Revista de Ingenierías Interfaces, Vol 9 (2) Julio-Diciembre 2026. ISSN 2619-4473 E-ISSN 2619-4465, pp 1-17.

Application of Blockchain Technology in a Prototype for Complaint Management at Family Police Stations: A Case Study of Fusagasugá, Colombia *

Aplicación de tecnología blockchain en un prototipo para la gestión de denuncias en Comisarías de Familia: estudio de caso en Fusagasugá, Colombia

Recibido: enero 18 de 2026 - Evaluado: abril 6 de 2026 - Aceptado: mayo 4 de 2026

Laurent F. Castañeda **
Jorge E. Camargo ***

Para citar este artículo / To cite this Article
L. F. Castañeda, J. E. Camargo "Application of Blockchain Technology in a Prototype for Complaint Management at Family Police Stations: A Case Study of Fusagasugá, Colombia" Revista de Ingenierías Interfaces, vol. 9, no. 2, pp.1-17, 2026.

Abstract

In the public sector, administrative procedures generate case files that are traditionally stored in physical archives or relational databases. Ensuring the authenticity, reliability, and integrity of these records is critical to achieving the mission of Colombian Family Police Stations (Comisarías de Familia), which protect and restore the rights of family members affected by intra-family violence. Nevertheless, conventional information systems can be vulnerable to falsification, unauthorized modification, and loss of traceability. This paper presents the design, implementation, and evaluation of a prototype that integrates blockchain technology — through smart contracts deployed on Ethereum — with a centralized microservices architecture to manage the registration and follow-up of complaints at the Family Police Station of Fusagasugá, Colombia. The methodology combined a qualitative deductive approach with Design Thinking and Business Process Management (BPM/BPMN) for the identification and modeling of processes, followed by agile software-engineering practices for construction. The prototype was tested by staff members of the Family Police Station through a controlled simulation using fictitious cases, and their perceptions were captured through a structured survey. Results indicate that 100% of participants considered that the prototype can validate the authenticity of documents, 75% perceived that blockchain-based public disclosure benefits stakeholders, and 75% agreed that the prototype improves complaint management. The study contributes a replicable open-source reference architecture for integrating permissionless blockchain with legacy public-sector workflows under Colombian archival regulations.

---

*Artículo inédito: "Application of Blockchain Technology in a Prototype for Complaint Management at Family Police Stations: A Case Study of Fusagasugá, Colombia".

** Magister en Ingeniería de Sistemas y Computación, Ingeniero de Sistemas, Universidad Nacional de Colombia, Correo electrónico: lfcastanedar@unal.edu.co, ORCID: 0009-0003-6514-2683, Bogotá, Colombia
***Doctorado en Ingeniería de Sistemas y Computación, Maestría en Ingeniería de Sistemas y Computación, Ingeniero de Sistemas, Universidad Nacional de Colombia, Correo electrónico: jecamargom@unal.edu.co, ORCID: 0000-0002-3562-4441, Bogotá, Colombia.

Keywords: Blockchain; Smart Contracts; Public Sector; Document Management; E-Government; Ethereum; Microservices; Design Thinking.

Resumen

En el sector público, los trámites administrativos generan expedientes que tradicionalmente se almacenan en archivos físicos o en bases de datos relacionales. Garantizar la autenticidad, la fiabilidad y la integridad de dichos registros es crítico para el cumplimiento de la misión de las Comisarías de Familia colombianas, encargadas de proteger y restablecer los derechos de los miembros del núcleo familiar afectados por violencia intrafamiliar. Sin embargo, los sistemas de información convencionales pueden ser vulnerables a la falsificación, la modificación no autorizada y la pérdida de trazabilidad. Este artículo presenta el diseño, la implementación y la evaluación de un prototipo que integra tecnología blockchain —mediante contratos inteligentes desplegados en Ethereum— con una arquitectura centralizada de microservicios, para gestionar el registro y seguimiento de denuncias en la Comisaría de Familia de Fusagasugá, Colombia. La metodología combinó un enfoque cualitativo deductivo con Design Thinking y Business Process Management (BPM/BPMN) para la identificación y modelamiento de los procesos, seguido de prácticas ágiles de ingeniería de software para la construcción. El prototipo fue probado por funcionarios de la Comisaría de Familia mediante una simulación controlada con casos ficticios, y sus percepciones se capturaron a través de una encuesta estructurada. Los resultados indican que el 100% de los participantes consideró que el prototipo permite validar la autenticidad de los documentos, el 75% percibió que la divulgación pública basada en blockchain beneficia a las partes interesadas, y el 75% coincidió en que el prototipo mejora la gestión de denuncias. El estudio aporta una arquitectura de referencia replicable y de código abierto para integrar blockchain no permisionada con flujos de trabajo heredados del sector público, en el marco de la normativa archivística colombiana.

Palabras clave: Blockchain; contratos inteligentes; sector público; gestión documental; gobierno electrónico; Ethereum; microservicios; Design Thinking.

1. Introduction

Blockchain has emerged as a disruptive technology that has drawn the attention of academics, entrepreneurs, and public officials alike. Its core value proposition lies in the validation, synchronization, and immutability of records, which together provide trust between interested parties without requiring a central authority [1], [12]. While the private sector has rapidly adopted blockchain for use cases ranging from finance and supply chains to real estate and healthcare, adoption in the public sector has lagged behind — partly because governments lack the flexibility and resources of private companies, and partly because of an ongoing debate about whether the State should deploy technologies that are still being tested elsewhere [5].

Despite this cautious approach, several relevant precedents exist worldwide. Estonia and other Baltic states have pioneered e-Residency and anti-corruption programs based on distributed ledger technology [19], [20]; Mongolia has deployed a blockchain-based medicine verification scheme [3]; and in Colombia, pilots led by the Inter-American Development Bank and the Office of the Attorney General have explored blockchain for public procurement (including the PAE school-meals program), land titling in partnership with the National Land Agency (ANT) and Universidad Nacional de Colombia, and academic-record integrity through the RITA network [34].

Family Police Stations (Comisarías de Familia) in Colombia, regulated by Law 2126 of 2021 [33], are municipal or inter-municipal bodies whose mission is to prevent, guarantee, restore, and repair the rights of family members in situations of intra-family violence. The daily activities of these institutions generate case files (expedientes) composed of documents that must be preserved according to strict archival principles of authenticity, reliability, and integrity [28], [30], [32]. In practice, however, information systems at many municipal Family Police Stations suffer from integrity weaknesses in several stages of their activity — a situation that may increase administrative costs, undermine community welfare, and damage the institutional image of local government.

This paper addresses that gap by designing, implementing, and evaluating a prototype that applies blockchain technology to the registration and follow-up of complaints at the Family Police Station of Fusagasugá, a mid-sized municipality in the department of Cundinamarca. The main contribution is a reference microservices architecture that combines (i) an Ethereum smart contract that stores the electronic index of each case file, (ii) a business-rules layer that enforces domain logic and user permissions, and (iii) a repository service that manages the actual documents and interacts with the blockchain network. The smart contract, the source code of the centralized services, the user manual, and the mockups have been released in public repositories so that researchers and practitioners can study, reuse, or extend them.

The remainder of this article is organized as follows. Section 2 reviews the theoretical background on blockchain, distributed ledger technology, and smart contracts, and surveys related work in the public sector. Section 3 describes the qualitative methodology based on Design Thinking and BPM/BPMN. Section 4 presents the requirements, architecture, and smart-contract design of the prototype. Section 5 details the implementation and deployment, while Section 6 reports the evaluation conducted with the staff of the Family Police Station. Section 7 discusses the results, and Section 8 presents conclusions and future work.

Background and Related Work

Blockchain and Distributed Ledger Technology

Blockchain is a technology — or, more precisely, a method — that allows the validation, maintenance, and synchronization of content across a shared digital ledger that is replicated among several participants [1], [12]. When a transaction is issued, it is grouped with others into a block; that block is then distributed across a peer-to-peer (P2P) network of nodes. Specialized nodes — commonly called miners — apply a consensus mechanism such as proof-of-work [25] to validate the block and append it to the chain. Every block is cryptographically linked to the previous one through a hash pointer, which makes retroactive modification computationally impractical and provides the immutability property for which blockchain is best known [8], [13].

Three main types of blockchain networks are commonly distinguished [41]: (i) public blockchains, which are open to anyone who wishes to mine or transact (e.g., Bitcoin, Ethereum); (ii) private blockchains, which require an invitation and restrict reading and writing to a specified group; and (iii) consortium blockchains, which combine centralized and decentralized elements and are jointly maintained by several organizations. Blockchain is part of the broader family of Distributed Ledger Technologies (DLT) [21], which enable digital value transfer between two unknown entities without a trusted third party and improve the transparency of information exchanges.

Because records stored in the public sector — civil registries, land titles, financial transactions, judicial files — must often be preserved for decades and remain trustworthy beyond the life cycle of any particular database or server, blockchain has been proposed as a promising solution to the problem of trustworthy recordkeeping [12]. Trust in data, however, begins with the creation process; a reliable record is one whose content is a complete and accurate representation of the transactions or activities it certifies, and whose identity and integrity are preserved from creation through preservation.

Smart Contracts

A smart contract is a self-executing program that runs on a blockchain network and whose behavior is determined by the code itself rather than by a trusted intermediary [15]. Smart contracts enable the automation of obligations between counterparties and have been explored as instruments for disintermediation in areas such as fintech [17], governance [18], cross-border business [20], and peer-review incentives [22]. In the context of this work, smart contracts are used as a tamper-evident electronic index that describes the composition and state of each case file.

Blockchain in the Public Sector

The literature reports several application areas of blockchain for government and public services. These include digital storage and authentication of land titles and intellectual property [8], [12]; identity management for migration, national security, and elections, including identity-fraud detection [9], [10], [11]; transparent public procurement and anti-corruption programs [4], [37]; augmentation of the security of digitized academic records [38]; land-registration systems [39]; quality management in additive manufacturing [40]; decentralized evidence archiving via IPFS [41]; and decentralized healthcare applications [42]. The information presented in these works consistently highlights transparency, auditability, and integrity as the main drivers of adoption, while pointing out legal regulation, ownership, interoperability between different blockchains, and control over the ledger as persistent challenges [1].

In Colombia, previous initiatives include a proof-of-concept for public procurement developed with the Inter-American Development Bank and the Office of the Attorney General, applied to the PAE school-meals program [34]; the Blockchain de Tierras project developed jointly by Universidad Nacional de Colombia, the National Land Agency (ANT), and the Ministry of Information and Communication Technologies (MinTIC), which addressed risks of manipulation and non-consensual adjustments in land-restitution adjudication [34]; and the RITA network at Universidad Francisco José de Caldas, which supports projects for diploma integrity, notarial systems, and traceability of the school-meals program [34]. No prior Colombian initiative has specifically addressed complaint management at Family Police Stations, which is the gap that this work aims to fill.

2. Methodology

A qualitative deductive research approach was adopted in order to move from a general understanding of the Family Police Station as an organization toward a detailed characterization of its processes, and then to derive a technological intervention. The methodology is organized around the five phases of Design Thinking — empathize, define, ideate, prototype, and evaluate — complemented by Business Process Management (BPM) with the Business Process Model and Notation (BPMN) for process identification and modeling [31].

➢ Empathize

The empathize phase included a review of the Colombian regulatory framework (Political Constitution Article 209; Law 594/2000; Law 2126/2021; Decree 4840/2007; Agreements 002/2014 and 003/2015 of the General Archive of the Nation; Decree 1080/2015), an institutional characterization of the Family Police Station of Fusagasugá — its mission, organizational pyramid, and staff composition — and participatory sessions with its personnel. This phase provided the contextual understanding needed to align any technological solution with existing legal and archival obligations.

➢ Define

In the define phase, the full set of processes carried out by the Family Police Station was identified through a process panorama and classified by type of complaint: childhood and adolescence, elderly care, and intra-family violence. For each category, four stages were modeled in BPMN — registration and diagnosis, opening, restoration of rights, and closure — in addition to the diagnostic sub-process that is common to all of them. This exercise made it possible to pinpoint activities that were most exposed to integrity and traceability risks and therefore more likely to benefit from a blockchain-based intervention.

- **Ideate**

The ideate phase was conducted through three rounds of participatory workshops with the staff of the Family Police Station. The first round surfaced challenges such as the high turnover of non-permanent personnel, difficulty in consulting the state of a complaint, loss of traceability of annexed documents, lack of public transparency for non-confidential information, and the tedious preparation of files for transfer to the General Archive of the Nation. The second round socialized and debated the responses, and the third round documented a consensus solution: a centralized web application, backed by blockchain, that would flexibly register each step of a complaint, guarantee the immutability of the control sheet, enforce document authenticity through hashing, allow public consultation of non-confidential information in the style of Colombian judicial portals, and automate the generation of file copies for the General Archive.

- **Prototype and Evaluate**

Based on the ideation outputs, a prototype was built using agile software-engineering practices. The prototype was iteratively refined through functional testing and finally evaluated by the staff of the Family Police Station through a controlled simulation with fictitious complaints. A structured survey was then applied to capture participants' perceptions, as reported in Section 6.

- **System Design**

Functional and Non-Functional Requirements

The requirements elicitation produced the following high-level specifications:

Functional requirements: (RF-1) web accessibility from desktop and mobile browsers; (RF-2) registration of complaints by process type; (RF-3) consultation of the state of a process, including by users who are not the case owner, while protecting confidential data; (RF-4) persistence and authenticity verification of documents through hashing; (RF-5) search of processes according to user-defined parameters; (RF-6) generation of the complete digital file on demand; (RF-7) role-based access control; (RF-8) annexation of PDF documents to the case file; and (RF-9) display of the electronic control sheet.

Non-functional requirements included usability, scalability, modularity, interoperability with the Ethereum ecosystem, and compliance with Colombian archival regulations.

Microservices Architecture

Rather than building a monolithic system, the prototype was designed as three independently deployable microservices, each with a single responsibility: (i) a User Interaction Microservice, responsible for the presentation layer and user experience; (ii) a Business Rules Microservice, which encapsulates the high-level domain logic governing complaint management at the Family Police Station, including user access control and an optimized local copy of blockchain data for fast queries; and (iii) a Repository Rules Microservice, which manages the document repository and interacts with the Ethereum network to deploy and invoke smart contracts.

This separation of concerns simplified testing, allowed the use of the most appropriate language and framework in each layer, and made independent scaling possible. Figure 1 provides a schematic view of the whole system, including the actors, the three microservices, the PostgreSQL cache, the off-chain document repository, and the Ethereum network that hosts the smart contract.

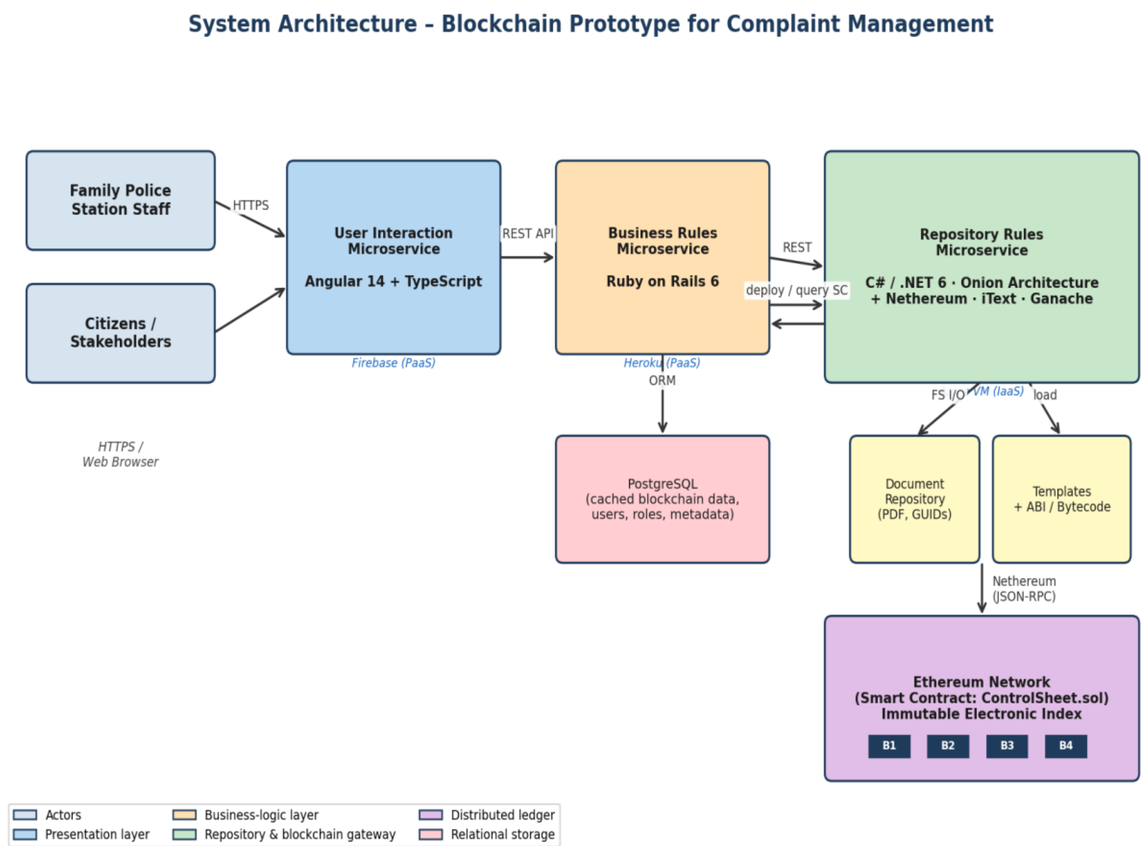

Figure 1. Reference architecture of the prototype. The User Interaction (Angular/Firebase) and Business Rules (Rails/Heroku) microservices are deployed on PaaS, while the Repository Rules microservice (.NET 6/Azure VM) acts as the blockchain gateway and manages the off-chain document repository.

Smart Contract and Electronic Index

The smart contract, named ControlSheet and implemented in Solidity 0.8.6, is responsible for the electronic index of each case file — that is, for the ordered sequence of documents and actions that occur during the life cycle of a complaint. Every time a complaint is registered, a new instance of the ControlSheet contract is deployed on the Ethereum network and associated with a unique cryptographic address. To minimize gas costs and preserve confidentiality, the contract does not store the actual documents; it stores only a header (title, module, document number, office, owner, open/closed status, and aggregate hash) and a body composed of paper-control entries (document identifier, name, hash, hash algorithm, order, start/end pages, format, origin, creator, and creation date). The full Solidity source code is available in Appendix 1 of the underlying thesis and in the public repository linked in Section 8.

Data Model and Sequence Flows

A relational entity–relationship model was designed as a supporting layer for the smart contracts, holding user accounts, roles, complaint metadata, and cached blockchain information for efficient querying. The main sequence flows modeled were: user login, registration of a complaint (which culminates in the deployment of a smart contract), transfer of a complaint to another officer, annexation of a document (which triggers hashing and an update to the electronic index), download of a single document, download of the complete file, and closure of the file. A state machine defines the admissible transitions for a complaint — from registered, through parties-registered, under review, in remission, and finalized. Figure 2 summarizes this lifecycle as a three-lane workflow in which officer actions trigger business-logic operations and, ultimately, smart-contract transactions on the Ethereum network.

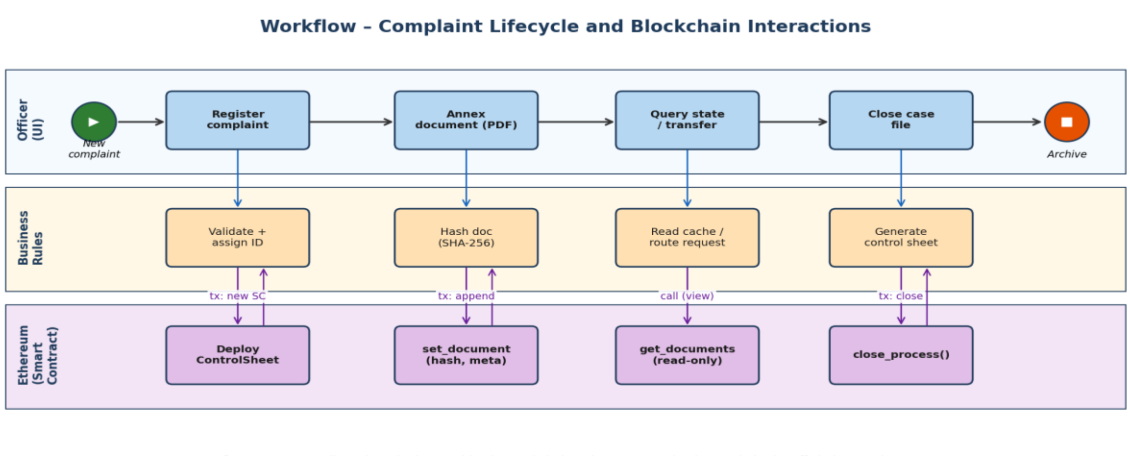

Figure 2. Complaint lifecycle and interaction with the blockchain layer. Each user action in the top lane flows through the Business Rules microservice and is persisted either as a state-changing transaction (tx) or as a read-only call on the ControlSheet smart contract.

➢ Implementation and Deployment

Technology Stack

The technology stack was selected to favor rapid learning, mature documentation, and compatibility with the Ethereum ecosystem:

Table I. Selected technologies by microservice.

Microservice	Language	Frameworks & Libraries
Repository Rules	C# / Solidity	.NET 6, Nethereum (Ethereum access), iText (PDF manipulation)
Business Rules	Ruby	Ruby on Rails 6, Devise (authentication), ActiveRecord (ORM)
User Interaction	HTML, CSS, TypeScript	Angular 14

Development Environment

Development and testing relied on Ganache, which simulates a local Ethereum network and enables the deployment and invocation of smart contracts without incurring gas costs; Remix, a browser-based IDE for Solidity development, testing, and debugging that also produces the ABI and bytecode; Visual Studio and Visual Studio Code as IDEs for .NET and scripting tasks, respectively; Docker for container-based packaging and reproducible deployment; PostgreSQL as the relational database backing the business-rules layer; and Node.js as the runtime for front-end tooling.

Smart-Contract Coding and Deployment

The ControlSheet contract was coded and unit-tested in Remix, then compiled to ABI and bytecode. Access-control checks were placed on state-changing functions — only the contract owner may add documents or close the file — and the contract guards against operations on closed files. Once validated locally against Ganache, the contract was staged for deployment from the Repository Rules Microservice, which uses Nethereum to interact with the Ethereum JSON-RPC endpoint.

Construction of the Microservices

The User Interaction Microservice was implemented in Angular 14. Angular was preferred over Vue.js and React because of its prescriptive MVC architecture, which reduces onboarding time, its use of TypeScript for safer refactoring, and its integration with Google Firebase for deployment. Figure 3 shows a representative view of the resulting interface, with the navigation sidebar, summary indicators for active cases, a table listing active complaints with their states and hash-integrity check, and a detail panel exposing the address of the smart contract associated with the selected case.

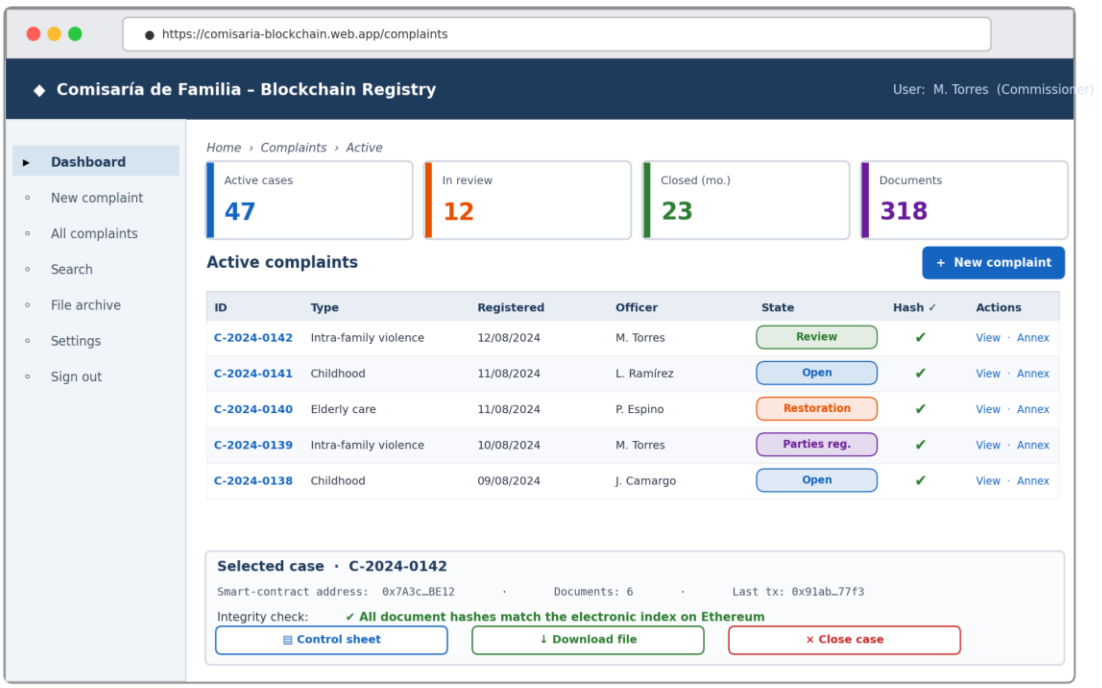

Figure 3. User Interaction microservice — dashboard view. The list exposes the state of each complaint and a per-case integrity indicator that compares the document hashes stored off-chain against the electronic index maintained by the ControlSheet smart contract.

The Business Rules Microservice was implemented in Ruby on Rails 6 and is responsible for encoding the domain logic of the Family Police Station, managing user access and permissions, keeping a local cache of blockchain data to optimize reads, and acting as an intermediary between user requests and the repository layer. Rails was chosen because of its rapid development cycle, the richness of its gem ecosystem (notably Devise for authentication and ActiveRecord as ORM), and its large community support. As user-facing presentation is handled elsewhere, the View layer of the MVC triad is intentionally minimized.

The Repository Rules Microservice was implemented in C# on .NET 6 following the Onion Architecture, because of its modular scalability — the Ethereum-facing service can evolve without impacting the domain core — its testability per layer, and its flexibility for experimenting with alternative libraries. Three storage paths are configured: Documents (the file repository for each complaint), Templates (the control-sheet and tamper-notification PDF templates), and ABI/Bytecode (the compiled smart-contract artifacts). When a digital file is created, a folder named after the file number is generated inside the virtual machine, and every annexed document is identified by a GUID to avoid name collisions.

Deployment Topology

The User Interaction Microservice and the Business Rules Microservice were deployed on Platform-as-a-Service (PaaS) offerings — Firebase and Heroku, respectively — which automate configuration, deployment, and functional test cycles. The Repository Rules Microservice could not be hosted on a PaaS because it requires specific hardware and software configurations, in particular an instance of Ganache acting as the Ethereum endpoint and a Windows Server environment for .NET 6. It was therefore deployed on an Infrastructure-as-a-Service (IaaS) virtual machine on Microsoft Azure, configured with IIS for web hosting and with dedicated storage for documents, compiled Solidity artifacts (JSON and bytecode), and the control-sheet and tamper-notification templates.

Functional Testing

A functional test plan was designed around the use cases and sequence diagrams. The results of the verification against functional requirements are summarized in Table II.

Table II. Verification of functional requirements.

Requirement	Verification question	Yes	No
RF-1 Web accessibility	Is the prototype accessible from desktop and mobile browsers?	✔	
RF-2 Type-based registration	Can processes be cataloged by type?	✔	
RF-3 Process state	Can the state be consulted by a user who is not the assignee?	✔	
RF-4 Document persistence	Does the system validate that each document matches its index hash?	✔	
RF-5 Process search	Can processes be searched by user-defined parameters?	✔	
RF-6 Digital file	Can the complete file be obtained on demand?	✔	
RF-7 Role-based permissions	Are permissions scoped by role?	✔	

- **Evaluation**

Design of the Evaluation

To validate the objective of the work, a proof-of-concept evaluation was conducted in which members of the Family Police Station managed fictitious complaints in their own workplace, using the infrastructure that is already available to them. The participants held the roles of Family Commissioner, Office Secretary, Psychosocial Worker, and Administrative Assistant. Sessions were kept concise and topic-linear because four of the participants are not on active duty during the standard attention schedule.

Evaluation Protocol

Three sessions were held:

• Session 1 — Presentation and objectives: the rationale, scope, and evaluation purpose of the work were presented; participants shared their expectations and suggestions.

• Session 2 — Prototype demonstration: a live demo was conducted around an intra-family violence process, followed by guided first interactions and a Q&A centered on information security.

• Session 3 — Simulated process management: participants managed two complete complaints with fictitious data, exercising registration, document annexation, transfer among roles, and closure.

At the end of the third session, a structured questionnaire was distributed to elicit opinions and improvement suggestions.

3. Results

The most salient outcomes are the unanimous agreement on document-authenticity validation (Q4) and the absence of disagreement about the prototype's capacity to improve management (Q6). The division of opinions on Q2 and Q5 is attributable to two factors identified during the sessions: concern about the disclosure of information subject to legal confidentiality (reserva sumarial) and the perception that alternative mechanisms already exist for some tasks. Regarding Q3, three out of four participants recognized that the ability to publish non-confidential information aligns with the principles of access to public information that govern Colombian public bodies.

Table III. Summary of survey results (n = 4).

Question	Main result
Q1. Have you heard of blockchain applications on products or platforms other than this prototype?	75% no; 25% yes (cryptocurrencies)
Q2. Do you trust that annexed documents are registered in an electronic index (control sheet) on blockchain?	50% trust; 25% uncertain; 25% prefer alternatives
Q3. Does public accessibility (excluding confidential data) on Ethereum benefit stakeholders?	50% yes; 25% current methods suffice; 25% no opinion
Q4. Can the prototype validate the authenticity of documents?	100% yes
Q5. Is confidential (reserva sumarial) information properly kept confidential?	50% yes; 25% uncertain; 25% no
Q6. Can the prototype improve management at the Family Police Station?	50% strongly agree; 25% agree; 25% neutral; 0% disagree

The evaluation suggests that blockchain is perceived as an effective mechanism to guarantee document authenticity within the workflow of a Family Police Station, which is consistent with the integrity and tamper-evidence properties reported in the general blockchain literature [1], [12] and in public-sector applications such as land registration [39] and digitized academic records [38]. The combination of an immutable electronic index on Ethereum with a centralized document repository respects the current Colombian archival framework — which requires centralized custody of materials subject to reserva sumarial — while still exposing non-confidential data to public scrutiny in the spirit of judicial transparency portals.

Compared with monolithic approaches, the microservices architecture simplified development, testing, and deployment, and allowed each layer to leverage the technology best suited to its responsibility (Solidity/.NET for the blockchain-facing layer, Rails for business logic, Angular for the user interface). The split also clarifies the regulatory boundary: the Ethereum-facing microservice handles hashes and metadata, while sensitive content remains inside the IaaS-hosted repository under institutional control.

Several limitations should be acknowledged. First, the evaluation involved four participants, which limits statistical generalization; however, it covers the full set of roles in a typical Family Police Station and therefore offers qualitative saturation. Second, although the public Ethereum network offers the strongest decentralization and neutrality, it also introduces gas costs that may be prohibitive for continuous operation at scale; permissioned alternatives (e.g., Hyperledger Fabric or a private Ethereum consortium among Colombian municipalities) would be worth exploring. Third, Colombian archival regulations have not yet been fully updated for distributed storage, which currently forces a centralized repository for documents containing reserva sumarial; a clearer normative framework would unlock richer decentralization designs.

Conclusions

This paper presented the design, implementation, and evaluation of a blockchain-based prototype for the registration and follow-up of complaints at the Family Police Station of Fusagasugá, Colombia. The prototype combines an Ethereum smart contract (ControlSheet) that acts as an immutable electronic index with a three-microservice architecture that handles user interaction, business rules, and document repository. The qualitative evaluation with the staff of the Family Police Station indicated that the solution is perceived as capable of validating document authenticity (100%) and improving complaint management (75% agreement or strong agreement). The smart contract, the source code of the centralized services, the user manual, and the mockups are publicly available in the repositories listed below.

Future work includes the expedition of a clearer Colombian normative framework for decentralized storage of case-file documents; the incorporation of WYSIWYG editors with institutional templates so that documents can be created and edited directly inside the prototype rather than uploaded; support for multimedia evidence (images, video, and audio captured by social workers) beyond PDF files; and the exploration of permissioned blockchain alternatives that reduce operational costs and provide explicit governance among municipalities.

Code and Data Availability

•User Interaction Microservice: https://github.com/lfcastanedar/UserInteraction

•Business Rules Microservice: https://github.com/lfcastanedar/BusinessRuleMicroservice

•Repository Rules Microservice: https://github.com/lfcastanedar/RepositoryRulesModel

•Project Documentation: https://github.com/lfcastanedar/FamilyCoinDocuments

•Live prototype: https://comisaria-blockchain.web.app/

Acknowledgments

The authors thank the staff of the Family Police Station of Fusagasugá for their time and insights during the participatory phases and the prototype evaluation, and the UNSecureLab Research Group of Universidad Nacional de Colombia for its institutional support.

References

[1] J. Prieto, A. K. Das, S. Ferretti, A. Pinto, and J. M. Corchado, Blockchain and Applications – International Congress, vol. 7. 2019.

[2] P. Grover, A. K. Kar, and P. Vigneswara Ilavarasan, "Blockchain for businesses: A systematic literature review," in Lecture Notes in Computer Science, vol. 11195, pp. 325–336, 2018.

[3] Observatory of Public Sector Innovation, Embracing Innovation in Government. Feb. 2019.

[4] I. Adam and M. Fazekas, Are Emerging Technologies Helping Win the Fight Against Corruption in Developing Countries? University of Oxford, 2019.

[5] T. Rahman, S. M. Rahman, and P. Ahokangas, Digital Government Review of Panama: Enhancing the Digital Transformation of the Public Sector.

[6] Observatory of Public Sector Innovation, Embracing Innovation in Government – Global Trends 2019. Feb. 2019.

[7] M. Xu, X. Chen, and G. Kou, "A systematic review of blockchain," Financial Innovation, 2019.

[8] J. Sun, J. Yan, and K. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," Financial Innovation, 2016.

[9] R. Herian, "Blockchain and the (re)imagining of trusts jurisprudence," Strategic Change, Aug. 2017.

[10] S. Manski, "Building the blockchain world: Technological commonwealth or just more of the same?" Strategic Change, Sep. 2017.

[11] C. Sullivan and E. Burger, "E-residency and blockchain," Computer Law & Security Review, vol. 33, no. 4, pp. 470–481, 2017.

[12] V. L. Lemieux, "Trusting records: Is blockchain technology the answer?" Records Management Journal, vol. 26, no. 2, pp. 110–139, 2016.

[13] D. Valdeolmillos, Y. Mezquita, A. González-Briones, and J. M. Corchado, "Blockchain technology: A review of the current challenges of cryptocurrency," 2020.

[14] B. Kewell, R. Adams, and G. Parry, "Blockchain for good?" Strategic Change, vol. 26, no. 5, pp. 429–437, 2017.

[15] M. Giancaspro, "Is a 'smart contract' really a smart idea? Insights from a legal perspective," Computer Law & Security Review, vol. 33, no. 6, pp. 825–835, 2017.

[16] G. J. Larios-Hernández, "Blockchain entrepreneurship opportunity in the practices of the unbanked," Business Horizons, vol. 60, no. 6, pp. 865–874, 2017.

[17] E. D. Zamani and G. M. Giaglis, "With a little help from the miners: Distributed ledger technology and market disintermediation," Industrial Management & Data Systems, vol. 118, no. 3, pp. 637–652, 2018.

[18] P. Gomber, R. J. Kauffman, C. Parker, and B. W. Weber, "On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services," Journal of Management Information Systems, vol. 35, no. 1, pp. 220–265, 2018.

[19] V. Shermin, "Disrupting governance with blockchains and smart contracts," Strategic Change, vol. 26, no. 5, pp. 499–509, 2017.

[20] T. Zalan, "Born global on blockchain," Review of International Business and Strategy, vol. 28, no. 1, pp. 19–34, 2018.

[21] M. Spearpoint, "A proposed currency system for academic peer review payments using the blockchain technology," Publications, vol. 5, no. 3, p. 19, 2017.

[22] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[23] M. Walport, Distributed Ledger Technology: Beyond Blockchain. UK Government Chief Scientific Adviser Report, 2016.

[24] M. Kranzberg, "Technology and history: 'Kranzberg's laws'," Technology and Culture, vol. 27, pp. 544–560, 1986.

[25] Congress of Colombia, Ley 594 de 2000 — Ley General de Archivos. Diario Oficial No. 44.084, Jun. 14, 2000.

[26] Presidency of Colombia, Decreto 4840 de 2007. Diario Oficial No. 46.846, Dec. 17, 2007.

[27] General Archive of the Nation (Colombia), Acuerdo 3 de 2015. Diario Oficial No. 49.431, Mar. 14, 2014.

[28] General Archive of the Nation (Colombia), Acuerdo 2 de 2014. Diario Oficial No. 49.097, Mar. 14, 2014.

[29] Colciencias, Manual de Gestión Documental, A104M03, v. 00, J. González, D. Yate, and G. Pereira.

[30] General Archive of the Nation (Colombia), G.INF.07 — Guía para la Gestión de Documentos y Expedientes Electrónicos, v. 1.0, 2017.

[31] Government of Colombia, Decreto 1080 de 2015. Diario Oficial No. 49.523, May 26, 2015.

[32] Congress of Colombia, Ley 2126 de 2021 — Comisarías de Familia. Diario Oficial No. 51.756, Aug. 4, 2021.

[33] S. Espinosa, Guía de Referencia de Blockchain para la Adopción e Implementación de Proyectos en el Estado Colombiano, v. 1, 2020.

[34] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? — A systematic review," PLoS ONE, 2016.

[35] B. Scott, J. Loonam, and V. Kumar, "Exploring the rise of blockchain technology: Towards distributed collaborative organizations," Strategic Change, vol. 26, no. 5, pp. 423–428, 2017.

[36] T. Kahn, A. Baron, J. Vieyra, and J. Cruz, Digital Technologies for Transparency in Public Investment: New Tools to Empower Citizens and Governments, 2018.

[37] A. E. Ibor, O. A. Ofem, and J. N. Obidinnu, "A conceptual framework for augmenting the security of digitized academic records in Nigerian tertiary institutions using blockchain technology," Apr. 2018.

[38] M. I. Khalid, J. Iqbal, A. Alturki, S. Hussain, A. Alabrah, and S. S. Ullah, "Blockchain-based land registration system: A conceptual framework," 2022.

[39] E. Westphal, B. Leiding, and H. Seitz, "Blockchain-based quality management for a digital additive manufacturing part record."

[40] M. Dave and R. Banoth, "Blockchain-based, decentralized evidence archive system using IPFS," 2022.

[41] P. Zhang, M. Walker, J. White, and D. C. Schmidt, "Metrics for assessing blockchain-based healthcare decentralized apps," 2017.

[42] Departamento Administrativo de la Función Pública, Concepto 115541 de 2023. Radicado No. 20236000115541, Mar. 21, 2023.