controller permits entry. If the QR code is invalid, expired, or tampered with, entry is denied. Once verified, the security officer permits the journalist to enter.
5. Audit Trail: For a highly secure access audit, the application automatically logs every verification event, creating a tamper-proof record for future reference

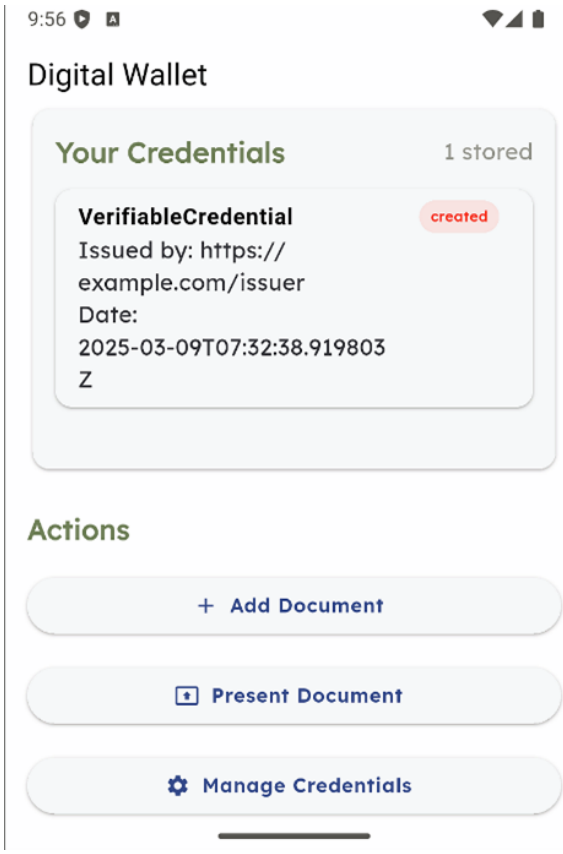


Figure 5. Digital wallet including the verifiable credential.

This implementation ensures a smooth, secure, and efficient process for controlling access based on accreditation integrated with a document management system.

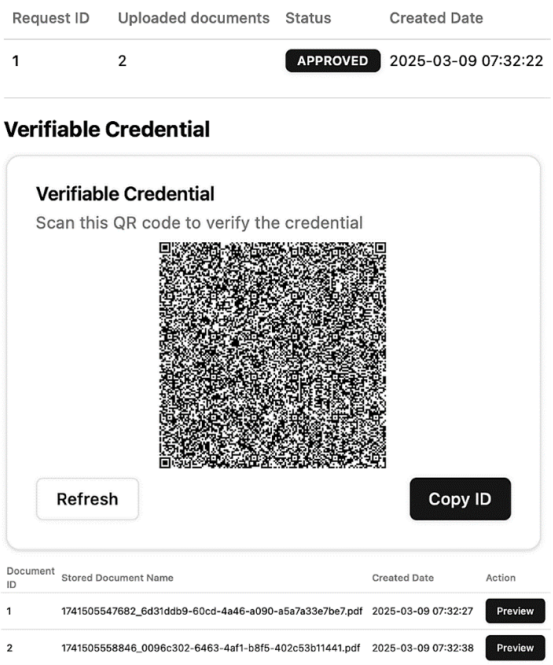


Figure 6. Journalist Authentication using QR code.

5. Results

To test the application, an experiment was performed on a Macbook Pro machine using version 15.6 of MacOS, with an Apple M4 Max processor and 48 GB of RAM, both the ethereum node and the containers for the backend and Postgres being locally ran. Using K6, an open-source tool that measures the performance and load of test applications, we have obtained a benchmark for the system under different loads based on the number of active users.

All tests were executed on the same request, with the id 11, and with the first status available, which is 'CREATED'. Between tests, the database was cleared to obtain comparable results. The load test script contains 3 main parts. The test options contain the number of virtual users (100, 200, 1000) as well as the number of minutes for which it will run (1 min).

One more aspect that needs to be cleared for the request is the headers for authorization. In this case an OpenID Connect (OIDC) provider is used and we are using a real user's token. This is used to link the uploaded document to a certain user as well as check if the user has authority to execute the requested operation.

The data metrics shown in Table 1 are based on the analysis of Hypertext Transfer Protocol (HTTP) request statistics, which encompass both the data received and the data sent. We can see from the results that the current prototype implementation handles easily the increase from 100 to 200 users then gracefully from 200 to 1000 users. While final deployment on premises will benefit from better infrastructure, even the current numbers are satisfactory for the envisioned number of requests in our scenarios.

Table 1. Test results.

No. Users	HTTP Reqs	HTTP Reqs/s	Avg	Min	Max
100	19,849	328.92	303.05 ms	200.29 ms	405.02 ms
200	39,715	659.28	302.9 ms	200.31 ms	439.61 ms
1000	40,569	658.71	1.49 s	200.24 ms	1.93 s

In the context of legislative processes monitoring and auditing, keeping in mind that the National Blockchain in Romania, managed by the Special Telecommunication Service is built on Ethereum [45], we have chosen to use Ethereum for possible future integration. Also, the Service was in charge of organizing the elections where it used a software solution on the Ethereum blockchain integrated with the European infrastructure EBSI (European Blockchain Services Infrastructure) intended to verify the right to vote and prevent illegal voting [46].

6. Migration from Document Workflow to Legislative Process

The second use case deals with the legislative process (Figure 7), a complex undertaking that can be facilitated by the implementation of a document management system with DLT.

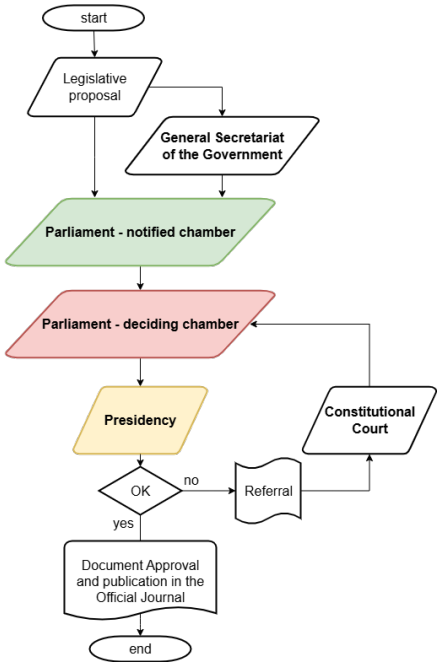


Figure 7. Overall legislative process for a new law in Romania.

The legislative process is started by drafting a bill or a legislative proposal. It can be generated by deputies or senators, by citizens, by a ministry or government or by other state authorities. This legislative proposal is submitted to the General Secretariat of the Government or to the Chamber of Parliament. After submission to the General Secretariat of the Government (SGG), the opinion of the Legislative Council (CL) is requested for the respective proposal Accompanied by this opinion, the proposal is adopted in the Government meeting, possibly with amendments, and is submitted to the first chamber of the Parliament. The legislative proposal follows a structured process, starting with its registration for debate in the designated parliamentary chamber. It goes through several stages of examination, including obtaining opinions from government institutions, specialized committees and economic and social councils. After the final debate and approval in plenary session, the adopted version is sent to the decision-making chamber of the Parliament. The next stage in the legislative process is registration for debate with the decision-making body. The opinions obtained at the previous stage are requested and sent to the committees giving the opinion and the specialized committees. After a waiting period, amendments are debated and approved in plenary session. This version is sent to the Presidency. Once the legislative proposal reaches the final stage, it is sent to the Presidency and assessed for constitutionality. If doubts arise, it is sent to the Constitutional

Court for review and revision. If it is deemed constitutional, the President promulgates the law, which is then published in the Official Journal. The President can only once veto the bill without suggesting changes or modifications. The President can notify the Constitutional Court to verify whether a law is constitutional, before promulgation. If the Court declares the law unconstitutional, the bill is sent back to Parliament for revision. If the Court declares the law constitutional, the President must promulgate it.

For e-government, where transparency and efficiency should coexist with bureaucracy, we propose a blockchain-based network, spanning the Government, Ministries, the Chamber of Deputies, the Senate, the Presidency, and the Constitutional Court. At the core of this system lies a unified blockchain that stores data (only the final version of each document issued by an administrative or legislative unit) and preserves history, making every action traceable and auditable. When a document is created, it is encrypted, timestamped, and added to the blockchain, accessible only to authorized stakeholders. Each institution maintains its own internal document management system, tailored to its unique needs and preferences. The internal system can be a central operated digital solution, paper-based documents and archiving, or even an independent institution-specific blockchain that operates alongside the primary general blockchain system. Any legislative body can draft legislation within its own system, then securely publish a validated version to the primary blockchain, where it becomes immutable and accessible to other governmental or legislative bodies. Using this approach for blockchain-driven governance, transparency is verifiable in reality. Figure 8 presents a detailed view of step by step process taking place in the first designated parliamentary chamber (identified as Parliament–notified chamber in Figure 7).

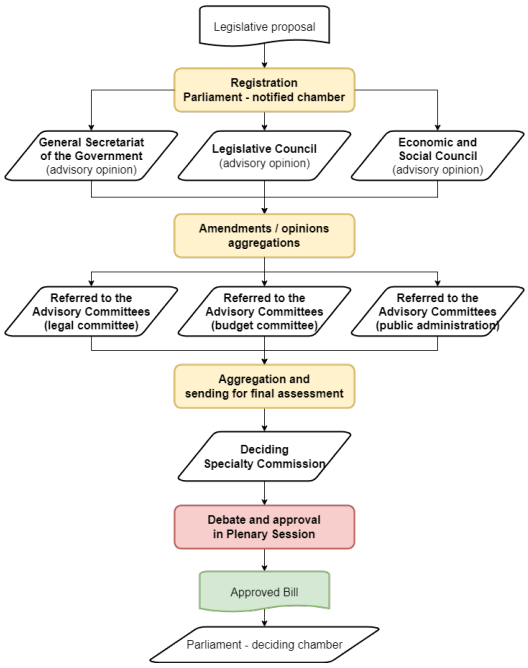


Figure 8. Legislative process in the first designated parliamentary chamber.

The legislative proposal is registered for debate in the designated parliamentary chamber. A request for an opinion or point of view is sent to the General Secretariat of the Government (SGG). The request for opinion is also sent to the Legislative Council (CL) and the Economic and Social Council (CES). After the expiry of the deadline for waiting for amendments, the legislative proposal is sent to the Committees that have to give an opinion.

The improved version is sent to the specialized Committees that have to give the final specialized report from the decision-making entity (committees in the field of the legislative

proposal). This report is sent for debate and approval to the plenary. After approval, the adopted version is submitted to the decision-making entity, the Chamber of Deputies or the Senate.

The workflow is presented in algorithmic format in Algorithm 1.

Algorithm 1 Legislative Document Workflow.

Input: Digital document D (file), metadata M (title, category, issuing unit), and access token T.
Output: Blockchain: $(\texttt{docUUID} \rightarrow \texttt{documentHash})$; Database: $(\texttt{docUUID} \rightarrow (\texttt{lawId}, \texttt{userId}, \texttt{stepId}))$, and $(\texttt{lawId} \rightarrow \texttt{locationPDF})$.

Preconditions:
1. User authenticates through Keycloak and receives an access token T.
2. The client wallet is bound to the institutional identity and role.
3. The blockchain network is running.

1. Ingestion and Hashing
Store D in the institutional repository (off-chain) and generate `docUUID`.
Compute $\texttt{initialDocumentHash} = \mathsf{sha256}(D)$.

2. Registration (Registrar)
Verify registrar permissions based on T and execute `DocumentRegistry(requestId, initialDocumentHash)`.
Store resulting block on the blockchain.

3. Review and State Transitions
for $s \in \{\mathsf{Registration}, \mathsf{Amendments}, \mathsf{Debate}\}$ **do**
    Receive updated document D, store it, and generate a new `docUUID`.
    Compute $\texttt{newDocumentHash} = \mathsf{sha256}(D)$.
    Authorized users with T call `DocumentRegistry(requestId, newDocumentHash)`.
end for

4. Voting (Members of Parliament)
Each MP records a vote $\in \{\mathsf{Yes}, \mathsf{No}, \mathsf{Abstain}\}$.
Append result to the document D and compute $\texttt{votedDocumentHash} = \mathsf{sha256}(D)$.
Authorized users with T call `DocumentRegistry(requestId, votedDocumentHash)`.

5. Publication and Public Access
Make document history available on the audit portal.
The public can view document status and hashes.

6. Verification (Public Users)
Public users recompute $\texttt{verifiedDocumentHash} = \mathsf{sha256}(D')$ and verify it matches on-chain.

Postconditions:
No personal data is stored on-chain.
The complete audit trail can be independently verified.

In the process of transferring the final bill from the chamber of parliament that has received notification to the chamber that is responsible for decision-making, it is sufficient to simply reiterate the final version of the document that has been submitted by the Specialty Commission and store it within the new blockchain. Subsequent applications will function in a manner analogous to the initial application; there is not necessary for re-validation of the origin or validity of the data.

From a blockchain perspective, we propose a single transaction should be automatically triggered at the exact moment when the last committee, out of a predefined sequence of multiple committees, signs its advisory opinion within the legislative process. This mechanism ensures that the transaction is executed only when all necessary evaluations and approvals have been completed, preventing premature actions before the full review cycle is finalized. The system should recognize the specific point at which the third and final advisory opinion is officially signed, treating it as the definitive confirmation that the legislative process has reached the required stage for the transaction to be initiated. By structuring the automation around this final approval, the transaction will be accurately timed to reflect the culmination of all committee evaluations, maintaining procedural integrity and ensuring that no steps are overlooked before execution. Structuring the transaction trigger around the final advisory opinion from the last committee helps prevent document forking. By ensuring that the transaction is executed only after all committees have completed their assessments, the system avoids premature or conflicting versions of the document being processed simultaneously.

In order to exemplify the implementation, we present in Figure 9 the process of a real draft law and the main stages it goes through in order to be adopted. We are referring to the "Draft law for the ratification of the Agreement between the Government of Romania and the Government of the Republic of Moldova on the coordinated control on the Romanian territory at the state border crossing point Galati (Romania)-Giurgiulesti (Republic of Moldova) by road, on the way into Romania, signed on 20 November 2024, in Bucharest "-L103/2025-" Proiect de lege pentru ratificarea Acordului între Guvernul României şi Guvernul Republicii Moldova privind controlul coordonat pe teritoriul României în punctul de trecere a frontierei de stat Galaţi (România)-Giurgiuleşti (Republica Moldova) rutier, pe sensul de intrare în România, semnat la 20 noiembrie 2024, la Bucureşti" [47].

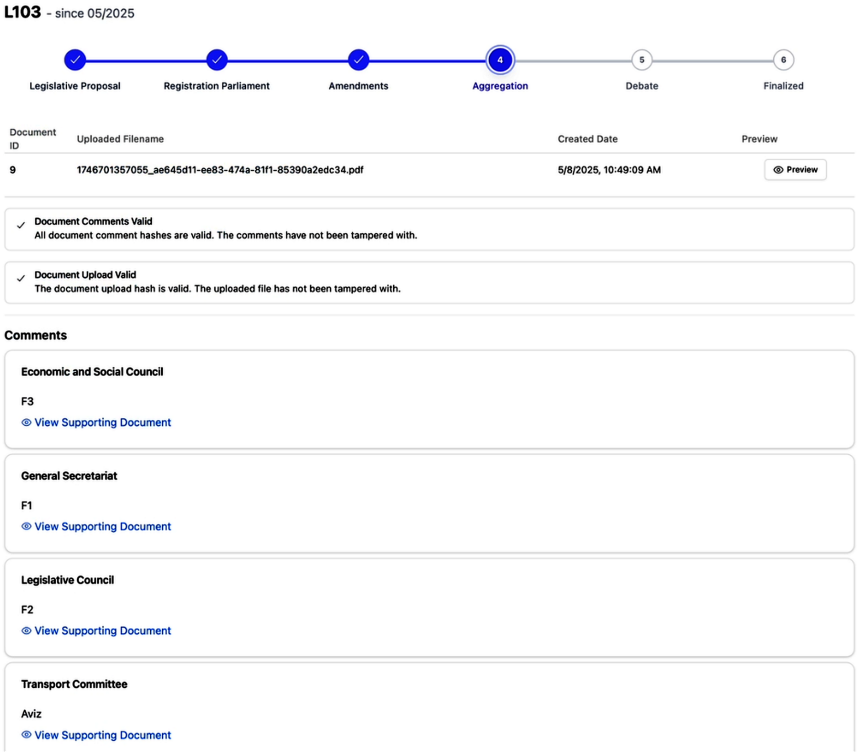


Figure 9. State transition for the proposed law L103/2025.

The draft version was registered under the number L103/2025 and is represented by the document "25L103FG forma initiatorului.pdf". It has been advised by the Committee on Transport and Infrastructure (document "25L103CA42 aviz comisia transporturi.pdf")

and by the Committee on Foreign Policy (document "25L103CA5 aviz comisia politica externa.pdf"). In the Committee for Defense, Public Order and National Security, the report of the specialized committee (document "25L103CR raport comisia aparare.pdf") was drafted and sent for debate in the Senate plenary session. The version adopted in the plenary session of the Senate is represented by the document "25L103FS forma adoptata de senat.pdf" which is sent for promulgation by the President (Figure 10).

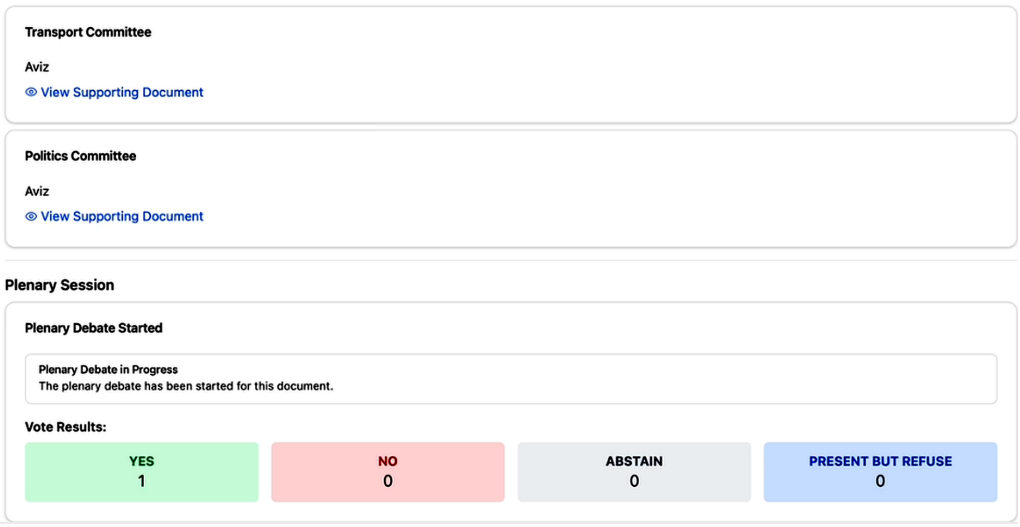


Figure 10. Voting process in the first parliamentary chamber.

For the validation phase, the prototype was presented to the IT department of the Parliament of Romania, the Senate, being met with favorable comments and a letter of interest was issued for further implementation and deployment. The end-users appreciated that the application correctly follows the real process of adopting a law and the possibility for third parties to verify the steps. Also, the interview highlighted some possible improvements, especially in the user interface area, for users not accustomed to the blockchain terminology.

The documents are stored off-chain in PDF format, the name of the file follows an internal encoding, an UUID Universally Unique Identifier and the timestamp of the document. The name of the document is mapped to the real name of the law, in a PostgreSQL table, and available for public access. Thus each transaction corresponding to a change in the state of the law (adoption, approval, adding of comments, debate) can be publicly verified in the blockchain, matched to the PDF version of the law, what will ultimately be published in the Official Journal. In order to verify transactions on the blockchain, a non-governmental organization or any citizen may utilize an independent tool that enables inspection of transactions and accounts on a node. In order to facilitate the verification process for bills and their corresponding comments, it is feasible to develop an open-source application. This application, accessible to the public for the purpose of validating a document, would receive a PDF document as an input and calculate its hash utilizing the same hash function as the primary system (Figure 11).

Subsequently, the input will be compared with the information stored on the blockchain. This approach would offer a more user-friendly interface than ChainLens while maintaining the same level of trust. Furthermore, we will propose to NGOs to host nodes that will host the same DLT as our application, enabling the verification of the law adopting process, with the required level of trust and transparency, providing free of charge verification services to the general public.

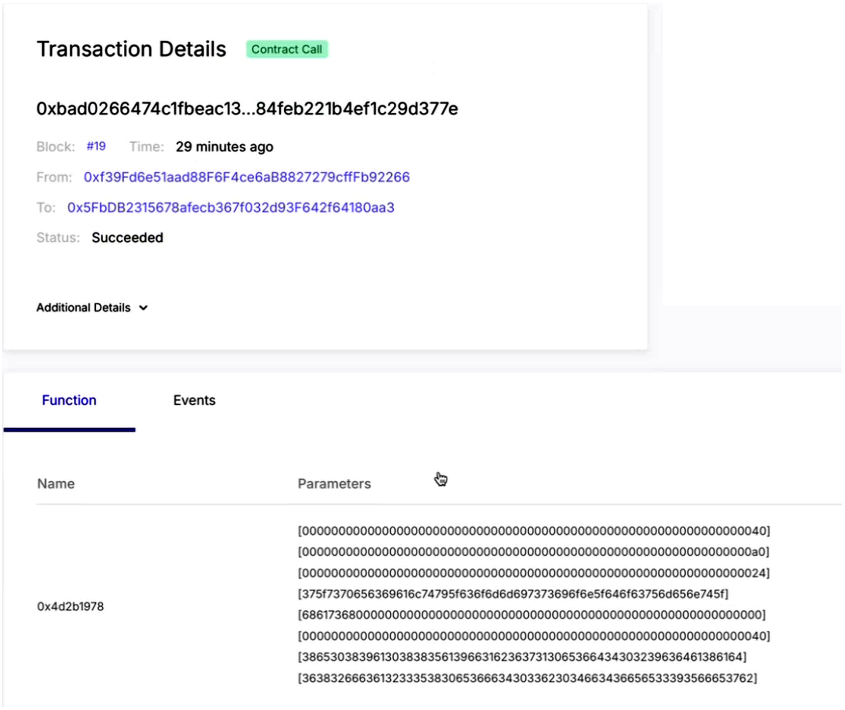


Figure 11. Blochchain inspection for the document transaction the first designated parliamentary chamber.

Below we detail the approach we used and provide context for the user-centered aspects of our implementation:

(a) Structured Usability Study:

While a formal usability study (e.g., task-based testing or standardized questionnaires) was not conducted, we did carry out a qualitative assessment through a series of interviews and consultations with key stakeholders. These included members of the Romanian Parliament, relevant administrative personnel, and the Information Technology and Communication IT&C manager responsible for digital solutions within the Parliament. These interviews aimed to gather feedback on user needs and expectations during the design and development phases.

(b) User Testing and Accessibility Analysis:

The interface was developed in direct collaboration with the Romanian Senate's IT&C department, based on specifications and usability requirements defined by end-users and institutional stakeholders. Although no independent accessibility audit was performed, the design process was guided by the department's extensive experience in supporting non-technical users. The director of the IT&C department, with over 18 years of experience working with the Parliament and Senate, oversaw the process to ensure usability and accessibility for the target user base.

(c) User Experience for Non-Technical Stakeholders:

The final implementation was reviewed and validated by the Senate's IT&C department through an internal evaluation process. An official letter from the department confirms that the solution met their expectations in terms of both functionality and ease of use. This validation reflects the department's confidence that the application supports the digital literacy levels of non-technical stakeholders within the institution.

Below we are discussing the legal, regulatory and security aspects related to the blockchain-based application presented in the paper.

(a) Storing Legislative Documents on Blockchain

The legislative documents integrated into our blockchain application are already public and available on the Romanian Parliament's official website. However, they are currently published only at selected milestones, without offering a traceable or immutable history of how documents evolve throughout the legislative process. Our blockchain implementation does not change the legal classification or accessibility of these documents but rather enhances transparency and auditability. By timestamping and storing the legislative artifacts on a blockchain, we provide a verifiable and tamper-evident record of the legislative workflow. This helps to close a transparency gap that exists in the current centralized system, particularly regarding the inclusion (or exclusion) of public consultations and comments during the law-making process. Such blockchain integration can help ensure procedural integrity without altering the legal treatment of the documents.

(b) Data Sovereignty and General Data Protection Regulation (GDPR) Compliance

In the Romanian legislative context, voting records, political declarations, and MP activity are classified as public information. For example, the official parliamentary portal displays how each member of the Chamber of Deputies or Senate voted on a bill. Therefore, the inclusion of such data on a blockchain does not conflict with GDPR principles, as no personal or sensitive data (as defined under GDPR Article 9) is processed. Additionally, the application was designed to handle only data that is already in the public domain and does not collect or process personal information related to private citizens. As such, issues like the right to erasure (Article 17 of GDPR) or data minimization do not apply. For future extensions where citizen engagement might be incorporated (e.g., public consultations), we note that a permissioned blockchain or off-chain storage with on-chain hashes would be necessary to maintain GDPR compliance and allow selective data revocation or access control.

No personal data or document contents are written to the blockchain ledger, which makes the system fully compatible with GDPR principles such as data minimization, purpose limitation, and the right to erasure.

While voting records and commission documents contain identifiable information (e.g., names, timestamps), these data describe the exercise of a public mandate, not private life. Under Article 4(1) GDPR, information concerning an individual acting in an official public capacity does not constitute "personal data" in the relevant sense, since it relates to the function rather than the person.

(c) Security

The system's security design follows a defense-in-depth strategy, addressing both blockchain-specific and conventional application threats. Key protected assets include document content, workflow metadata, authentication tokens, smart contracts, and cryptographic keys. The main risks identified are first-mile tampering (altering a document before hashing), unauthorized access, key compromise, and metadata leakage. This approach covers the basic security at network level (firewalls, apps access authorisation, etc.) and continues at application infrastructure security which includes:

- real time monitoring with a focus on access logs and auditing functionalities;
- user authorization based on MFA;
- applications authorization based on key management;
- data infrastructure (database and file system storage) protected by encryption and always on redundancy.

At operational level, backups are realised periodically on two separate sites and recovery is tested after multiple incremental backups are performed. The security threat architecture is presented in Figure 12.

The classic first-mile (ingest) trust gap can be observed in blockchain systems. Blockchain immutability guarantees that what is committed on-chain cannot later be changed but it does not guarantee that the first copy of a file or the metadata that gets hashed and placed on-chain is the true/original authoritative artefact. If an attacker or a malicious insider replaces or tampers the off-chain file BEFORE the first hash/commit is created, the chain will faithfully record the hash of the tampered file and thus the on-chain proof becomes useless for establishing original provenance. In order to eliminate or reduce first-mile risk, our approach which is the best practice in other blockchain-based implementation, focuses on client-side hashing & signing. That implies to compute the file hash at client side (in a browser or a signed client app) and send that hash to the backend BEFORE uploading the file. Optionally sign that hash with the user's private key (an organizational key) so the system receives a signed hash, user. This reduces the chance that the server substitutes content before hashing and upload in the database. The digital signatures of public officials (or role holders) require authorized actors (MPs, committee chairs) to digitally sign the document (or the document hash) before the system accepts it as "official". The usage of organizational PKI is recommended. Signed hashes create an auditable binding between the actor, the content, and the timestamp.

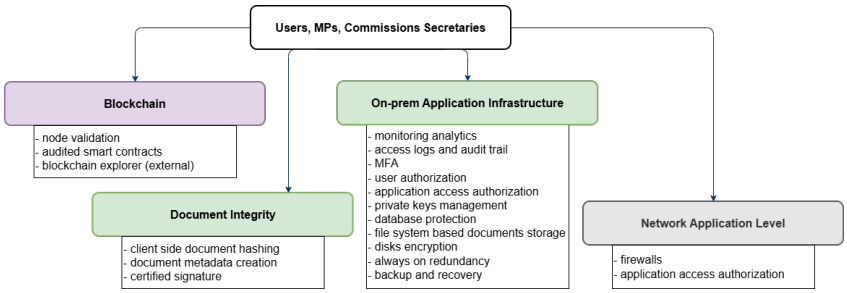


Figure 12. Data protection architecture diagram.

Another method concerns the organizational process controls and segregation of duties. That involves separation between uploader, approver, and node operators. No single person can both alter the file and anchor it on chain. Another approach is mandatory multi-party approval for "official" commit which require two or more approving signatures (e.g., author + committee secretary) before anchor is considered final. Two-person approvals reduce risk of single-actor compromise. So, as a conclusion, the concrete mitigations procedures involve:

- Digital signatures of elected officials/role holders: binds person to action/document; non-repudiation; legal evidence.
- Qualified timestamps: an authoritative, legally recognized time attestation for the client hash; if the timestamp attestation is later published on-chain or kept as a receipt, it proves existence/time independent of server.
- Client-side signing and immediate anchoring

For the purposes of disaster recovery and key management, we will regularly back up encrypted key metadata (not keys) and set the media configuration to offline, kept in safe storage at least in two separated locations. If the account owning the contract (the admin/owner key) is lost (private key lost or compromised and then inaccessible), depending on how the contract was written the admin may lose the ability to upgrade the contract, change parameters, or perform admin operations. To mitigate this problem, we

plan not use a single externally private key as the admin. We propose to use a multiple signature system (a cryptographic control mechanism that requires multiple independent digital signatures) such that multiple admin/owner of important privileges are required to reach a threshold of keys to perform admin actions; this approach reduces also single-point-of-failure risk.

While the costs of the solution will depend on the client existing hardware on-premises, we have made an approximation considering costs of hosting the solution in the cloud, using AWS pricing calculator in Table 2. AWS Fargate is configured with 3 containers (one for backend, two for the blockchain nodes), Amazon RDS for PostgreSQL handles the relational database storage, Amazon Simple Storage is configured with 20GB/month for storing documents and Amazon CloudFront is used for CDN for the frontend. It results in a monthly cost of USD 354.25.

Table 2. Cost approximation.

Service Name	Upfront Cost	Monthly Cost
AWS Fargate	0.00	248.69 USD
Amazon RDS for PostgreSQL	0.00	104.01 USD
Amazon Simple Storage	0.00	0.51 USD
Amazon CloudFront	0.00	1.05 USD

7. Conclusions

The intended users of the application include central and local public administration (county councils, city halls, etc.) where the auditing and tracking of documents in a workflow is a mandatory requirement. This system is also applicable in law offices and any legal professional institutions. In addition to the aforementioned functions, the system facilitates transparency and offers a means of verifying the veracity of information from external sources, accessible to any individual. The system was validated by experts from the IT&C Department of the Senate, Romanian Parliament.

This study set out to answer three research questions: (RQ1) how a blockchain-based audit layer can be designed to ensure end-to-end traceability of legislative document workflows, including intermediate drafts, while maintaining compliance with existing workflows; (RQ2) how a blockchain-enabled web application can be designed to deliver verifiable, real-time insights into legislative processes; and (RQ3) how smart contracts that govern workflow events can be subjected to verification and validation to guarantee functional correctness and adherence to legislative process constraints. For RQ1, the proposed system records each modification to legislative documents, creating an immutable, chronological chain of custody that adds extra traceability in addition to the final publication in the Official Gazette. For RQ2, the system introduces a monitoring interface, enabling independent, real-time oversight and providing a tamper-evident view into parliamentary activity not achievable through traditional, post-facto publication. For RQ3, smart contracts governing workflow transitions were validated using a combination of automated testing in Hardhat, Chainlens, and static analysis tools, ensuring that the encoded business logic enforces legislative process constraints without introducing security vulnerabilities. Together, these findings demonstrate that the proposed architecture not only addresses recognized challenges in legislative transparency and traceability but also advances methodological rigor in smart contract verification within governance contexts. The DSR framework provided a structured means to integrate technical innovation—such as blockchain auditing and smart contract verification—with the legal and organizational constraints of a legislative environment.

The qualitative validation conducted with the Senate's IT&C Department confirmed that the proposed system effectively mirrors the actual stages of the Romanian legislative workflow. Participants emphasized that the blockchain audit layer significantly enhanced the traceability and transparency of document circulation, compared with existing tools. The visual workflow representation and real-time audit trail were repeatedly cited as features that improved process comprehension and accountability. This feedback supports the study's research questions (RQ2 and RQ3), demonstrating that the blockchain-enabled interface can deliver verifiable, real-time insights into legislative processes while maintaining procedural integrity.

Furthermore, respondents highlighted that the system's design and terminology should be further adapted to accommodate users with limited technical experience, suggesting that enhanced interface simplicity would improve adoption among non-specialist staff. Despite this, evaluators expressed a strong institutional acceptance of the prototype, viewing it as a viable transparency tool for legislative and administrative workflows. Overall, the qualitative findings substantiate the system's functional alignment with user needs and validate its potential to extend blockchain-based audit mechanisms to broader e-government contexts.

As a prospective enhancement, the implementation of a digital signature generation module for internal use in conjunction with the document management system is planned, in addition to the existing usage of qualified digital signatures. That way, we decrease the systems' total cost of ownership; electronic signatures qualified by a CA and already owned by the end user will be used only to sign the final approved document for external purposes and verification. A second area of development is the integration of the application with an automated document logging system, with a particular focus on institutions where the auditing requirements are of paramount importance.

Author Contributions: Conceptualization, C.V.M. and A.V.; methodology A.V.; software, D.S.R.; validation, D.A.M.; writing—review and editing, C.V.M., A.V. and D.A.M.; supervision, C.V.M.; project administration, D.A.M.; funding acquisition, D.A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Romanian Alliance of Technical Universities, University Politehnica of Bucharest (Alianta Romana a Universitatilor Tehnice, Universitatea POLITEHNICA din Bucuresti) under National Research Grants (Granturi Naționale de Cercetare-GNaC 2023 ARUT UPB) for the project "Blockchain application for digital governance/Aplicatie Blockchain pentru guvernarea digitala" grant number 130/2023.

Data Availability Statement: The original contributions presented in this study are included in the article. The code is available at https://github.com/rusudinu/journalist-accreditation-with-dlt (accessed on 23 October 2025). Further inquiries can be directed to the corresponding author.

Acknowledgments: The authors would like to express their gratitude to the experts of the IT&C Department of the Senate, Romanian Parliament, who provided invaluable insights and whose expertise was instrumental in advancing our research.

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

Abbreviations

The following abbreviations are used in this manuscript:

API	Application Programming Interface
CL	Legislative Council
DLT	Distributed Ledger Technology
EBSI	European Blockchain Services Infrastructure

ES	ECMAScript
GDPR	General Data Protection Regulation
IT&C	Information Technology and Communication
NGO	Non-Governmental Organizations
SGG	General Secretariat of the Government
UI	User Interface

References

1. Marakas, G.M.; O'Brien, J.A. *Enterprise Information Systems*, 13th ed.; McGraw-Hill Higher Education: New York, NY, USA, 2007.
2. Anttiroiko, A.V. *Electronic Government: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2008; Volume 3.
3. Popa, A.M.; Mocanu, S. Scalable Ecosystem Dedicated To Digitalization Of Citizen-Administration Interaction. *UPB Sci. Bull. Ser. C* **2021**, *83*, 59–72.
4. Farida, I.; Setiawan, R.; Maryatmi, A.S.; Juwita, M.N. The implementation of E-government in the industrial revolution era 4.0 in Indonesia. *Int. J. Progress. Sci. Technol.* **2020**, *22*, 340–346.
5. Masiero, S. Digital identity as platform-mediated surveillance. *Big Data Soc.* **2023**, *10*, 20539517221135176. [CrossRef]
6. Júnior, L.A.F.; Guimarães, L.G.d.A.; Segundo, E.M.D.; Batista da Costa, W.P.L.; El-Aouar, W.A. Open Government and E-Government: Concepts, Gaps, Interfaces, and Trends. In *Global Encyclopedia of Public Administration, Public Policy, and Governance*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 8750–8760.
7. Theocharis, S.; Tsihrintzis, G.A. E-government: The concept, the environment and critical issues for the Back-office systems. In *Semantic Knowledge Modelling via Open Linked Ontologies: Ontologies in E-Governance*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 7–49.
8. Neacsu, E.; Schiopu, P. A Security Analysis Of Public Key Cryptographic Systems Used For Electronic Signature. *UPB. Sci. Bull. Ser. C* **2021**, *83*, 135–146.
9. Bonyuet, D. Overview and impact of blockchain on auditing. *Int. J. Digit. Account. Res.* **2020**, *20*, 31–43. [CrossRef]
10. Hevner, A.R.; March, S.T.; Park, J.; Ram, S. Design science in information systems research. *MIS Q.* **2004**, *28*, 75–105. [CrossRef]
11. Ranjith Kumar, M.; Bhalaji, N. Blockchain based chameleon hashing technique for privacy preservation in E-governance system. *Wirel. Pers. Commun.* **2021**, *117*, 987–1006. [CrossRef]
12. EBSI. Understanding EBSI's Blockchain Ecosystem. Available online: https://hub.ebsi.eu/blockchain (accessed on 11 May 2025).
13. STS. Rețeaua Europeană de Blockchain, Extinsă în România de căTre STS. Available online: https://sts.ro/ro/reteaua-europeana-de-blockchain-extinsa-in-romania-de-catre-sts (accessed on 11 May 2025).
14. Lykidis, I.; Drosatos, G.; Rantos, K. The use of blockchain technology in e-government services. *Computers* **2021**, *10*, 168. [CrossRef]
15. Fraga-Lamas, P.; Fernandez-Carames, T.M.; da Cruz, A.M.R.; Lopes, S.I. An overview of blockchain for Industry 5.0: Towards human-centric, sustainable and resilient applications. *IEEE Access* **2024**, *12*, 116162–116201. [CrossRef]
16. Hermus, M.; van Buuren, A.; Bekkers, V. Applying design in public administration: A literature review to explore the state of the art. *Policy Politics* **2020**, *48*, 21–48. [CrossRef]
17. Tan, E.; Lerouge, E.; Du Caju, J.; Du Seuil, D. Verification of education credentials on European Blockchain Services Infrastructure (EBSI): Action research in a cross-border use case between Belgium and Italy. *Big Data Cogn. Comput.* **2023**, *7*, 79. [CrossRef]
18. Liu, Y.; He, D.; Obaidat, M.S.; Kumar, N.; Khan, M.K.; Choo, K.K.R. Blockchain-based identity management systems: A review. *J. Netw. Comput. Appl.* **2020**, *166*, 102731. [CrossRef]
19. Shuaib, M.; Daud, S.M.; Alam, S.; Khan, W.Z. Blockchain-based framework for secure and reliable land registry system. *TELKOMNIKA Telecommun. Comput. Electron. Control.* **2020**, *18*, 2560–2571. [CrossRef]
20. Idrees, S.M.; Nowostawski, M.; Jameel, R.; Mourya, A.K. Security aspects of blockchain technology intended for industrial applications. *Electronics* **2021**, *10*, 951. [CrossRef]
21. Jafar, U.; Aziz, M.J.A.; Shukur, Z. Blockchain for electronic voting system—review and open research challenges. *Sensors* **2021**, *21*, 5874. [CrossRef] [PubMed]
22. Huang, J.; He, D.; Obaidat, M.S.; Vijayakumar, P.; Luo, M.; Choo, K.K.R. The application of the blockchain technology in voting systems: A review. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–28. [CrossRef]
23. Esmaeilian, B.; Sarkis, J.; Lewis, K.; Behdad, S. Blockchain for the future of sustainable supply chain management in Industry 4.0. *Resour. Conserv. Recycl.* **2020**, *163*, 105064. [CrossRef]
24. Korepanova, D.; Kruglik, S.; Madhwal, Y.; Myaldzin, T.; Prokhorov, I.; Shiyanov, I.; Vorobyov, S.; Yanovich, Y. Blockchain-based solution to prevent postage stamps fraud. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Republic of Korea, 14–17 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 171–175.

25. Cagigas, D.; Clifton, J.; Diaz-Fuentes, D.; Fernández-Gutiérrez, M. Blockchain for public services: A systematic literature review. *IEEE Access* **2021**, *9*, 13904–13921. [CrossRef]
26. Demirhan, H. Effective taxation system by blockchain technology. In *Blockchain Economics and Financial Market Innovation: Financial Innovations in the Digital Age*; Springer International Publishing: Cham, Switzerland, 2019; pp. 347–360.
27. Chaleenutthawut, Y.; Davydov, V.; Evdokimov, M.; Kasemsuk, S.; Kruglik, S.; Melnikov, G.; Yanovich, Y. Loan portfolio dataset from MakerDAO blockchain project. *IEEE Access* **2024**, *12*, 24843–24854. [CrossRef]
28. Crypto Valley. Zug Citizens Open to More Blockchain-Based E-Voting. 2020. Available online: https://members.cryptovalley.swiss/news/270202 (accessed on 14 August 2025).
29. National Association of Secretaries of State. The West Virginia Mobile Voting Pilot. 2019. Available online: https://www.nass.org/sites/default/files/2019-02/white-paper-voatz-nass-winter19.pdf (accessed on 14 August 2025).
30. European Parliament. Distributed Ledger Technologies and Blockchains: Building Trust with Disintermediation. 2017. Available online: https://oeil.secure.europarl.europa.eu/oeil/en/procedure-file?reference=2017/2772(RSP) (accessed on 14 August 2025).
31. European Commission. Shaping Europe's Digital Future. Available online: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain (accessed on 10 April 2025).
32. Deloitte. The Impact of Blockchain Technology on Audit. Available online: https://www2.deloitte.com/us/en/pages/audit/articles/impact-of-blockchain-in-accounting.html (accessed on 11 May 2025).
33. Basly, S.; Saunier, P.L. Blockchain adoption in the accounting and auditing industry: An exploratory study in France. In *Decentralized Finance: The Impact of Blockchain-Based Financial Innovations on Entrepreneurship*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 95–110.
34. ISACA. Impacts of Blockchain on the Auditing Profession. 2018. Available online: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/impacts-of-blockchain-on-the-auditing-profession (accessed on 10 April 2025).
35. Palmirani, M.; Bomprezzi, C.; Papalia, L. The Use of Blockchain for Legislative Simplification and Tracking. In Proceedings of the 2025 Eleventh International Conference on eDemocracy and eGovernment (ICEDEG), Bern, Switzerland, 18–20 June 2025; pp. 97–105. [CrossRef]
36. Tan, E.; Mahula, S.; Crompvoets, J. Blockchain governance in the public sector: A conceptual framework for public management. *Gov. Inf. Q.* **2022**, *39*, 101625. [CrossRef]
37. Elisa, N.; Yang, L.; Chao, F.; Cao, Y. A framework of blockchain-based secure and privacy-preserving E-government system. *Wirel. Netw.* **2023**, *29*, 1005–1015. [CrossRef]
38. Bustamante, P.; Cai, M.; Gomez, M.; Harris, C.; Krishnamurthy, P.; Law, W.; Madison, M.J.; Murtazashvili, I.; Murtazashvili, J.B.; Mylovanov, T.; et al. Government by Code? Blockchain Applications to Public Sector Governance. *Front. Blockchain* **2022**, *5*, 869665. [CrossRef]
39. Department of Budget and Management Philippines. A Blockchain-Powered System for Tracking SARO and NCA Documents. Available online: https://blockchain.dbm.gov.ph/ (accessed on 14 October 2025).
40. e-Estonia. KSI Blockchain. 2025. Available online: https://e-estonia.com/solutions/cyber-security/ksi-blockchain/ (accessed on 14 October 2025).
41. Lazuashvili, N.; Norta, A.; Draheim, D. Integration of blockchain technology into a land registration system for immutable traceability: A casestudy of Georgia. In Proceedings of the International Conference on Business Process Management, Vienna, Austria, 1–6 September 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 219–233.
42. Peng, S. The Application of Blockchain Technology in the Field of Electronic Document Management: A Case Study of the ARCHANGEL Project. *Suntext Rev. Case Rep. Image* **2024**, *5*, 116.
43. Chainlens. Your Gateway to EVM Blockchain Exploration. Available online: https://www.chainlens.com/ (accessed on 11 May 2025).
44. World Wide Web Consortium (W3C). Verifiable Credentials Data Model v2.0. 2025. Available online: https://www.w3.org/TR/vc-data-model-2.0/ (accessed on 14 October 2025).
45. Bratu, A.; Aloman, A.; Goga, N. Blockchain Bridge Between Private Guvernamental Blockchains. In Proceedings of the 2024 IEEE SmartBlock4Africa, Accra, Ghana, 30 September–4 October 2024. [CrossRef]
46. Special Telecommunication Service. STS Blockchain Explorer. 2025. Available online: https://explorer.blockchain.stslink.ro (accessed on 14 August 2025).
47. Servicii Online Senat. Servicii Online Senat. Available online: https://www.senat.ro/ (accessed on 7 May 2025).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.