From Collection to Analysis: A Blockchain Solution for Transparent and Reliable Chain of Custody in the O&G Sector

Theo Caldas[1][a], Ana Lara Mangeth[1][b], Yang Ricardo Miranda[1], Paulo Henrique Alves[1][c], Rafael Nasser[1][d], Gustavo Robichez[1], Gil Marcio Silva[2] and Fernando Pellon de Miranda[2]

[1] *ECOA Institute, Pontifical Catholic University of Rio de Janeiro, RJ, Brazil*

[2] *Petrobras, Rio de Janeiro, Brazil*

{*theocaldas, analara-mangeth, yang, ph.alves, nasser, robichez*}*@puc-rio.br*, {*gilmarcio, fmiranda*}*@petrobras.com.br*

Keywords: Chain of Custody, Blockchain, Smart Contracts, Oil Spil, Oiled Fauna.

Abstract: The oil and gas (O&G) sector relies on a robust chain of custody mechanisms to ensure the transparency, integrity, and traceability of materials and environmental evidence. Traditional custody systems often suffer from inefficiencies, data fragmentation, and vulnerabilities to unauthorized alterations. This paper presents CustódiaBR, a blockchain-based solution designed to enhance the registration and monitoring of oily waste and oiled fauna samples collected during Petrobras's Beach Monitoring Projects (Projetos de Monitoramento de Praias - PMPs). CustódiaBR integrates real-time data from a centralized monitoring system and leverages the Brazilian Blockchain Network (RBB) to provide a transparent, immutable, and auditable custody record. The proposed system employs a hybrid on-chain/off-chain architecture, composed of five major components, ensuring data integrity while preserving confidentiality through cryptographic hash verification. Through a comparative analysis with existing blockchain-based forensic solutions, this study highlights the advantages of public-permissioned blockchain in industrial applications, demonstrating how CustódiaBR can serve as a model for digital chain of custody systems.

1 INTRODUCTION

The oil and gas (O&G) sector is characterized by complex operations that require high levels of traceability, transparency, and regulatory compliance. One critical aspect of these operations is the chain of custody, which ensures the proper documentation and tracking of materials, samples, and waste throughout their lifecycle (Bullerdiek et al., 2025). Chain of custody systems play a vital role in maintaining accountability and preventing unauthorized alterations or data loss. In particular, environmental monitoring programs depend on reliable custody mechanisms to track the collection, transportation, and analysis of oily waste and oiled fauna resulting from oil spills. Ensuring data integrity, transparency, and accessibility across multiple stakeholders is a key challenge in these processes, requiring innovative technological solutions.

Blockchain technology has emerged as a promising tool to enhance the reliability and auditability of custody systems in various industries, including O&G (Batista et al., 2023). Traditional document-based recordkeeping is susceptible to manipulation, inefficiencies, and inconsistencies between different organizations. By leveraging distributed ledger technology (DLT), blockchain introduces an immutable, decentralized, and tamper-resistant approach to storing and verifying custody-related data. While public blockchains provide high transparency, they present scalability and cost limitations, making permissioned blockchains a more suitable alternative for industry applications that require controlled access and regulatory compliance.

In this context, the Brazilian Blockchain Network (RBB) stands out as a government-led initiative that enables secure, permissioned data registration for public and private organizations in Brazil. RBB employs a modular architecture based on Hyperledger Besu, using Quorum Byzantine Fault Tolerant (QBFT) consensus mechanism to achieve high performance with reduced energy consumption. The network's hybrid governance model, often referred to

[a] https://orcid.org/0009-0003-3673-2692
[b] https://orcid.org/0000-0003-1624-1645
[c] https://orcid.org/0000-0002-0084-9157
[d] https://orcid.org/0000-0002-6118-0151

Caldas, T., Mangeth, A. L., Miranda, Y. R., Alves, P. H., Nasser, R., Robichez, G., Silva, G. M. and Pellon de Miranda, F.
From Collection to Analysis: A Blockchain Solution for Transparent and Reliable Chain of Custody in the O&G Sector.
DOI: 10.5220/0013497600003929

In *Proceedings of the 27th International Conference on Enterprise Information Systems (ICEIS 2025) - Volume 1*, pages 410-417
ISBN: 978-989-758-749-8; ISSN: 2184-4992

as public-permissioned, allows public read-access of the ledger, while restricting write and validate operations to trusted authenticated parties. The network topology, which includes validator, writer, and observer nodes, allows for efficient custody registration while ensuring compliance with industry regulations. This makes RBB a strong candidate for applications that demand robust traceability, transparency, and collaboration across multiple institutions.

This work presents CustódiaBR, a blockchain-based solution developed to enhance the chain of custody for oily waste and oiled fauna monitoring in Beach Monitoring Projects (Projetos de Monitoramento de Praias - PMPs). The system is designed to meet high industrial standards, as Petrobras acts at the global-level O&G sector, particularly in offshore exploration and production, and plays a crucial role in Brazil's economy and the international energy market. The full system-level architecture includes five integrated subsystems: (i) Backend Server / Database; (ii) GatewayBR Web3 Proxy; (iii) VIA (Sample Integrity Verifier) Frontend Application; (iv) Self-hosted Dashboard; and (v) Self-hosted Block Explorer. It integrates real-time data from Petrobras's SIMBA API and registers key custody events on RBB. It employs a hybrid on-chain/off-chain architecture, where critical metadata are recorded on the blockchain to ensure immutability, while more detailed custody records are stored in secure off-chain databases. This approach not only ensures data integrity and traceability but also addresses privacy concerns by preventing the exposure of sensitive environmental data.

This paper is structured as follows. Section 2 is focused on the concepts of chain of custody and public-permissioned blockchains. Section 3 presents the related work and Section 4 details the CustódiaBR solution. Finally, section 5 presents the conclusion and future work.

2 BACKGROUND

2.1 Chain of Custody in O&G Sector

Chain of custody refers to the systematic recording and accountability of custody, control, transfer, analysis, and disposition of an asset or evidence (Chopade et al., 2019). The chain of custody establishes a clear and verifiable pathway, demonstrating uninterrupted control and handling of assets from their origin to their ultimate destination. Ensuring accuracy in the chain of custody is important to avoid unauthorized access, tampering, or loss of assets and evidence. It is fundamental in legal, forensic and regulatory environments, as it ensures both the integrity and admissibility of evidence during judicial proceedings.

This process involves documenting key details such as date, time, location, individuals involved, and changes in custody. To meet these objectives, chain of custody protocols typically demand strict compliance with established procedures, prioritizing the preservation of the integrity and authenticity of assets throughout their lifecycle.

In the context of O&G, the chain of custody is also of great significance (Bullerdiek et al., 2025). In this field, effective control and traceability of materials, oily waste, and evidence handled throughout operational stages are essential. Examples of chain of custody applications in O&G include the traceability of oily waste, quality control of O&G samples, and fraud prevention in logistic operations.

This work focuses on the registration of the chain of custody for oily waste and oiled fauna resulting from oil spills, utilizing blockchain technology. These items are identified within the scope of PMPs, which oversee monitoring activities related to environmental licensing and aim to assess the impact of Petrobras's exploration and production (E&P) activities on marine tetrapods, which include birds, turtles, and marine mammals.

During beach monitoring, oily waste and oiled fauna samples are collected directly on the beach, where they are identified and stored for transfer to the PMP support base. Subsequently, they are transported to Petrobras laboratories for analysis. Thus, the sample follows a workflow comprising three main stages: (i) collection and delivery, (ii) reception and registration, and (iii) analysis and conclusion. At each of these stages, a specific system is used to record information, since the sample changes environments and custodians. In the first stage, the Aquatic Biota Monitoring Information System (Sistema de Informação de Monitoramento da Biota Aquática - SIMBA) system is employed, whereas in stages 2 and 3, Petrobras's laboratory information management system is utilized.

Hence, for the chain of custody, it is crucial that each handling step of the sample is thoroughly recorded. Relevant data related to these samples in the different stages include: the date and time they were found, the latitude and longitude of the location where they were collected, the name of the monitor responsible for the collection, the name of the field coordinator who registered the sample, the sample number, the laboratory identifier number, and the names of the custodians responsible for the analysis. The immutable blockchain registration of this set of information for each sample ensures the integrity, transparency, and traceability of the collected evidence, while also enabling the consultation of this data in case an audit is required.

2.2 Governamental Permissioned Blockchain

Blockchain governance is categorized into two distinct types: permissioned blockchains and permissionless blockchains. A permissioned blockchain is a DLT in which access to the network is restricted to authorized participants. Unlike public blockchains, which allow anyone to join and validate transactions, permissioned blockchains require pre-approved identities and specific governance mechanisms. This structure enhances security, ensures compliance with regulatory frameworks, and allows organizations to tailor the blockchain's architecture to specific operational needs. In the context of chain of custody, permissioned blockchains provide a controlled environment that ensures data integrity, transparency, and accountability while maintaining confidentiality where necessary.

The primary differences between permissioned and public blockchains lie in access control, performance, cost, and consensus mechanisms. Public blockchains, operate in a decentralized and trustless manner, leveraging mechanisms like Proof of Work (PoW) or Proof of Stake (PoS) to validate transactions. These consensus protocols often result in higher computational costs and lower transaction throughput due to their reliance on global validation processes.

In contrast, permissioned blockchains employ more efficient consensus algorithms, such as Practical Byzantine Fault Tolerance (PBFT) or Raft, which require fewer computational resources and provide faster transaction finality. Additionally, permissioned blockchains allow organizations to optimize network governance, reducing operational costs while maintaining robust security guarantees. In scenarios where a chain of custody must be established, a permissioned blockchain offers a more scalable and cost-effective solution by enabling selective participants to record data and faster transaction processing.

A relevant example of a permissioned-based blockchain initiative is RBB. It is a government-led initiative designed to provide a reliable and transparent infrastructure for public institutions and private entities in Brazil. It aims to improve the security and traceability of digital records while promoting interoperability between different organizations (Miranda et al., 2023). It is often referred to as a public-permissioned blockchain, since its governance model keeps the security and efficiency qualities of a permissioned network, through the usage of a Proof-of-Authority consensus mechanism, while enabling read-access to the general public. The network consists of multiple node types, including validator nodes responsible for consensus, writer nodes that submit transactions, and observer nodes that allow read-only access.

RBB employs Hyperledger Besu as its blockchain protocol, leveraging an energy-efficient consensus mechanism such as QBFT. This setup enables high throughput and low transaction costs while ensuring the immutability of records. In the context of chain of custody, the RBB stands out by offering a permissioned and auditable infrastructure where evidence records can be securely stored, preventing tampering and unauthorized modifications. Its governance model ensures accountability while maintaining efficiency, making it a strong candidate for applications that require rigorous data integrity standards.

3 RELATED WORK

This section provides an overview of the current state of the art in digital innovations in the O&G sector related to the chain of custody field. It particularly focuses on core industry activities, such as data traceability, transparency, and forensic investigation. The goal is to highlight the advancements and identify possible gaps compared to our solution.

Zawoad and Hasan propose Faiot, a forensics-aware ecosystem designed to integrate forensic capabilities directly into IoT devices (Zawoad and Hasan, 2015). Their approach aims to ensure the integrity and availability of digital evidence during investigations. In this sense, CustódiaBR operates at a broader operational level by integrating data from multiple centralized sources and registering relevant custody data in a public-permissioned blockchain. This allows CustódiaBR to achieve not only evidence integrity, but also greater traceability across the chain of custody, while mitigating data exposure risks through a hybrid on-chain/off-chain architecture.

Nelufule et al. propose an adaptive digital forensic framework tailored to address challenges in Industry 4.0 and 5.0. Their framework emphasizes the adaptation of forensic methodologies to evolving technological complexities (Nelufule et al., 2024). In contrast, CustódiaBR goes beyond forensic adaptation by operationalizing blockchain in a specific industrial application in the O&G sector. CustódiaBR integrates real-time data from Petrobras's SIMBA API and ensures reliable custody evidence through blockchain, providing end-to-end transparency in custody systems.

Kumar et al. introduce CourtSafe, a blockchain-based system for the secure storage and management of legal records (Kumar et al., 2024). While their solution is tailored for legal record management, CustódiaBR applies blockchain in a dynamic industrial context with real-time operational data. Additionally, CustódiaBR leverages its modular architecture, including GatewayBR for blockchain abstraction and a hash-based data integrity mechanism, to efficiently handle high-volume data while ensuring traceability.

Pawar et al. explore the use of graph-based neural networks combined with blockchain to enhance forensic investigations (Pawar et al., 2024). Their work focuses on improving anomaly detection and evidence analysis. CustódiaBR, on the other hand, ensures data integrity and transparency in a chain of custody specific to the O&G industry. Its practical integration of blockchain technology, supported by a modular and flexible infrastructure such as GatewayBR, addresses real-world challenges like regulatory compliance and blockchain interoperability, which are not directly addressed in the solution proposed by Pawar et al.

Rani et al. present a secure digital evidence preservation system for IoT-enabled smart environments using IPFS (InterPlanetary File System), blockchain, and smart contracts (Rani et al., 2025). Their solution focuses on ensuring the immutability and traceability of digital evidence. CustódiaBR differentiates itself by implementing a modular solution that includes GatewayBR, that supports multiple EVM-compatible networks. Moreover, CustódiaBR addresses privacy and computational efficiency concerns by storing sensitive data off-chain and ensuring data integrity using cryptographic hashes, making it more compliant with regulations such as the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais - LGPD).

These studies illustrate the transition from conventional document-centric methodologies to data-driven approaches facilitated by blockchain technology. In this context, solutions like CustódiaBR serve as key milestones in enabling the structured distribution of complex operational data. Moreover, they enhance coordination in multiparty environments by leveraging blockchain's immutability and decentralized trust model, ensuring greater transparency, efficiency, and reliability in custody-related processes.

4 DECENTRALIZED CHAIN OF CUSTODY SOLUTION

4.1 Architecture

CustódiaBR is a solution designed to leverage blockchain technology to promote traceability, transparency and integrity of operational data across custody systems in the O&G sector. It solves the task of collecting data from multiple centralized sources and registering relevant content in a public-permissioned blockchain, creating trustworthy and publicly available custody evidence while protecting sensitive data from undesired exposure.

In this research, the deployed CustódiaBR solution extracts sample-based data, e.g., geographic location of an oil leakage, from Petrobras SIMBA public REST API and writes it out to RBB via EVM-compatible smart contract. The full system-level architecture of CustódiaBR is the result of the integration of five subsystems, deployed as individual Docker containers:

- Backend Server / Database;
- GatewayBR Web3-Proxy Server;
- VIA Frontend Application;
- Self-hosted Dashboard; and
- Self-hosted Block Explorer.

Figure 1 presents the data flow diagram between these main components, regarding Petrobras DMZ infrastructure. The diagram also depicts the SIMBA data source, RBB blockchain service, and public external access.

[Backend Server]. It is a Java Quarkus application that schedules background routines to request RESTful data from the provided data sources and persists them in a unified PostgreSQL Database. The latter is of utter importance as different data sources may contain sample data at different stages of custody control. The server also fires routines to send a cluster of collected data to the RBB blockchain service by smart contract transaction call. This request is intermediated by GatewayBR Web3-Proxy Server, which will be described later on. The server provides sample data to the VIA Frontend Application through public REST API.

[GatewayBR]. It is a middleware designed to optimize communication between the application layer and blockchain service providers, working as a Web3 proxy to client applications. The developed server is a NestJS application that abstracts the complexities of blockchain networks, providing a REST API interface for deploying smart contracts and sending trans-

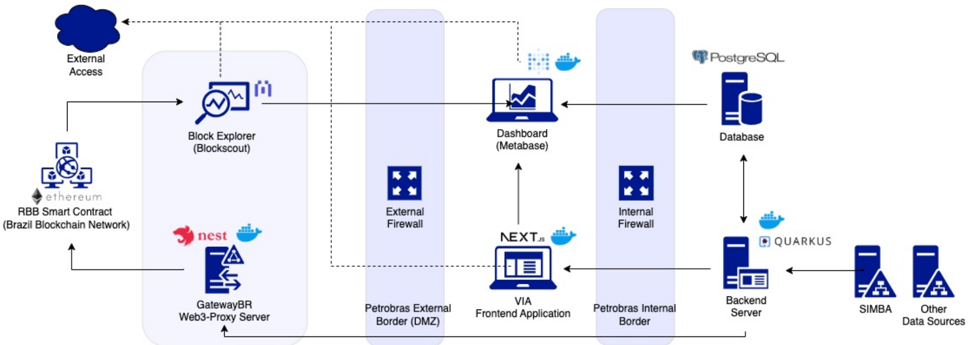

Figure 1: CustódiaBR system-level architecture.

actions. As blockchain technology evolves and execution and consensus protocols are replaced, the need for an intermediate layer architecture is crucial, especially because the application-to-network relation is many-to-many.

In fact, blockchain networks that use the same technology should be switchable in both the development and production application phases. Manually implementing these changes at the application level not only increases code cost, but also reveals security complexity on permissioned networks. Moreover, this “Plug and Play” approach allows flexibility in choosing blockchain service providers, reducing system coupling and promoting a more resilient and adaptable infrastructure.

GatewayBR REST API supports blockchain service providers operating on either Hyperledger Besu or Hyperledger Fabric platforms. In case of a provider based on Besu ETH-Client, such as the RBB network, the API expects the provider to be registered via `/evm-besu/chains` POST call. The client application informs the chain ID, a network alias and the URL to a valid JSON-HTTP-RPC node to receive further requests. Then, GatewayBR is able to process transactions by `/evm-besu/chains/{chainId}/transactions` POST call, which should include the chain ID, the deployed contract address, the command name (e.g., `registerCustodyEvent`) and the encoded call data. Also, it expects the client application to generate a UUID for the created transaction, facilitating later identification of the final status and the recipe that may contain logs from smart contract execution, block number and public transaction ID.

In the context of CustódiaBR, GatewayBR receives API calls from the Backend Server and transfers them to a registered RBB node, which interacts with the smart contract method `registerCustodyEvent` to persist sample data. The requests must include the chain ID linked to the previously registered network node.

[Frontend Application]. VIA is a NextJS web server that provides a solution for verifying data integrity in the chain of custody. It improves transparency and reliability in sample data audit and surpasses limitations imposed by data protection and computational performance, which excludes certain fields from its record on the blockchain (off-chain data). To mitigate vulnerabilities in off-chain data, the solution uses an approach based on cryptographic hashes, which enables fast validation of the collected data without exposing sensitive details, ensuring a more accessible, secure and efficient audit process. The VIA Frontend Application makes requests to the Backend Server through its provided REST API.

[Dashboard]. It is a Metabase[1] distribution that mirrors CustódiaBR Backend’s Database and enables user-friendly creation of interactive dashboards and custom queries. This improves sample data analytics and traceability, exposing relations between data from multiple sources.

[Block Explorer]. It is a Blockscout[2] instance, a block explorer service that enables transaction visualization of verified Solidity smart contracts, which was shown to be very helpful in the audit process. The service reads validated block information directly from public RBB network observer nodes, promoting transparent access through its web interface.

4.2 Data Source

CustódiaBR is designed to receive data from multiple data sources. However, the deployed version of the system was restrictively built upon Petrobras project for monitoring beaches along the Southeastern and Northeastern coast of Brazil. The objective is to evaluate possible interferences of Petrobras activities in the lifespan of aquatic and bird species located nearby oil offshore platforms.

[1] Metabase - https://www.metabase.com/

[2] Blockscout - https://www.blockscout.com/

As one of the many environmental transparency initiatives from Petrobras, data entries in Petrobras PMP are of public interest. The registered data is public-available through SIMBA, which offers, alongside its web application[3] a public non-authenticated REST API. It supports a single endpoint with multiple query parameters, retrieving sample occurrence data in XML format.

CustódiaBR Backend Server is a client of SIMBA public API, scheduling routines to fetch sample data within a date range. The query parameters `start_date` and `end_date` expose this filter option. To request data for a specific sample occurrence, it is possible to enter a `record_number` value, which refers to the `organismID` associated with that same sample. Other data filter options are listed in SIMBA official documentation[4].

For every fetched sample occurrence, there is an XML response, which contains a cluster of domain-related data, such as location, date and observations of the occurrence, as well as the name of the institution and the employee responsible for its registry. In case the occurrence refers to a dead or injured animal organism, data related to its taxonomy and life stage are also reported. Most retrieved occurrences also include measurement values of the sample.

Therefore, the ultimate goal of the deployed CustódiaBR blockchain solution is to guarantee the integrity of obtained SIMBA data in a transparent manner. This is key in custody control because, as shown in the mapped process mentioned in Section 2.1, those reports and pieces of evidence are transferred back and forth to other systems and laboratories. The blockchain layer of CustódiaBR acts as a shared source of truth between partners, since any adulteration of the collected data must be easily audited and noticed, so to mitigate inconsistencies in the chain of custody.

4.3 Blockchain Data Record

CustódiaBR blockchain layer, supported by GatewayBR, is adaptable to handle migrations between blockchain service providers. However, it is limited to EVM-compatible (Ethereum Client) providers operating under Hyperledger Besu. This design choice concerns the use of publicly readable decentralized ledgers, such as the RBB network, and the recording of sample data by transactions to smart contracts written in Solidity.

The smart contract should be structured in a non-cost-expensive way. Although RBB's underlying consensus mechanism is QBFT, known to be a low-computational Proof-of-Authority option for permissioned networks, any unnecessary data storage represents a performance reduction of the block validation flow. It would be unfeasible to record the many dozens of data fields for every fetched sample.

Another baseline aspect of smart contract development that should be considered is not exposing any personal/sensitive data since blockchain is an immutable database. Brazil's regulations on the collection, storage, and processing of private digital data are determined by LGPD, which currently does not contain a law that covers blockchain use cases.

Regarding both aspects, as mentioned before, the solution is to split the dataset into two categories: on-chain and off-chain data. In this context, on-chain data refers to a minimal cluster of values, for every fetched sample, that are written in the block record. This includes SIMBA sample identifiers - for instance, `organismID` and `measurementID` - and a calculated hash string of the entire XML response object, to preserve the integrity of the collected data as a whole. On the other hand, off-chain data are values excluded from the blockchain layer and stored in a secure database. It contains the majority of SIMBA API response fields.

The restriction of the values written on the blockchain may decrease the total transparency of on-chain data. To avoid that, off-chain data is stored in the CustódiaBR local Database and, then, displayed through the CustódiaBR Dashboard system, which aggregates all data fetched from SIMBA and links back to the blockchain record via transaction ID. That is, the solution depends on both on-chain and off-chain data, as the former guarantees the integrity of the latter, and the latter promotes transparency to the former.

4.4 Dashboard

The CustódiaBR Dashboard is a self-hosted Metabase service and has two main objectives: (i) to generate metrics and graphical visualizations of sample displacements; and (ii) to provide a single view that consolidates the core data of the entire chain of custody for a given sample, which includes both on-chain and off-chain stored data. The Dashboard is designed to receive, through database connection, data from various data sources involved in the custody control of the evidence and to generate different types of visualizations and analyses that may be relevant for diagnosis. An example of graphical visualization is the

[3] SIMBA - https://simba.petrobras.com.br/simba/web/

[4] SIMBA Documentation - https://simba.petrobras.com.br/simba/web/occurrences/doc

number of samples collected on a specific beach, filtered by time period, and the names of who monitored this place.

The Dashboard enhances the organization and visualization of data obtained from different systems (e.g., Petrobras's SIMBA API) on a single timeline. This includes data on all stages the sample has undergone (collection, registration, and analysis) and the custodians involved, as well as the status of the evidence at the time of access.

The view is fully customizable and can be adjusted to increase or decrease the level of data detail displayed. Filters can also be applied to facilitate user navigation. For every sample record, the view also links to the Block Explorer page on which its on-chain data was recorded, and displays a blockchain status value to identify if has been successfully recorded on the blockchain or remain unregistered.

The custom Dashboard view innovates by consolidating all the information in one place, enhancing transparency regarding the evidence chain of custody and facilitating control and accountability.

4.5 Integrity Verifier

Verifying the integrity of sample data is a core principle of CustódiaBR, ensuring a transparent audit workflow for the chain of custody. A key aspect of this process is the hash-based approach, in which the server records the hash string of the original collected data on the blockchain.

The Block Explorer web service allows public access to blockchain data, enhancing transparency through direct access to the network ledger. Once the deployed Solidity smart contract is verified, users can search for a transaction ID to find the recorded hash of a sample, calculated when it was retrieved from the Backend Server.

The audit workflow involves refetching the sample data from its original source, such as making a request to the SIMBA API using the sample's `organismID`, and manually recalculating its hash. If the recalculated hash matches the one stored on-chain, the data remains unchanged. Otherwise, it indicates that the data has been altered at the source.

Although the described steps illustrate a valid integrity verification process, they raise two main concerns that may affect the audit workflow effectiveness. Firstly, regarding Petrobras' general public interest, most users experience readability difficulties when accessing low-level block explorer data. The system should output with confidence that a said cluster of data is reliable without the user's need to know blockchain-related concepts, such as validated blocks, transactions, smart contracts, log events, and so forth. This kind of abstraction can be achieved by a custom user-friendly GUI.

The second issue relates to the fact that hash calculations are highly sensitive to any change in its input. For a valid hash comparison, the digital artifact being verified must be structurally identical to the one stored on-chain. Any digital modification, at the bit level, will produce a different hash, regardless of whether it alters the meaning of the data itself. This sensitivity makes user-driven hash calculations prone to errors and incorrect conclusions. The system should be able to mitigate these inconsistencies by automatically returning the valid hash string of the refetched original data.

The CustódiaBR VIA Frontend Application simplifies integrity verification with an intuitive web interface, as depicted in Figure 2. Users provide the sample data and receive an instant hash comparison result. The deployed application processes XML responses from the SIMBA API and enhances the audit workflow. If data modification is suspected, the user retrieves the `organismID` from the Dashboard and requests the original XML file from the SIMBA public API using this ID. The XML input data can be manually entered into the web interface or uploaded as a file. The application immediately calculates the hash on the client side using the SHA-256 function.

The system then detects the sample identifier and requests the on-chain hash from the Backend Server. The application displays the final comparison message and the two hash values: one from the user-provided XML and the other from the blockchain. If the hashes match, the data is considered unchanged. Otherwise, modifications have occurred between the original registration and retrieval.

5 CONCLUSION AND FUTURE WORK

This paper explored the application of public-permissioned blockchain technology to enhance chain of custody processes in the O&G sector, particularly in the context of environmental monitoring. By integrating RBB as blockchain infrastructure with existing digital systems, the proposed solution ensures data transparency, integrity, and traceability, enabling reliable custody records. The hybrid on-chain/off-chain architecture avoids exposing sensible recorded data while maintaining the immutability of custody records.

The future work relies on expanding the scope of blockchain integration beyond environmental custody

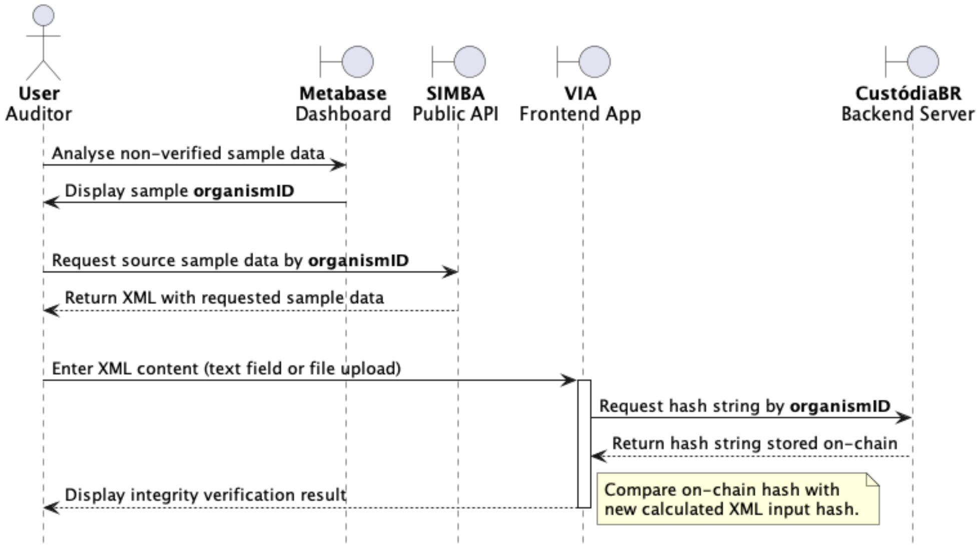
User
Auditor
Metabase
Dashboard
SIMBA
Public API
VIA
Frontend App
CustódiaBR
Backend Server
Analyse non-verified sample data
Display sample organismID
Request source sample data by organismID
Return XML with requested sample data
Enter XML content (text field or file upload)
Request hash string by organismID
Return hash string stored on-chain
Compare on-chain hash with new calculated XML input hash.
Display integrity verification result

Figure 2: Sequence diagram of the audit workflow.

to include logistics, asset management, and regulatory compliance frameworks in O&G operations. Enhancing smart contract automation for custody validation, anomaly alert mechanisms, and integration with IoT-enabled tracking devices could further improve system efficiency and data reliability.

Additionally, the next step should focus on interoperability between multiple blockchain networks, to enable cross-organizational data exchange while preserving privacy and security. This includes exploring zero-knowledge proofs (ZKPs) and confidential computing to enhance data confidentiality in blockchain-based custody records.

REFERENCES

Batista, D., Mangeth, A. L., Frajhof, I., Alves, P. H., Nasser, R., Robichez, G., Silva, G. M., and Miranda, F. P. d. (2023). Exploring blockchain technology for chain of custody control in physical evidence: A systematic literature review. *Journal of Risk and Financial Management*, 16(8).

Bullerdiek, N., Pechstein, J., Quante, G., and Kaltschmitt, M. (2025). Chain-of-custody models for renewable fuels: A comparison of basic characteristics. In *Powerfuels*, pages 1025–1056. Springer.

Chopade, M., Khan, S., Shaikh, U., and Pawar, R. (2019). Digital forensics: Maintaining chain of custody using blockchain. In *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pages 744–747. IEEE.

Kumar, R., Agarwal, H., Tayal, A., and Nagaraja, H. (2024). Courtsafe: Legal records storage & management using blockchain. In *Proceedings of the 2024 Sixteenth International Conference on Contemporary Computing*, pages 726–734.

Miranda, Y., Alves, P., Paskin, R., Nasser, R., Robichez, G., Faria, L., Trindade, R., Silva, J., Peixoto, L., and Miranda, F. (2023). Enhancing corporate social responsibility with blockchain-based trackable esg tokens. In *Anais do VI Workshop em Blockchain: Teoria, Tecnologias e Aplicações*, pages 112–125, Porto Alegre, RS, Brasil. SBC.

Nelufule, N., Singano, T., Masemola, K., Shadung, D., Nkwe, B., and Mokoena, J. (2024). An adaptive digital forensic framework for the evolving digital landscape in industry 4.0 and 5.0. In *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, pages 1686–1693. IEEE.

Pawar, P. P., Kumar, D., Bhujang, R. K., Pareek, P. K., Manoj, H., and Deepika, K. (2024). Investigation on digital forensic using graph based neural network with blockchain technology. In *2024 International Conference on Data Science and Network Security (ICDSNS)*, pages 1–7. IEEE.

Rani, D., Gill, N. S., Gulia, P., Yahya, M., Ahanger, T. A., Hassan, M. M., Abdallah, F. B., and Shukla, P. K. (2025). A secure digital evidence preservation system for an iot-enabled smart environment using ipfs, blockchain, and smart contracts. *Peer-to-Peer Networking and Applications*, 18(2):1–29.

Zawoad, S. and Hasan, R. (2015). Faiot: Towards building a forensics aware eco system for the internet of things. In *2015 IEEE International Conference on Services Computing*, pages 279–284. IEEE.